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

Wing Commander Maxmillan GG[@]

"क्रोधाद्भवति सम्मोह: सम्मोहात्स्मृतिविभ्रम: |

स्मृतिभ्रंशाद् बुद्धिनाशो बुद्धिनाशात्प्रणश्यति ||"

"Anger leads to clouding of judgment, which results in bewilderment of memory. When memory is bewildered, the intellect gets destroyed; and when the intellect is destroyed, one is ruined".

— Chapter 2, Verse 63 - Bhagavad Gita

Abstract

This essay examines cognitive warfare as a critical and evolving domain in modern conflict, focused on influencing human minds. Tracing the fundamentals of Cognitive Warfare (CW) strategies, the essay establishes its reach beyond traditional psychological and information warfare. It further assesses global strategic threats, focusing on international players, state and non-state actors. This essay proposes a comprehensive National Cognitive Warfare Strategy for India, blending traditional wisdom with today's security needs. It identifies key pillars for building global ecosystem engagement, defensive

---

[@]**Wing Commander Maxmillan GG** is an Indian Air Force officer with 18 years of service and extensive experience as a Weapon System Operator on Su-30 MKI aircraft. He specialises in aerial warfare, war planning, electronic warfare, multi-domain operations and imagery intelligence. A qualified Psychologist Assessor, he has experience in inter-service operations, policy formulation and humanitarian assistance and disaster relief. He holds postgraduate degrees in Aviation Law and Air Transport Management and Psychology.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

resilience and offensive capabilities, while addressing institutional challenges, legal reforms and future technological trends. Ultimately, it lays out a vision for moving forward that focuses on merging different sectors, updating laws, using innovative and balanced strategies, developing talent, fostering innovation, and expanding into new areas. The essay underscores CW's pivotal role as a sixth domain of warfare in shaping India's advance as a global leader.

Introduction

In modern warfare, the functionality of human cognitive components—perceptions, attitudes, and behaviour—is a critical determinant of outcomes. Historical strategists like Sun Tzu, Clausewitz, and Kautilya discussed altering cognition in conflict, though Cognitive Warfare (CW) was not formally recognised as a distinct domain. Traditionally, CW manifested through psychological and information warfare methods such as perception management, information control, deception, decoys, concealment, or economic strangulation to gain advantage with minimal physical confrontation. In the 21st Century, technological progress has radically expanded the scale and speed of information and mis/disinformation dissemination. Internet of Things, social networks, and mobile technologies propel this hyper-connectivity.[1] Intra- or inter-connected homophilic societies make distances and boundaries almost non-existent. The world is at a crossroads where opinion-driven narratives overshadow facts, and human mind polarisation is the new norm. This paradigm shift elevates CW beyond traditional warfare mechanics as a quintessential method clasping its tentacles around the originator and progressors of war–the 'Human Mind'.[2]

Diverging from prevailing Indian commentary, this essay examines CW as an interconnected, penetrating method of warfare that extends beyond information and psychological warfare. It will first explain CW. Secondly, it will examine the strategic threat landscape. Thirdly, it will propose a national cognitive warfare strategy for India. Fourthly, it will identify key pillars of India's cognitive warfare approach.

And fifthly, it will analyse challenges to institutionalising CW and recommend a domain-specific path for India.

Understanding Cognitive Warfare

Cognitive Science. A foundational understanding reveals cognitive science as an interdisciplinary field.[3] It transcends the spectral boundaries of science, social science and allied arts. It includes subjects like psychology, anthropology, computer modelling, and Artificial Intelligence (AI),[4] philosophy, political science, sociology, and neuroscience. The North Atlantic Treaty Organisation (NATO) describes it as the convergence of cyber-psychology, the weaponisation of neuroscience, and cyber-influence.[5] CW is the superset of coordinated information, psychological and cyber operations.[6]

Defining CW. A useful definition: 'Cognitive Warfare is a strategy that focuses on altering how a target population thinks and, through that, how it acts'.[7] It alters natural cognitive processing of how others think, feel or act. By shaping the 'Who' (Communicator), 'What' (Message), 'Which' (Medium), 'Whom' (Receiver), 'When' (State) and 'How' (Effect) of communication[8]. It is deemed to exist when the end game of altered behaviour is achieved through shaped perceptions, influenced attitudes or hindered memory processing.

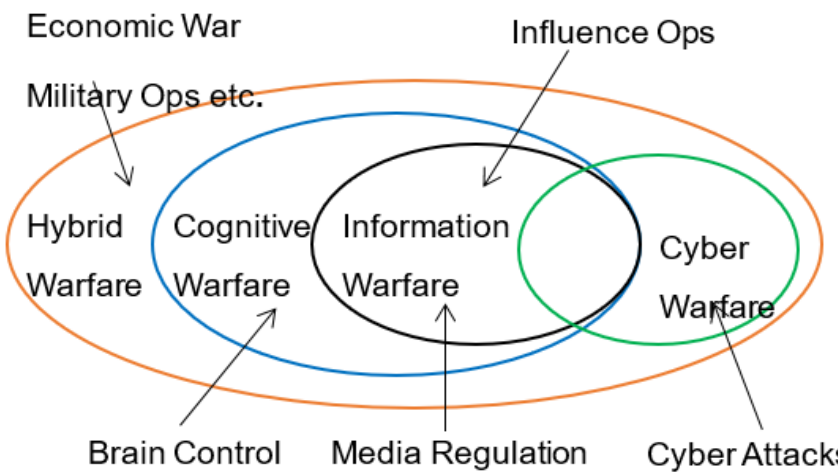


Figure 1: Relationship among Cognitive Warfare and Other Types of Warfare

Source: Journal of Global Security Studies[9]

Segments of CW. For effective application, CW involves influence, information, psychological, cyber, space, and neuroscience operations, with a legal watch for ethical regulation. It penetrates deeper into neurological, socio-cultural and behavioural systems, disrupting social unity and undermining group resolve to impact society's collective cognition. Unlike traditional warfare, it steers individuals or societies overtly or covertly to achieve victory without a battle. It permeates all existing domains—land, sea, air, space, and cyberspace—emerging as the sixth domain of warfare.[10]

The Strategic Threat Landscape

NATO Perspective. Having understood the significance of CW, it is essential to grasp its evolving strategic threat landscape. The NATO Warfighting Capstone Concept already recognises a CW strategy.[11] The inaugural NATO scientific meeting on CW was held at Bordeaux in France on 21 Jun 2021.[12] NATO Allied Command Transformation in Norfolk, United States (US), emphasises the militarisation of Nanotechnology, Biotechnology, Information Technology, and Cognitive Science technologies. Like the Modelling and Simulation Group, their teams focus on research and development.[13]

Adversarial CW. The West depicts Russia as a key CW actor and a model for China, Iran, and North Korea.[14] They claim that Russian tactics, rooted in the Soviet concept of reflexive control,[15] are used to challenge democratic processes in the US,[16] Baltic states and France.[17] The Chinese Communist Party's United Front is implicated in electoral interference in Canada, Australia, and New Zealand.[18] North Korea combines nuclear coercion with cognitive manipulation to influence decision-making,[19] while Iran spreads social and moral jihad propaganda against the US and Israel through universities and religious centres to foment internal dissent.[20]

China's Three Warfares. CW in the Indian neighbourhood is a significant and evolving challenge. China implements the '*San Zhong Zhanfa'* or Three Warfares strategy, which involves public opinion, psychological, and legal warfare.[21] It is a stratagem based on Sun Tzu's principle of subduing adversaries without direct conflict. These

strategies were evident during the Doklam standoff (2017) and the Galwan Valley clash (2020). China preferred non-kinetic tactics, using government information departments to shape perceptions and avoid direct military engagement with India.

Pakistan's CW. Pakistan's Inter-Services Public Relations abuses social media to invoke societal divisions and incite unrest.[22] During Operation Sindoor, Pakistan employed AI-generated deep fakes and disinformation targeting India's democracy, leadership, military and public sentiments.[23] India's Ministry of Information and Broadcasting, backed by the Army's Corps of Signals and the National Cyber Coordination Centre, stepped in to push back. Indian approach was centred on open updates, primarily through daily briefings from the Ministry of External Affairs. While the response was quick, it was reactive. It was neither coordinated nor built from any long-term system, relying more on exposing misinformation than being proactive.

Non-State CW. Beyond conventional conflict scenarios, proxies, non-state actors, and institutions adopt CW to manipulate perceptions, influence behaviour and destabilise societies. Terrorist and separatist groups in Jammu and Kashmir have exploited CW through social media to further their agendas, recruit youth and incite religious extremism to fuel unrest and undermine security forces.[24] The Havana Syndrome case, though unattributed, exemplifies CW infiltrating the physical domain and causing neurological damage.[25]

Classifications of CW Threats. An assessment of the threat landscape identifies three broad categories of CW targets based on scale: large groups sharing common characteristics (such as populations and ethnic or religious communities), smaller groups united by common objectives (such as companies, teams and armed forces), and critical individuals (such as decision-makers and leaders). These targets can be further classified by their degree of cognitive permeability into open societies (democracies), closed societies (dictatorships or autocratic regimes), and controlled societies, where stringent regulations or legal frameworks restrict information dissemination.

India's National Cognitive Warfare Strategy

Need for NCWS. The emerging strategic threat landscape highlights the vulnerabilities of this sixth dimension of warfare, emphasising the need to develop India's National Cognitive Warfare Strategy (NCWS). Kautilya's Arthashastra, our ancient treatise on statecraft, posits that 'A Well-reasoned Policy' serves as the fundamental thread that ensures the stability of the state.[26] Therefore, this formulation process must be elaborate, resolving asymmetric balances and questioning confusing dogmas focused purely on risk management and reduction.[27]

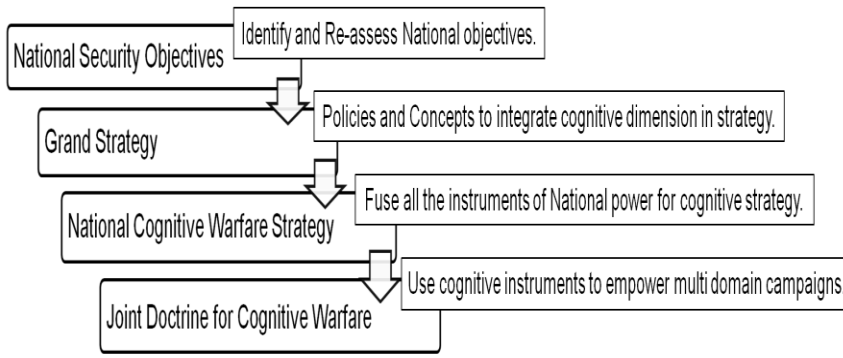


Figure 2: India's National Cognitive Warfare Strategy
Source: Compiled by the author

NCWS Framework. The NCWS must align with national security objectives and grand strategy, leverage contemporary strengths, and address gaps. A practical, pragmatic roadmap for the NCWS may be led by a high-level national security authority, such as the National Security Coordination Secretariat, which would act as a facilitator, advocate, and guardian. It should be a unified, specialised framework integrated across all instruments of national power, with grand strategy serving as the overarching mechanism synchronising military and non-military elements. Under its umbrella must exist the Joint National Cognitive Task Force, a purpose-driven, whole-of-nation team of government agencies, intelligence, armed forces, paramilitary, think tanks, academia, cyber institutions, industry, start-ups and society.

NCW Doctrine. A National Cognitive Warfare Doctrine (NCWD) must derive from the NCWS to establish actionable subordinate doctrines across all national power instruments at strategic, operational, and tactical levels. Respecting the sensitive nature of some elements, the NCWD can have public and classified versions.

Joint CW Doctrine. Drawing inspiration from the combined national approach, the military must weave its own Joint Doctrine for Cognitive Warfare (JDCW). This doctrine must be built on the existing Joint Doctrine for Multi-Domain Operations, Joint Doctrine for Perception Management and Psychological Operations, and the Joint Doctrine for Cyber Space Operations. This doctrine should form a flexible framework aligned with the grand strategy, coordinating all military CW capabilities through the Joint Planning Coordination Centre under the Chiefs of Staff Committee.[28] The JDCW should adopt a future-oriented, holistic outlook, emphasising strategic resource allocation and inter-agency coordination for seamless implementation. It should remain fundamentally stable, allowing only structural updates dictated by the doctrinal loop. It must establish clear strategic definitions to streamline operational planning and approvals across conflict levels.

Joint CW Team. Driven from a military vantage, a Joint Cognitive Warfare Team can execute goal-specific tactical cognitive operations. Because it is military-heavy, the team can also include embedded elements from all other segments of national power. Further, individual services should establish specialised teams to explore this domain without rigid boundaries hindering effectiveness.

Key pillars to India's Cognitive Warfare approach

India's CW approach should be based on the principle of 'One for All, All for One'. Based on this philosophy, the three pillars are the global ecosystem, defensive (domestic), and offensive (adversary), as shown in Figure 3. These pillars have co-functionality to prevent counter productivity, mandating existence in parallels and intersections.

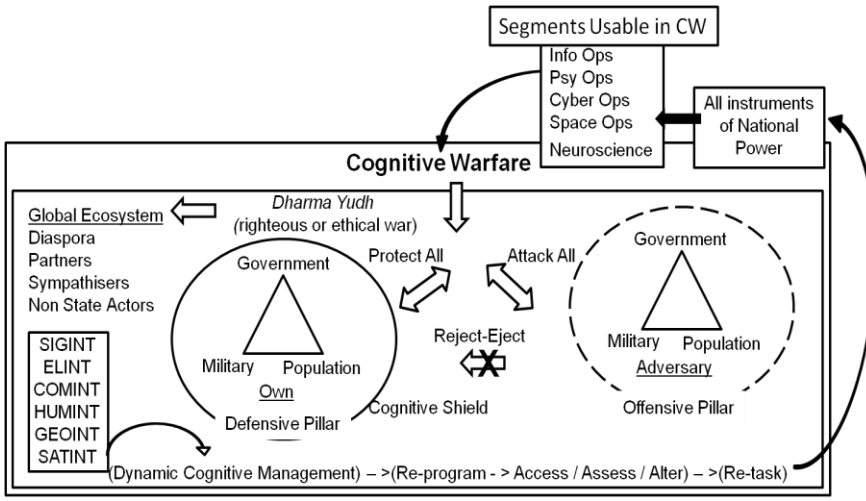


Figure 3: Pillars to India's Cognitive Warfare Approach
Source: Compiled by the author

The Global Ecosystem Pillar. India's CW strategy calls for unified global outreach that leverages soft power to shape international perceptions favourably. This includes engaging the diaspora, partners, non-state actors, and sympathisers through think tanks, media, sports, and cultural interfaces like yoga, arts, literature, cuisine, cinema, democratic traditions, and socio-economic exchanges.[29] Emphasising spirituality, socio-cultural values and democratic principles, India should spearhead multilateral cognitive organisations, convene summits and conduct cognitive gaming exercises to address security challenges collaboratively. Each kinetic military action should be paired with a cognitive initiative ensuring transparency and global support under the *Dharma Yuddha* (righteous or ethical war) principle. Platforms like the Raisina Dialogue and the Indian Ocean Conference aid coalition building, diplomatic isolation of adversaries and strategic communication.

Defensive Pillar: Safeguard One's Own Interests. Establishing cognitive safeguards to thwart adversarial attempts and secure India's national power instruments, including the population, government, and military, is essential. A cognitive shield must begin with a comprehensive risk assessment of the population-government-military trinity. Clear demarcation of cognitive

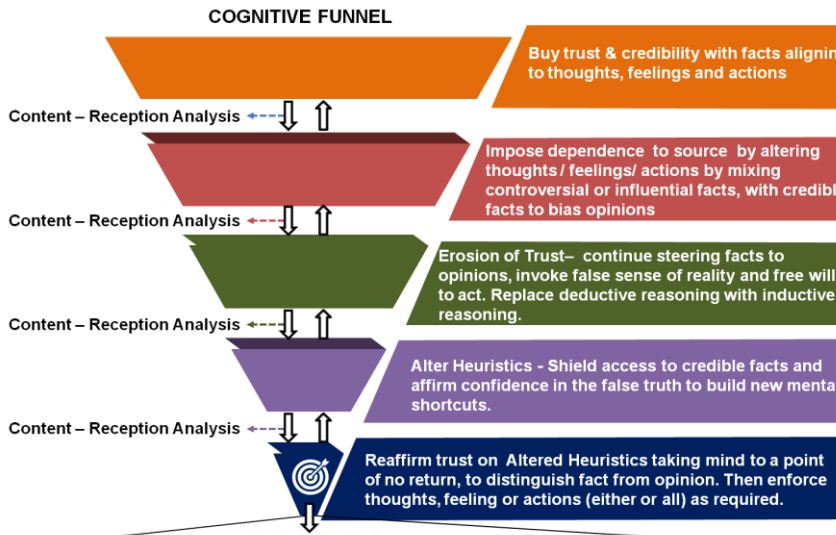
boundaries and management of functional overlaps is vital to create impenetrable defences. India's vast digital ecosystem, with over 700 million internet users, is a critical battleground. A layered resilience posture that incorporates these strategies can insulate the shield against foreign propaganda and targeted disinformation. Mass digital literacy is imperative to withstand shocks and prevent information operations and psychological tactics enhanced by AI and machine learning from eroding trust in democratic institutions.

Cognitive Resilience. An enhanced 'Observe, Orient, Decide, Act loop' for all decision-makers, built on unhindered access to factual data, will be the pillar's foundation. This involves redundancy in critical systems, supported by a culture of continuous learning. Allowing citizens to verify facts is vital to demystifying CW identification and data transparency. Such heightened awareness is essential for the stability and security of India's 1.46 billion citizens. Effective defence measures should serve as proactive deterrents, ensuring unhindered battlefield visibility through satellite surveillance and high-resolution imagery. Additionally, initiatives to condition hearts and reprogram minds are indispensable.

Offensive Pillar. Indian values of Ahimsa and Non-Alignment have kept Indians rooted in collective consciousness for peaceful co-existence. However, provocations necessitate defensive and offensive counterbalancing. Employing a hierarchical CW Matrix with escalation and de-escalation protocols maintains this equilibrium. Offence begins with eliminating attack detection and attribution errors, followed by clear rules for engagement, intrusion, neutralisation, extraction, and termination to ensure precision and control. The matrix should follow the principles of war and manoeuvre warfare at lower levels, unsettle the enemy's Centre of Gravity, and target vulnerabilities to fracture adversarial cohesion. Advanced phases must engage multi-spectral cognitive traps across all its segments to disrupt decision-making covertly. A Dynamic Cognitive Management Team can continuously adapt the response to match the progression of warfare.

Cognitive Trap. The author proposes exploring spiralling neural pathways through a cognitive funnel into a cognitive trap (shown in

Figure 4). This psychologically grounded strategy will be particularly effective for dominating CW. As shown, establishing a causal effects relationship shall permit deployment of harmful payloads to achieve cognitive supremacy. Such methods can be applied broadly within the Offensive Pillar. Other methods include unplug, corrupt, disorganise, diagnose and enhance.[30]



Likely Cause	Cognitive Dissonance, Distortion, Intrusive Thoughts	Apathy/Avolition, Cognitive overload, Thought blocking,	Counterfactual thinking, Overgeneralization, Faulty Emotional Regulation, Bandwagon effect	Precognition, Learned helplessness, Distorted Perception	Emotional override	Affect heuristic	
THINK	✓	✗	✗	✓	✓	✗	✗
FEEL	✗	✓	✗	✓	✗	✓	✗
ACT	✗	✗	✓	✗	✓	✓	✗
Likely Effect	Belief Bias, Emotional Numbing or Dissociation, Confirmation Bias, Loss Aversion, Counterfactual Thinking, Unconscious biases, Negativity bias	Availability Heuristic, Framing Effects, Hindsight Bias	Intention-Behavior Gap, Automaticity, Attention Bias, Foolhardiness, Fear (flee), Representativeness heuristic	Anchoring bias, Confirmation bias, Paralysis by Analysis, Status Quo Bias		,	Total Non - functionality
✓	Functioning of the specific component of Cognition, though not confirmed to be at desired level.						
✗	Non - functioning of the component of Cognition at desired level, though not confirmed to be purely non-functional.						

Figure 4: Suggested usage of Offensive Pillar
Source: Compiled by the author

Challenges to institutionalising CW

While India has seen how to build her CW strategy, one must understand certain challenges when employing it.

Intent to understand, appreciate, and employ it. CW is inherently disruptive and non-linear, and requires recognition of its dual nature as both a threat and an opportunity in hybrid and grey zone conflicts. Its distinction from cyber, information and psychological warfare must not be overlooked. Effective employment requires a pragmatic strengths, weaknesses, opportunities and threats analysis. Reluctance to formalise strategies stems from rigidity and fear of criticism, hindering effective risk management.

Barriers to Unified Integration and Collective Thinking. This domain rides upon advancing technological capabilities. Siloed research, insufficient interdisciplinary collaboration, and fragmented national efforts across government, military, intelligence, media, and information technology sectors exacerbate contradictory cognitive missions. Unaddressed fundamental gaps, a void of cohesion, integration and fusion- shake the foundations of the pillars of national cognitive strongholds.

Capability Building Measures in Human Resources and Infrastructure. A limited indigenous focus on AI, machine learning, and cloud infrastructure hinders capability building. Innovations fail to transition from academia to industry because research remains limited to theoretical or small-scale studies. Micro, small and medium enterprises face financial and regulatory barriers, resulting in low technology adoption and skill gaps.[31] Scalability requires enhanced infrastructure and streamlined processes.

Ethical and Human Rights Concerns. Current legal and regulatory frameworks lag behind technology, requiring a strong ethical and legal structure to isolate aberrant actors. CW operates in international legal grey areas and lacks explicit provisions under international humanitarian law or the UN Charter. Cognitive operations below armed conflict thresholds pose significant legal challenges. The capacity of *the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam of*

2023 to attribute cognitive activities as offences against the state, organised crime, and terrorism is ambiguous.[32]

Way forward

Advance from Integration to Fusion for Domain Capability. Capability development should commence with robust cognitive shielding and progressively evolve towards offensive cognitive capabilities. Strengthen population resilience through digital literacy, critical thinking, and metacognitive training to counter misinformation, disinformation, deep fakes, and engineered social media narratives. Long-term capacity-building should leverage advanced technologies, including artificial intelligence and data analytics, to maintain an up-to-date understanding of adversary information ecosystems and behavioural patterns. An integrated whole-of-nation approach that brings together government, military, academia, industry, and civil society is essential to bridge existing capability gaps and ensure inclusivity. A centralised national agency should provide strategic direction, standards, and oversight, supported by decentralised operational entities for effective implementation. Finally, sustained global engagement with leading research institutions and think tanks, coupled with the creation of autonomous, mission-oriented innovation teams, will foster indigenous expertise and accelerate the development of cognitive warfare capabilities within a robust national security framework.[33]

Legal Reforms and International Cooperation. Implement policy reforms and strengthen international cooperation. Expand the legal framework to regulate the misuse of the cognitive domain at both the domestic and international levels. Establish a legal tribunal within the national security architecture to oversee violations relating to cognitive warfare. Adopt adaptive cybersecurity laws and information-sharing models inspired by Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA), while safeguarding democratic freedoms and freedom of expression.

Develop Balance for CW Tactics. Cognitive tools can either exploit or enhance human cognition, making the offence-defence balance crucial for preserving force and optimising performance. This includes integrating counter-propaganda, strategic communication, and resilience training. Develop advanced AI-driven detection of disinformation and social engineering to mitigate echo chambers, biases, and targeted manipulation. The focus of offence must evolve from merely understanding adversaries' minds to actively shaping their actions.

Invest in Human Resources and Innovate Emerging Technologies. Invest in human resources and innovation through multidisciplinary convergence. Support talent development, public-private partnerships and advances in cognitive sciences, including generative AI, cyber forensics, machine learning, deep learning and quantum computing. Build infrastructure for related industries such as semiconductors, encrypted networks, satellite systems and sustainable energy. Promote initiatives like Innovations for Defence Excellence and Ran Samwad to drive cognitive war games and disruptive technology innovation.

Explore Novel Applications in the Domain. Exploring CW requires the intelligent application of smart power, blending soft and hard power strategies. Cultural influence must complement kinetic readiness. Future planning should anticipate advances in biometric targeting, neurotechnologies, and metaverse operations. Cognitive Warfare will increasingly involve neuromorphic systems, neural interfaces, advanced neuromodulation, and humanoids that integrate human and machine cognition. Having studied the challenges and the whole-of-nation approach required to implement CW, Table 1 presents a suggested practical way forward across various CW segments.

Segments Usable in CW	**Levels of CW**		
-	**Strategic**	**Operational**	**Tactical**
Influence Ops	Ministry of External Affairs, Tourism Ministry, Ministry of Finance	Embassies, United Nations, Intergovernmental organisations	Armed Forces, Paramilitary, Police, Journalists, Content Creators, Social Media Influencers, Veterans, Diaspora, Tourists, Legal cell, Defence Public Sector Undertakings (DPSUs), Public-Funded Research Institutions, large corporates, Small and Medium Enterprises (MSMEs), Start-ups, Academia, Think Tanks, Non-State Actors, Civil Society Groups, and Expats.
Information Ops	Information and Broadcast Ministry, Ministry of Home Affairs	All Intelligence Agencies, Own media in foreign vernacular, social media	
Psychological Ops	Ministry of Defence	Defence Institute of Psychological Research, Indian Psychological Association	
Cyber Ops	Ministry of Electronics and Information Technology, Ministry of Science and Technology	Computer Emergency Response Team, Defence Cyber Agency, Department of Scientific and Industrial Research	
Space Ops	Indian Space Research Organisation	Defence Space Agency	
Legal	Supreme Court of India	High Courts (CW Tribunal*)	

Segments Usable in CW	**Levels of CW**		
-	**Strategic**	**Operational**	**Tactical**
Neuro Science	Ministry of Health and Family Welfare	Central Drugs Standard Control Organisation (Directorate General of Health Services), National Institute of Mental Health and Neurosciences	
Note: All segments must operate with balanced independence and interdependence, employed in land, sea, air, cyber, and space domains synchronously through an integrated command and control, with tactical elements interoperable across segments. All three pillars of CW outlined in the essay must be addressed at every level. The military should have access to any segment as required, under the aegis of JDCW. (* is put for the organisations that need to be constituted from existing resources).			

Table 1: Way forward to use various segments of CW
Source: Compiled by the author

Conclusion

CW cannot be viewed only through the prevailing distinct prisms of psychological, information and cyber operations. Future war complexities will require multi-domain approaches, where CW arguably disrupts the other five domains of warfare. Harnessed effectively, it can drive India toward becoming a Vishwa Guru (global leader) on the *Viksit Bharat* (Developed India) pathway. Our philosophy of *Vasudhaiva Kutumbakam* (The world is one family) shall permit our cognitive expertise to safeguard both global interests and national aspirations. India's ethos supports a defensive cognitive shield promoting a free and transparent world order. Adversaries

resistant to global equality require innovative cognitive traps leveraging emerging technologies. The National Cognitive Warfare Strategy will guide a balanced defensive and offensive posture with clear red lines, enabling precise and calculated responses. Through the 'One for All, All for One, India for All' strategy, India seeks to foster a global collective consciousness for worldwide benefit.

Endnotes

1 "The Global State of Digital 2022: Top Takeaways", *Hootsuite, 2022,* accessed 15 Aug 2025, https://www.ttuhsc.edu/communications-marketing/documents/downloads/Hootsuite-Digital-2022.pdf

2 Christoph Deppe and Gary S. Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept", *Frontiers in Big Data* 7 (2024), accessed 15 Aug 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/#B9

3 Paul Thagard, "Cognitive Science", *Stanford Encyclopedia of Philosophy*, substantive revision 31 Jan 2023, accessed 15 Aug 2025, https://plato.stanford.edu/entries/cognitive-science/

4 Robert Frodeman, ed., *The Oxford Handbook of Interdisciplinarity*, 2nd ed. (Oxford: Oxford University Press, 2017).

5 Bernard Claverie, Baptiste Prébot, Norbou Buchler, and François du Cluzel, eds., *Cognitive Warfare: The Future of Cognitive Dominance* (Neuilly-sur-Seine: NATO Collaboration Support Office, Mar 2022), ISBN 978-92-837-2392-9, accessed 16 Aug 2025, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf

6 Yvonne R. Masakowski, "Newport Lecture Series: 'Artificial Intelligence & Cognitive Warfare'", *Naval War College Foundation, YouTube video*, 11 Apr 2022, accessed Aug 2025, https://youtu.be/6Ev8eNR5k4w16

7 Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, "Fall 2020 Cognitive Warfare: An Attack on Truth and Thought" (*Baltimore, MD: NATO Innovation Hub and Johns Hopkins* University, 2020), accessed Aug 2025, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

8 Fabio Ibrahim, Steffen Rhode, and Monika Daseking, “A Systematic Review of Cognitive and Psychological Warfare”, *The Defence Horizon Journal* (Dec 2023), DOI: 10.5281/zenodo.10205600, accessed 17 Aug 2025, https://doi.org/10.5281/zenodo.10205600

9 Tzu-Chieh Hung and Tzu-Wei Hung, “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” *Journal of Global Security Studies* 7, no. 4 (Dec 2022): ogac016, accessed 17 Aug 2025, https://doi.org/10.1093/jogss/ogac016

10 Sandra Pereira, “NATO Study on the ‘Weaponisation of Brain Sciences’ for the Purposes of ‘Cognitive Warfare’”, *European Parliament, Parliamentary Question* E-001093/2022, 16 Mar 2022, accessed 17 Aug 2025, https://www.europarl.europa.eu/doceo/document/E-9-2022-001093_EN.html

11 Rear Admiral John W Tammen, “NATO’s Warfighting Capstone Concept: Anticipating the Changing Character of War”, *NATO Review*, 09 Jul 2021, accessed 17 Aug 2025, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html

12 Ibid.

13 Ibid.

14 Nataliya Bugayova and Kateryna Stepanenko, “A Primer on Russian Cognitive Warfare”, *Institute for the Study of War*, 30 Jun 2025, accessed 17 Aug 2025, https://www.understandingwar.org/backgrounder/primer-russian-cognitive-warfare

15 John Merriam, “One Move Ahead—Diagnosing and Countering Russian Reflexive Control”, *The Journal of Slavic Military Studies* 36, no. 1 (2023): 1–27, DOI: 10.1080/13518046.2023.2201113, accessed 18 Aug 2025, https://doi.org/10.1080/13518046.2023.2201113

16 Andrew S Bowen, *Russian Military Intelligence: Background and Issues for Congress*, Congressional Research Service Report R46616, 24 Nov 2020, accessed 18 Aug 2025, https://www.congress.gov/crs_external_products/R/PDF/R46616/R46616.6.pdf

17 Oliver Backes and Andrew Swab, "Cognitive Warfare—The Russian Threat to Election Integrity in the Baltic States", Policy Analysis Exercise, Belfer Center for Science and International Affairs, Harvard Kennedy School, Nov 2019, accessed 18 Aug 2025, https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

18 Alexis von Sydow, "China's Foreign Election Interference: An Overview of Its Global Impact", *Swedish National China Centre Brief*, no. 4 (2024), accessed 18 Aug 2025, https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/chinas-foreign-election-interference-an-overview-of-its-global-impact.pdf

19 Hanbyeol Sohn and Changwoo Kang, "North Korea's Nuclear-Cognitive Warfare Strategy", *38 North*, 10 Apr 2025, accessed 19 Aug 2025, https://www.38north.org/2025/04/north-koreas-nuclear-cognitive-warfare-strategy/

20 Aviram Bellaishe, "Iran's 'Cognitive War' Is More Dangerous than Missiles and Killer Drones", *Jerusalem Center for Security and Foreign Affairs*, 26 May 2024, accessed 19 Aug 2025, https://jcfa.org/article/irans-cognitive-war-is-more-dangerous-than-missiles-and-killer-drones/

21 Paweł Behrendt, "San Zhong Zhanfa or Three Warfares: Chinese Hybrid Warfare", *Boym Institute*, 19 Apr 2022, accessed 19 Aug 2025, https://instytutboyma.org/en/san-zhong-zhanfa-or-three-warfares-chinese-hybrid-warfare/

22 Pradip R. Sagar, "Weapons of Mass Dissemination: The India-Pakistan Cyber Frontier", *India Today Insight*, 18 May 2025, accessed 19 Aug 2025, https://www.indiatoday.in/india-today-insight/story/weapons-of-mass-dissemination-the-india-pakistan-cyber-frontier-2726677-2025-05-18

23 "Pakistan Ran a Coordinated Anti-India Campaign During Op Sindoor, Forensic Analysis Finds", *The New Indian Express*, 08 Jul 2025, accessed 19 Aug 2025, https://www.newindianexpress.com/nation/2025/Jul/08/pakistan-ran-coordinated-anti-india-campaign-during-op-sindoor-forensic-analysis-finds

24 Sabrina Gabel, Lilian Reichert, and Christian Reuter, "Discussing Conflict in Social Media: The Use of Twitter in the Jammu and Kashmir Conflict", *Media, War & Conflict* 15, no. 4 (Dec 2022): 504–529, DOI: 10.1177/1750635220970997, accessed 19 Aug 2025, https://journals.sagepub.com/doi/pdf/10.1177/1750635220970997

25 Lewis Regenstein, “Havana Syndrome: The History Behind the Mystery”, *Foreign Policy Research Institute*, 01 Apr 2024, accessed 19 Aug 2025, https://www.fpri.org/article/2024/04/havana-syndrome-the-history-behind-the-mystery/

26 Dr. Punit Kumar, “Saam, Daam, Dand, Bheda: The Pillars of Indian Diplomacy from Arthashastra to Modern Times”, *Organiser*, 18 May 2025, accessed 19 Aug 2025, https://organiser.org/2025/05/18/291978/bharat/saam-daam-dand-bheda-the-pillars-of-indian-diplomacy-from-arthashastra-to-modern-times/

27 Col. Denis M. Drew and Dr. Donald M. Snow, *Making Strategy: An Introduction to National Security Processes and Problems* (Maxwell Air Force Base, AL: Air University Press, Aug 1988).

28 IAF Chief Proposes Joint Planning, Coordination Centre in Delhi, *The Hindu*, 27 Aug 2025, accessed 28 Aug 2025, https://www.thehindu.com/news/national/iaf-chief-proposes-joint-planning-coordination-centre-in-delhi/article69980913.ece

29 Committee on External Affairs, “India’s Soft Power and Cultural Diplomacy: Prospects & Limitations”, Sixteenth Report, Seventeenth Lok Sabha (New Delhi: Lok Sabha Secretariat, Dec 2022), accessed 20 Aug 2025, https://elibrary.sansad.in/server/api/core/bitstreams/b1effdb6-685d-4436-a5d5-f9fe331ad30f/view

30 Torvald F Ask, Ricardo G Lugo, Stefan Sütterlin, Matthew Canham, Daniel Hermansen, and Benjamin J Knox, “The UnCODE System: A Neurocentric Systems Approach for Classifying the Goals and Methods of Cognitive Warfare”, paper presented at the HFM-361 Symposium on *Mitigating and Responding to Cognitive Warfare*, Madrid, Spain, Nov 2023, accessed 20 Aug 2025, https://hal.science/hal-04945655/document

31 Protium, “Key Challenges for MSMEs: Compliance, Technology, and Skilling Gaps”, 20 Jun 2025, accessed 20 Aug 2025, https://protium.co.in/key-challenges-for-msmes-compliance-technology-and-skilling-gaps/

32 “The Bharatiya Nyaya Sanhita, 2023”, Act No. 45 of 2023 (New Delhi: Government of India, 2023), accessed 20 Aug 2025, https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita,_2023.pdf

33 Regina E Dugan and Kaigham J Gabriel, “Special Forces” Innovation: How DARPA Attacks Problems,” *Harvard Business Review* 91, no. 10 (Oct

2013): 74–84, accessed 20 Aug 2025, https://hbr.org/2013/10/special-forces-innovation-how-darpa-attacks-problems