MANOHAR PARRIKAR idsa
MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Cognitive Warfare: Key Aspects

Sukhbir Kaur Minhas

August 18, 2025

Summary

Though the concept of Cognitive Warfare (CW) has historical roots in the practice of Psychological Operations/Warfare (PsyOps) and later Information Warfare (IW), scientific advances of the digital age and Artificial Intelligence (AI) have enabled its transition to an evolved form. Proponents of the cognitive domain argue that it fills 'a critical gap' by addressing the human element that shapes the battlefield. Democratic nations must navigate the CW domain carefully while balancing its offensive elements with transparency, accountability and individual freedoms.

"Preceded by mind are phenomena,

Led by mind, formed by mind.

If with a mind polluted, one speaks or acts,

Then pain follows,

As a wheel follows the draft ox's foot."

Gautama Buddha, *Dhammapada*[1]

Introduction

The first verse of the *Dhammapada* (teachings of the Buddha), dating back to the third century BCE, discusses the need to understand the human capacity for experience, referred to as 'the mind', as part of a discourse on internal conflict and the search for life's meaning. Over 2000 years later, when applied to modern warfare, the core message remains the same, highlighting that intrapersonal or conflicts between states ultimately revolve around the human mind.

Geopolitical conflicts and recent wars have seen increased indicators of a new warfare domain in which the "human brain is positioned as a key battleground".[2] Narrative building, information and strategic messaging leading up to conventional conflict between Israel and Iran—Operations *Rising Lion* and *Midnight Hammer*—amplify these aspects. Both operations were characterised by a covert, subtle and nuanced interplay of kinetic and non-kinetic means, targeting not just adversarial military infrastructure and leadership but select sections of populations and the 'world view'. The purported use of social media tools such as 'TikTok' by China and Russia to shape public opinion of specific audiences in Taiwan and Ukraine, respectively, highlights digital platforms' impact on exploiting psychological vulnerabilities and societal fault lines to meet strategic ends.[3]

Referred to as Cognitive Warfare (CW), this form of battle aims to influence an adversary's cognitive functions, from "peacetime public opinion to wartime decision-making".[4] Though the concept is rooted in historical warfare in the practice of Psychological Operations/Warfare (PsyOps) and later Information Warfare (IW),

[1] Glenn Wallis, **"*The Dhammapada: Verses on the Way*"**, Random House Publishing Group, 2007.

[2] Arijana Marjanović and Drazen Smiljanic, **"Cognitive Warfare - The Human Mind As The New Battlefield"**, Proceedings of the Defence and Security Conference, April 2025.

[3] Yenting Lin, **"Digital Propaganda: How China Uses Short-Form Videos to Target Taiwan's Youth"**, *Small Wars Journal*, 6 July 2025; Patrick Tucker, **"How China Used Tiktok, AI, And Big Data to Target Taiwan's Elections"**, *Defense One*, 8 April 2024; Valerie Wirtschafter, **"Tracing the Rise of Russian State Media on Tiktok"**, Brookings, 2 May 2024.

[4] Beauchamp-Mustafaga, **"Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations"**, RAND Corporation, 14 May 2021.

scientific advances of the digital age and Artificial Intelligence (AI) have enabled its transition to an evolved form, as opposed to its preceding interpretations.

Research also suggests exploitation of CW during peacetime through a planned, systematic whole-of-government approach, citing examples such as Russia's influence on US presidential elections and the United Kingdom's Brexit vote, and China's interference in Australia and New Zealand, and the discrediting of Taiwan's COVID-19 management.[5] The doctrinal evolution of militaries has also mirrored the recognition of this concept. Spain and Poland formally include it as the sixth domain in their Multi-Domain Operations (MDO) concept, and the North Atlantic Treaty Organization (NATO) recognised it in 2023.

Given its impact on modern warfare, the global strategic community must enable dialogue, deliberation and discussion for scholarly guidance of respective policy-makers and militaries. This brief analyses the concept's genesis and historical evolution and the Russian and Chinese use of CW. It then sketches likely scenarios under which CW could be used to undermine democracies with fictional examples and ends with some recommendations to counter such efforts.

Historical Context

Concepts of deception, propaganda, IW and PsyOps are as old as warfare itself. Texts such as Kautilya's *Arthashastra* and *Panchatantra* from India and Sun Tzu's *The Art of War* from China, highlight deceit, perception management and information control to one's advantage.[6] Carl von Clausewitz's seminal 19th-century work on theories of war carries the same flavour (of the inseparability of the human element in warfare). It is used extensively today as a framework to understand aspects of modern-day CW, such as in the Russia–Ukraine conflict.[7]

A careful reading reveals that human cognition and 'mind training' were central to the teaching of War and Statecraft in ancient times and were viewed as the overarching domain through which kinetic operations were conducted. In the military lexicon, the concept of CW evolved from the terms 'Psychological Warfare', 'Information Warfare' and 'Cyber Warfare'. Their understanding and usage have evolved linearly with advances in technology and modes of media.

[5] 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*, Vol. 7, No. 4, 2022.

[6] Patrick Olivelle, **"*Pañcatantra-The Book of India's Folk Wisdom*"**, Oxford World Classics, 1997.

[7] Amber Brittain-Hale, **"Clausewitzian Theory of War in the Age of Cognitive Warfare"**, *The Defence Horizon Journal*, 14 December 2023.

In its modern form, the first of these concepts borrows from the art of propaganda, which flourished during World War I. Governments on both sides used developments in print technology to influence audiences through posters, postcards and trade cards.[8] British military historian J.F.C. Fuller's analysis of the war in 1920 led to the formal coining of the term 'Psychological Warfare'. Fuller's predictions for future wars included a replacement of the kinetic dimension by this form of 'brain warfare', launched against an adversary's leadership, resulting in demoralising enemies without direct combat.[9]

This form of warfare was enhanced during World War II and later during the Cold War years, as radio broadcasts, films, cinema, and even chess (as a symbol of ideological superiority)[10] were used by opposing powers to rally populations, affect morale and influence international opinion.[11] IW caught the media's attention when the Gulf War was shown on television screens. Some labelled it the 'first information war'.[12] Enabled by the internet, it is today understood as the 'war of information',[13] controlled to shape perceptions, confuse adversaries and dominate the narrative.

Post-Gulf War, IW was back in focus in Kosovo, with the spotlight on the internet (as broadcast media was perceived as biased), causing it to be named 'the first internet war'.[14] Enhanced cyber capabilities during the decade brought in a covert dimension. As IW matured, it came of age through attacks on Iran's Natanz nuclear facility by 'zero-day' bugs of the Stuxnet worm,[15] cyberattacks on Estonia's financial and other computer services in 2008, '*Shamoon*' malware attacks on Saudi Aramco in 2012[16], and the 2015–16 power outage attacks on Ukraine.[17]

Its military parlance triggered by the developments of the 1990s came to be understood as 'Information Operations and Warfare', through capabilities of "computer network operations, electronic warfare, operational security,

[8] Allison Rudnick, "**Humor and Horror: Printed Propaganda during World War I**", 28 December 2017.

[9] Sunil Narula, "**Psychological Operations (PSYOPs): A Conceptual Overview**", *Strategic Analysis*, Vol. 28, No. 1, 2004, pp. 177–192.

[10] "**Chess as a Tool of Propaganda During the Cold War**", *Chess.com*, 15 August 2024.

[11] Maureen Grzan, Rachel Lee, Kevin Pham and Tasha Mamoody, "**Film as Propaganda in America during WWII**"; Sarah Lee, "**Cold War Propaganda: A Historical Analysis**", *Number Analytics*, 24 May 2025.

[12] Maj Karl Kuschner, "**Legal and Practical Constraints on Information Warfare**", Naval War College Newport, RI, 14 June 1996.

[13] Emily Bienvenue, Sian Troath and Zac Rogers, "**Cognitive Warfare Is The Fight We've Got And We Must Reorient Ate To Meet This Challenge**", *The Cove*, 20 September 2018.

[14] Philip Hammond, "**Lessons of the Kosovo Information War**", FUTURE NON STOP, Living Archive for Digital Culture in Theory and Practice, 13 July 2000.

[15] Josh Fruhlinger, "**Stuxnet Explained: The First Known Cyberweapon**", CSO, 31 August 2022.

[16] "**Compromise of Saudi Aramco and RasGas**", Council on Foreign Relations, August 2012.

[17] Julia E Sullivan and Dmitriy Kamensky, "**How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid**", *The Electricity Journal*, Vol. 30, No. 3, 2017, pp. 30–35.

psychological operations, and deception".[18] The aim was to enhance the gathering of tactical information and propaganda dissemination.[19] Today, Austria, France and Switzerland officially recognise the Information domain as a formal domain and the sixth domain in their concept of MDO.[20] As cyberspace transformed from a 'force multiplier' to an 'enabler of operations' in other domains, some nations have also treated it as an independent domain.[21] NATO recognised cyberspace in 2016 as such. Most military literature considers cyber warfare an integral part of the larger 'Information ops' undertaken as an augmentation of the kinetic means employed in its warfare paradigm.[22]

Cognitive Warfare: A New Terminology

The term 'cognitive domain' was initially introduced by the US Department of Defense in its 2001 congressional report on 'Network Centric Warfare' (along with the physical and information domains), which, through its later iterations in US military lexicon, sought to employ psychological operations and deception to 'influence and mislead adversaries'.[23]

The concept's prevalence today (starting around 2017) results from a self-reinforcing loop as researchers in the US/Western nations and China/Russia sought to invest in its strategic value to match each other's progress. That it is an evolutionary successor of IW can be deduced from developments in concepts, technology and 'actors'. The explosive proliferation of social media over the early 21st century enabled non-state actors to join the battle of the narratives and minds, adding weight to concepts of hybrid and asymmetric warfare. Meanwhile, advancements in cognitive psychology, 'neurowarfare', AI and 'metaverse' allowed militaries to invest in research on strategies to exploit and counter cognitive domain operations.

Its definition encompasses the nuanced use of 'neuroscience, behavioural science, and digital technologies', targeting influence and disruption of human cognition.[24]

[18] Philip M. Taylor, "**Mind Games: A Brief History of Information Warfare**", *Tablet*, 7 October 2010.

[19] Jiayue Li, Yonghong Dai, Tewodros Woldearegay and Soumyodeep Deb, "**Cognitive Warfare and the Logic of Power: Reinterpreting Offensive Realism in Russia's Strategic Information Operations**", *Defence Studies*, 2025, pp. 1–22.

[20] "**Multi-Domain Multinational Understanding**", Multinational Capability Development Campaign (MCDC), November 2022.

[21] Paul J. MacKenzie, "**Cyberspace and Multi-Domain Operations**", Joint Air Power Competence Centre, June 2019

[22] Daniel T. Kuehl, "**Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age**", U.S. Naval War College, 2002.

[23] Beauchamp-Mustafaga, "**Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations**", RAND Corporation, 14 May 2021.

[24] Christoph Deppe and Gary S. Schaal, "**Cognitive Warfare: A Conceptual Analysis of The NATO ACT Cognitive Warfare Exploratory Concept**", *Front. Big Data*, 2024.

Its application combines aspects of modern PsyOps, IW, political warfare, "Hearts and Minds" and propaganda through sophisticated strategies, indicating coordinated political, military, economic and information efforts.[25]

Citing its real-world use (such as interference in democratic political processes and public opinion), researchers argue that its relevance and span in shaping the global security environment are increasing. Adversaries now seek to apply this strategy from peace through war—a single *continuous* effort to disrupt and deny the cognitive conditions in which whole societies are situated.[26] Current scholarly work on the concept as a warfare strategy is mostly by analysts from the US and Western nations, who study the Russian and Chinese concepts to develop counter-strategies. The succeeding paragraphs give a concise summary of the same.

China and Cognitive Warfare

China's emphasis on 'Cognitive Domain Operations' (CDO) is aligned with its historical strategy of using human psychology and deception in warfare, also referred to as the 'war of attacking the heart' and Sun Tzu's insights, such as "All warfare is based on deception".[27] In response to the US's perceived use of this domain during the Arab Spring, China started developing its current CDO concept by researching ideas such as 'National Cognitive Security' (2013) and 'Mind Superiority' (2014).[28]

Hinting at its application in Taiwan (2018 election and as a long-term strategy), analysts highlight the PLA's goal of 'mind superiority' as the next phase in the evolution of the traditional concept of the three superiorities (sea superiority, air superiority and information superiority).[29] As assessed by the US DoD, the PLA has invested in 'neurocognitive warfare' capabilities under the PRC's China Brain Project (2016–2030) and employs the concept as an extension of its earlier three warfare strategy (psychological warfare, public opinion warfare and legal warfare).[30]

The CDO framework has been assessed by researchers under six technologies and two categories of Cognitive Influence (Survey, Interference and Strengthening) and

[25] Fabio Ibrahim, Steffen Rhode and Monika Daseking, "**A Systematic Review of Cognitive and Psychological Warfare**", *The Defence Horizon Journal*, 1_December 2023.

[26] Emily Bienvenue, Sian Troath and Zac Rogers, "**Cognitive Warfare is the Fight We've Got and We Must Reorient Ate to Meet This Challenge**", *The Cove*, 20 September 2018.

[27] Josh Baughman, "**How China Wins the Cognitive Domain**", China Aerospace Studies Institute, 23 January 2023; Fabio Ibrahim, Steffen Rhode and Monika Daseking, "**A Systematic Review of Cognitive and Psychological Warfare**", 1_December 2023.

[28] Beauchamp-Mustafaga, "**Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations**", RAND Corporation, 14 May 2021.

[29] Ibid.

[30] "**Military and Security Developments Involving The People's Republic of China 2024 Annual Report to Congress**", U.S. Department of Defense, 18 December 2024.

Subliminal Cognitive Influence (processing, implantation and detection). It is suggested that CDO uses applications from neuroscience and psychology apart from leveraging emerging and future technologies of social media, brain-computer interfaces (to optimise decision-making), and AI to manipulate target perception and behaviour to advance battles into "the realm of the human mind".[31]

While real-world applications remain to be analysed thoroughly, it has been postulated that China effectively demonstrated CDO in action during former US Speaker Nancy Pelosi's visit to Taiwan in August 2022 by integrating its disinformation campaign with cyber-attacks.[32] News reports also indicate possible research in the development of 'neuro-strike weapons' to target adversary leadership.[33]

Russia and Cognitive Warfare

Like China, Western theorists ascribe the Russian approach to CW to its historical emphasis on achieving advantages through information and deception as tools of statecraft. The 2008 Russo-Georgian crisis, followed by the Crimea crisis and the ongoing conflict with Ukraine, are quoted as examples to justify this assessment. It is also proposed that through this strategy, Russia serves as a role model for China, Iran and North Korea.[34]

Originally proposed as an alternative to game theory in the 1960s by Soviet scholar Vladimir Lefebvre, Reflexive Control (RC) aims to influence a target's decision-making process through disguised manipulation, providing them with specific information inclined towards a desired outcome (unlike the traditional military doctrines employing force). The role of the Wagner Group in the Crimea crisis, support to former Syrian leader Bashar al-Assad, and its participation during Ukraine operations are seen as examples of RC in action, allowing Russia "the benefit of plausible deniability", and "strategic ambiguity", making attribution of responsibility significantly more difficult.[35]

The notion of 'Mental Warfare' has been introduced in recent discourse. This concept is trending in discussions within Russia and combines earlier concepts of

[31] Andrew MacDonald and Ryan Ratcliffe, **"Cognitive Warfare: Maneuvering in the Human Dimension"**, U.S. Naval Institute, April 2023.

[32] Josh Rogin, **"Taiwan is on the Frontlines of China's Worldwide Cyberwar"**, *The Washington Post*, 8 November 2022.

[33] Bill Gertz, **"China Crafts Weapons to Alter Brain Function; Report Says Tech Meant to Influence Government Leaders"**, *The Washington Times*, 6 July 2023.

[34] Nataliya Bugayova and Kateryna Stepanenko, **"A Primer on Russian Cognitive Warfare"**, Institute for the Study of War (ISW), 30 June 2025.

[35] Miranda Mchedlishvili, **"Beyond the Battlefield: How Russia's Private Military Companies Reinvent Reflexive Control"**, STEAR, 4 June 2025.

information-psychological warfare, reflexive control and strategic deception.[36] This form of warfare targets the opposing side's mentality, identity, historical traditions and values. Interestingly, Russian literature considers this form of warfare a ‘civilisational war’, employed by the West against itself and other unaligned countries.

Experts also point out that Russia, in turn, mirrors this tactic in employment against the West, to exploit the gaps in rival nations and bring favourable political forces to power instead of seizing territory.[37] This approach bears stark similarity to China’s four tactics approach to CDO as suggested by Chinese analyst Zeng Huafeng of the National University of Defense Technology (NUDT) in 2017, namely, ‘perception manipulation, cutting off historical memory, changing the paradigm of thinking, and deconstructing symbols’.[38]

Information Warfare and Cognitive Warfare: Bridging the Gap

Against this backdrop, many Western military analysts claim that CW is now viewed as a domain, alongside the other five traditional domains.[39] Analysts associated with the Australian Department of Defence[40] point out that, through the years of the ‘war on terror’, adversaries of US/Western nations have successfully recognised and bridged the growing disconnect between military victory and non-enduring political success. These states have since transformed IW from its military/intelligence-led episodic effort supporting kinetic operations to a continuous, single and whole-of-government effort.

Similarly, US policy analysts point out that besides interfering in electoral results (US, Moldova, Brexit vote), Russia has consistently exploited this strategy in the Baltic states through traditional and social media, with “narratives designed to divide ethnic Russians and Russian-speakers from the rest of the society”, to influence political outcomes and influence their linkages to the EU and NATO.[41] The result is

[36] Mari Puurunen, **“From Information to Cognition: Mental Warfare from the Russian Perspective”**, Jyväskylän Yliopisto, 2025.

[37] Jānis Bērziņš, **“The Cognitive Battlefeld: Exploring the Western and Russian Views”**, Centre for Security and Strategic Research, National Defence Academy of Latvia, 2023.

[38] Beauchamp-Mustafaga, **“Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations”**, RAND Corporation, 14 May 2021.

[39] Bernard Claverie and François du Cluzel, **“The Cognitive Warfare Concept”**, NATO Innovation Hub, 2022.

[40] Emily Bienvenue, Sian Troath and Zac Rogers, **“Cognitive Warfare is the Fight We've Got and We Must Reorient Ate to Meet This Challenge”**, *The Cove*, 20 September 2018.

[41] Oliver Backes and Andrew Swab, **“Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States”**, Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019.

to achieve long-term shifts in the target population's thinking through covert and subtle data-driven manipulation.

Commentators such as Albert Palazzo point out that the end state of strategic success has been lost in Western militaries' current predilection for lethal kinetic action over asymmetric means. He sees MDO in its current form as limited to an 'instrument of combat' without addressing 'the strategic level of war'.[42] While maintaining the significance of cognitive warfare, researchers argue that since MDO is a model-based concept employed at the operational level, integrating abstract human aspects and their effects under a separate domain may not be pragmatically feasible for operational planners. For example, the effects of deception/narrative of collateral damage in an air campaign are better understood in that domain rather than clubbing in a separate domain.[43]

The question that spurred the development of the MDO concept was, 'What after joint?'.[44] Cohesive strategies applied synergistically across two or more domains, was seen as essential by the American Military Forces. MDO sought to effect simultaneous interaction, rather than sequential (as was the case till the Gulf War), to exploit the enemy's vulnerabilities and create the desired outcomes. For example, the temporary disabling of an adversary's surface-to-air weapons through a cyber-attack would enable successful air raids.[45] Another aspect of MDO worth noting is that it does not necessarily require the interaction of all domains all the time, implying its activity-based characteristic. From this view, proponents of the cognitive domain argue that it fills 'a critical gap' by addressing the human element that shapes the battlefield.[46] It is proposed that recognising cognitive warfare as an overarching domain may inform warfighting at a strategic level rather than as an enabler to the kinetic form—a shift that Western military theorists strongly recommend.

Cognitive Warfare and Democracies: Scenarios

What does a CW strategy with kinetic means look like when applied to a democracy? Borrowing a leaf from Zeng Huafeng's four-tactic approach and the 'Scenario

[42] Albert Palazzo, "**Multi-Domain Battle: Getting the Name Right**", *Small Wars Journal*, 14 October 2017.

[43] Patrick Hofstetter and Flurin Jossen, "**There Is No Need For A Cognitive Domain**", *The Defence Horizon Journal*, 2 November 2023.

[44] Jeffrey M. Reilly, "**Multidomain Operations: A Subtle but Significant Transition in Military Thought**", *Air & Space Power Journal*, 2016.

[45] Jean-Christophe Noël, "**The American Origins of the Multi-Domain Concept**", Institute for Strategic Research at the Military School, June 2021.

[46] Scottie Moore, "**A Case for the Cognitive Domain in U.S. Multi-Domain Operations**", *LinkedIn*, 20 November 2024.

Method',[47] a fictional case of a decade-long (2025–2035) CW campaign by Nation 'A' against an adversarial Nation 'B' (which is a democracy) is sketched below:

'Perception Manipulation'

Starting in 2025, based on data collected through 'Cognitive Survey Technologies' (such as social media and marketing apps), Nation A gradually feeds state-backed narratives using AI tech on Nation B's social media, amongst other outlets. Embedded in routine messages, the targeted content portrays the government, security apparatus, election process and press freedom of Nation B as ineffective, corrupt, racist and biased, seeking to sow divisions in its multi-ethnic population. AI-driven bots amplify disinformation, portraying Nation A as a global visionary power that Nation B could do well to emulate. By 2030, falling prey to tailored and disguised PsyOps, public trust in Nation B erodes, with questions raised on electoral integrity, security, justice and media agencies.

'Cutting off Historical Memory'

By 2028, Nation A sponsors cultural (including cinema), sports and academic exchange programmes with Nation B to subtly undermine Nation B's sense of history and pride in culture. Content funded by Nation A (such as journals, books, movies, documentaries) downplays its democratic milestones, while highlighting a growing polarity in its social fabric and economic regress, emphasising the failures of its government's functioning. Online campaigns and polls question the moral standing of historical figures, national heroes and freedom fighters, aiming to dent Nation B's belief in its heritage. By 2033, surveys indicate about 30 per cent of youth questioning their foundations and growth *vis-à-vis* other nations.

'Changing Thinking Paradigms'

Nation A targets Nation B's academia, policymakers, opposition leaders, influencers and journalists through think tank partnerships, international seminars and cultural institutes. By 2030, these elites advocate even more open governance models, citing current systems' lack of transparency and inefficiency. Public discourse shifts, with a section of elites reinforcing feelings of growing unrest, weakening democratic resolve.

'Deconstructing Symbols'

From 2027, Nation A launches sporadic cyberattacks, spreading memes, mocking languages and defacing key symbols of its multi-ethnic population. It also targets

[47] Andrew MacDonald and Ryan Ratcliffe, **"Cognitive Warfare: Maneuvering in the Human Dimension"**, U.S. Naval Institute, April 2023.

Nation B's national flag and anthem. By 2032, national symbols lose resonance, with a section of citizens reporting a decline in patriotic sentiments.

Kinetic Coordination

In 2034, coinciding with heightened cognitive operations, Nation A escalates grey zone tactics of mercenary incursions on the boundary, coastline and airspace, along with suspected use of military grade laser technology, rumours of 'neuro-weapons' in use against soldiers and military leadership, and cyber-attacks on critical civilian infrastructure. Amidst heightened tensions, a military exercise by Nation A on Nation B's border is used as a trigger event, leading to subsequent escalation to kinetic action. With a raging CW spread to international and domestic media, international pressure forces Nation B's leadership to negotiate under duress.

Countering Cognitive Warfare

The above scenarios (generated partly with an AI tool's assistance) indicate that though CW can be tailored for adversaries of all kinds, its potential damage is larger for democratic nations with relatively open access to information systems, technology platforms and viewpoints. Accessing data on perceptions, attitudes and behaviours of target population groups through seemingly harmless digital applications over social media and 'weaponising' the same through tailored content embedded in regular messaging over time is a possibility. Subsequently, introducing confusion and chaos during contingency situations becomes plausible, undermining populations' confidence in their own governance and security apparatus. Hence, democratic nations must invest in a better understanding of Cognitive Warfare.[48] A suggested approach is explained below:

Approach to Cognitive Warfare

Democratic nations must navigate the CW domain carefully while balancing its offensive element with transparency, accountability and individual freedom. If aligned with indigenous strategic thought and values, investment in this domain will likely be more effective. Hence, a focus on defence (countering adversarial campaigns), offence (strategic communication, shaping narratives aligned to own values), and resilience (building larger immunity to manipulation)[49] is recommended.[50]

[48] Michael Miklaucic, "**Seizing the Edge in Cognitive Warfare**", Center for the Study of Democracy, 3 July 2025.

[49] "**Taiwan Provides Insights for Democracies to Counter Cognitive Warfare**", Indo-Pacific Defense Forum, 2 June 2024.

[50] Stefan Holitschke, "**Cognitive Warfare and Democracy: A Critical Analysis of the Ethical Challenges and Solutions**", *LinkedIn*, 9 March 2024.

Identifying Vulnerabilities

Enhancing joint academic and military discourse on the subject is necessary for democracies to develop effective counter-measures through an all-inclusive approach. The strategic community of a democracy—including its academia, policymakers, influencers and the military—can enable the same. Contextualising citizens' cognitive biases, decision-making and social influence is necessary to predict and counter manipulation tactics. The same can be achieved by funding projects in Behavioural Science and Psychology. Similar projects in Neuroscience and Human-Machine Interfaces to explore the interface of cognitive processes and technology (brain-computer interfaces/ immersive VR propaganda) will help and anticipate future threats. Leveraging AI tools to analyse disinformation campaigns, deep fakes, etc., on domestic social media platforms also helps establish existing and emerging propaganda trends.[51]

Strengthening Existing Frameworks

Besides strengthening cybersecurity, social media monitoring tools and content authentication solutions provide technological grounding for preventing and mitigating CW attacks. Existing security agencies specialising in cyber warfare and strategic communication can also collaborate with domestic tech companies and friendly nations to share best practices and lessons learnt.[52]

Value of Indigenous Thinking/Literature

Returning to the roots and owning indigenous strategic thought is an effective way for democracies to integrate populations and instill a sense of historical pride. When nations own their indigenous strategic culture and literature, they are less likely to be swayed by attempts at manipulation from adversaries. Funding nationwide formal education programmes to infuse this thought and build psychological resilience from a young age until the policy-making level is an effort that must be continuous and long-term.

Ethical and Legal Considerations

Establishing oversight agencies and adhering to data protection laws is necessary for democracies to mitigate the chances of these investments in CW undermining their transparency. Simulation and war gaming that involve all agencies to test national responses will enhance contingency reactions and build trust in government-civil society.[53]

[51] **"Countering Cognitive Warfare: Awareness and Resilience"**, Johns Hopkins University and Imperial College London, 20 May 2021.

[52] Robin Burda, **"Cognitive Warfare as Part of Society Never-Ending Battle for Minds"**, The Hague Centre for Strategic Studies, 6 June 2023.

[53] Jiayue Li, Yonghong Dai, Tewodros Woldearegay and Soumyodeep Deb, **"Cognitive Warfare and the Logic of Power: Reinterpreting Offensive Realism in Russia's Strategic Information Operations"**, *Defence Studies*, 2025, pp. 1–22.

About the Author

Group Captain Sukhbir Kaur Minhas is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses