# CHINESE COGNITIVE WARFARE: EXPLORING A FRAMEWORK AND IDENTIFYING CONTOURS

**ABHISHEK KUMAR**

## INTRODUCTION

The apparently synonymous terms cognitive warfare, psychological warfare, information warfare and influence operations, not only add to the security jargon but also to the complexity of warfare in the cognitive domain. Contemporary Chinese exploitation of the cognitive domain is aimed at creating a pro-China perception and reducing threats to the survival of the Chinese Communist Party (CCP). China has made global inroads in countries, including Taiwan, Australia, US and India, in influencing the cognitive domain. This article uses exploratory qualitative research in, firstly, attempting to create a framework for the term Cognitive Warfare (CW) and thereafter identifying the contours of Chinese CW. Having identified the contours of Chinese CW, the article endeavours to frame a possible Chinese strategy for CW, in an ends-ways-means construct.

Contemporary usage of offensive influence operations for external interference in elections and sovereign functioning of

Colonel **Abhishek Kumar**, SM earned his Master's Degree from US Army's Command and General Staff College, Fort Leavenworth. He has written previously on ancient Indian strategy and contemporary warfare.

democratic countries has brought operations aimed at influencing human cognition into sharp focus. China leverages an internet firewall to shield its domestic society from external influences, while concurrently influencing societies outside China, in pursuit of Chinese national interests. China's 'sharp power' in contrast to the 'soft power', penetrates the socio-political and information environment of such targeted countries.[1]

In such an environment, the concept of CW and the contours of Chinese CW, acquire salience. As per scholars, CW leverages "cyber tools" to exploit "mental biases or reflexive thinking", in order to change the adversary's "cognitive processes" and influence individual as well as collective thoughts and decisions.[2] Other works on warfare in the cognitive domain, use a bouquet of terms such as CW, Psychological Warfare (PsyW), Political Warfare (PW), Influence Operations (IO), Information Environment (IE), propaganda and Information Warfare (IW), among others.

Global reports, testimonies, and studies have attempted to identify the scale of Chinese influence operations in multiple countries. One such study carried out in 30 democratic countries in 2022, regarding China's global media influence, indicated that 16 countries had a high or very high level of the CCP's influence on their media.[3] Furthermore, propaganda and espionage by Chinese Confucius Institutes have led to security concerns in multiple countries, including India and the US.[4]

This article endeavours to add to the existing body of research on the subject through an exploratory mode of qualitative research. In

1. Juan Pablo Cardenal, et al., "Sharp Power: Rising Authoritarian Influence: New Forum Report"', National Endowment for Democracy, December 5, 2017, p. 6, https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/. Accessed on May 10, 2024.
2. Bernard Claverie and François du Cluzel, ''The Cognitive Warfare Concept'', NATO Innovation Hub, p. 2, https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf. Accessed on May 1, 2024.
3. Sarah Cook, et. al., ''Beijing's Global Media Influence'', Freedom House, September 2022, p.3, https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience. Accessed on March 11, 2024.
4. ''Hearing: China's Global Influence and Interference Activities'' German Marshall Funds of the United States, March 23, 2023, pp. 298-99, https://www.uscc.gov/hearings/chinas-global-influence-and-interference-activities. Accessed on December 14, 2023.

the first part, it shall endeavour to propose a conceptual framework for CW. In the second part, the article shall try to discern the contours of Chinese CW, by identifying the *raison d'etre*, aims, goals, categories, architecture and trends of Chinese CW. In identifying the contours of Chinese CW, the article shall also attempt to frame a possible Chinese strategy for CW in an ends-ways-means framework.

## CONCEPTUAL FRAMEWORK OF CW

To arrive at an illustrative framework for better understanding the concept of CW, navigating through the terms of information, propaganda, IE, PsyW, PW, IW and IO, is the first research stepping stone. Clarity on similar Chinese terms in Chinese concepts in the Chinese doctrine, is also vital in arriving at the author's conceptual illustration of CW.

### *Information, Human Behaviour, Propaganda and the Information Environment*

The term information and the use or misuse of information by human beings is one of the foundational concepts in relation to CW. Human beings utilise information for decision-making, communication and assimilation. On the receipt of information, human behaviour is typically driven by attitudes, cognition, emotions, culture, desire, language, memory, narrative and perception. In this context, the term narrative implies a method of presenting information in a manner that supports a particular viewpoint, while the term cognition refers to the cycle of receiving, storing, understanding, retrieving and processing information.[5] Manipulation of human behavioural response, on receipt of information, is connected to the concepts of propaganda and disinformation.

To manipulate human behaviour, propaganda and the sub-concept of disinformation play a key role, often leveraging the rapid spread of biased or inaccurate information. Jowett defines propaganda as the communication of information in a systematic effort aimed at

5. ''JP 3-04, Information in Joint Operations'', US Department of Defence, September 2022, pp. I-5 - I-6, https://pavilion.dinfos.edu/Policy-Doctrine/Article/3232089/jp-3-04/https%3A%2F%2Fpavilion.dinfos.edu%2FPolicy-Doctrine%2FArticle%2F3232089%2Fjp-3-04%2F. Accessed on April 14, 2024.

conditioning, manipulating, shaping and directing human behaviour as well as perceptions.[6] Disinformation, on the other hand, is the use of black propaganda i.e., misleading and false information.[7] From a security perspective, the interplay between various stakeholders and information, can be framed in an environment within which the interplay acts out.

IE is akin to an all-encompassing sheath that covers various operational domains, for military warfare as well as operations. The US Department of Defence (DoD) defines IE as the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information consisting of physical, informational, and cognitive dimensions".[8]

***Operational Domains, IW, IO, PW, PsyW and CW***

Domains for warfare include both physical demarcations such as land, sea or air as well as abstract ones such as cyber space. The British Joint Military Doctrine identifies five operational domains. These are (1) land; (2) maritime; (3) air; (4) space; and (5) cyber and electro-magnetic.[9] Cyber space refers to the "capabilities and activities primarily related to operating within the interdependent networks of information, technology infrastructures and resident data, including the internet, telecommunications, networks, computer systems and embedded processors."[10] The human mind or the cognitive domain is arguably a connecting realm, which links these five domains and within which PW, PsyW and IW play out.

IW, IO, PW and PsyW are terms, which are found frequently used in literature on warfare involving the human mind. The concept of a cognitive domain includes the human minds of the collective

6. Garth Jowett, *Propaganda & Persuasion* (California: Sage Publications, 2012), pp. 1-7, http://archive.org/details/propagandapersua0000jowe_m3v7. Accessed on February 10, 2024.
7. Ibid., pp. 23-24.
8. n. 5 , p. II–1.
9. Ministry of Defence, United Kingdom, ''Joint Concept Note 1/20, Multi-Domain Integration'', November 2020, pp. 17–18, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950789/20201112-JCN_1_20_MDI.PDF. Accessed on January 29, 2024.
10. Ministry of Defence, United Kingdom, "Allied Joint Publication-01 Allied Joint Doctrine", December 2022, p. 154, https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine. Accessed on March 29, 2024.

population as well as the individuals involved in a conflict.[11] IW can be identified as a type of PW, short of armed conflict, both protecting and exploiting IE, "where targets include a nation state's government, military, private sector, and general population."[12] IW exploits information for gaining advantage, through both offensive and defensive operations against adversaries, within an IE, for forcing decisions and building public opinion.[13]

Cyber space serves as a "force multiplier for IW activities", wherein "cyber space operations", such as "offensive cyber attack" can be leveraged for "strategic information warfare goals" such as "psychological effects in a target population" which alter human behaviour and influences decision-makers.[14]

IW is executed at the strategic level, while IO implements the IW strategy at the operational level.[15] RAND defines IO as a "coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviours or decisions by foreign target audiences" to further national interests.[16]

PW is perhaps best defined by Cold War diplomat George Keenan as:

> Employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign

11. Arthur L. Money, "Report on Network-Centric Warfare", March 2001, p. 7, http://www.dodccrp.org/files/ncw_report/report/ncw_sense.pdf. Accessed on February 10, 2024.
12. Catherine A. Theohary, "Information Warfare: Issues for Congress", US Congressional Research Service, March 5, 2018), p. 1, R45142, https://crsreports.congress.gov/product/details?prodcode=R45142. Accessed on April 16, 2024.
13. n. 5 , p. II.
14. Theohary, n. 12, p. 6.
15. Ibid., p. 2.
16. Eric V. Larson, et. al., "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities", RAND Corporation, May 27, 2009, p. xii, https://www.rand.org/pubs/monographs/MG654.html. Accessed on January 10, 2024.

> elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states.[17]

PsyW is the state use of *propaganda* and associated "informational measures", to influence the "opinions, emotions, attitudes and behaviour of enemy, neutral or friendly foreign groups to achieve national aims".[18] CW "sits at the intersection of psychological operations, cyber operations and influence operations".[19]

In terms of linkages among information, IW and CW, scholars argue that while IW "seeks to control pure information in all forms", CW "seeks to control how individuals and populations react to presented information".[20] CW, in a worst-case scenario, may be potentially employed in fracturing societies, by degrading the "collective will to resist an adversary's intentions" thereby, removing the need for application of "force or coercion" against the society.[21]

Plausibly, CW as a concept, harmoniously aligns with Sun Tzu's age-old stratagem of winning over "the enemy's army without fighting".[22] In fact, China's Three Warfares Strategy which comprises "public opinion warfare, psychological warfare, and legal warfare", endeavours to achieve victory without fighting.[23] So, how do the Chinese perceive CW?

17. George F. Kennan, "Document 269, FRUS, Emergence of the Intelligence Establishment", Wilson Centre Digital Archive, April 30, 1948, p. 1, https://www.iwp.edu/wp-content/uploads/2019/05/20180116_KennanOnOrganizingPoliticalWarfareMemo.pdf. Accessed on April 11, 2024.
18. "Definition of the Term 'Psychological Warfare '", Central Intelligence Agency, 2004, p.3,https://www.cia.gov/readingroom/document/cia-rdp84-00022r000400110010-8. Accessed on January 29, 2024.
19. Claverie and du Cluzel, n. 2, p. 5.
20. Aonso Bernal, et al., "Cognitive Warfare: An Attack on Truth and Thought" NATO Innovation Hub, 2020, p. 9, https://www.innovationhub-act.org/cw-documents-0. Accessed on January 29, 2024.
21. "NATO Review: Countering Cognitive Warfare: Awareness and Resilience", *NATO Review*, May 20, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html. Accessed on March 2, 2024.
22. Sourced from Sun Tzu, *The Art Of War* (New York: Dover Publications, 2002).
23. Paul Charon and J.B. Jeangène Vilmer, "Chinese Influence Operations: A Machiavellian Moment",Institute for Strategic Research, October 2021, p. 45, https://www.irsem.fr/report.html. Accessed on January 19, 2024.

### *CW in Chinese Doctrine*

The Chinese doctrinal text, *Science of Military Strategy* (SMS) 2020, states that "maintaining [Chinese] cyber sovereignty is an indispensable and inevitable choice to stop hostile forces from creating social turmoil and subverting political stability."[24] SMS 2020 amplifies the Chinese concept of "cyber electromagnetic space warfare [CESW]", which "targets the opponent's psychology, cognitive domain and decision-making system, as well as the electromagnetic and information infrastructure."[25]

SMS 2020, also elaborates upon "public opinion struggle", which refers to the weaponisation of public opinion for targeted propaganda, to "unify the military and civilian ideological will, weaken and disintegrate the enemy's fighting will, create a favorable environment for public opinion, and control and discuss information".[26]

The Chinese concept of Cognitive Domain Operations (CDOs), as identified by French scholars, is inspired by the Chinese United Front ideology and the Three Warfares strategy.[27] CDOs leverage information, to influence the enemy's "cognitive functions, spanning from peacetime public opinion to wartime decision-making".[28]

### *A Conceptual Framework for CW*

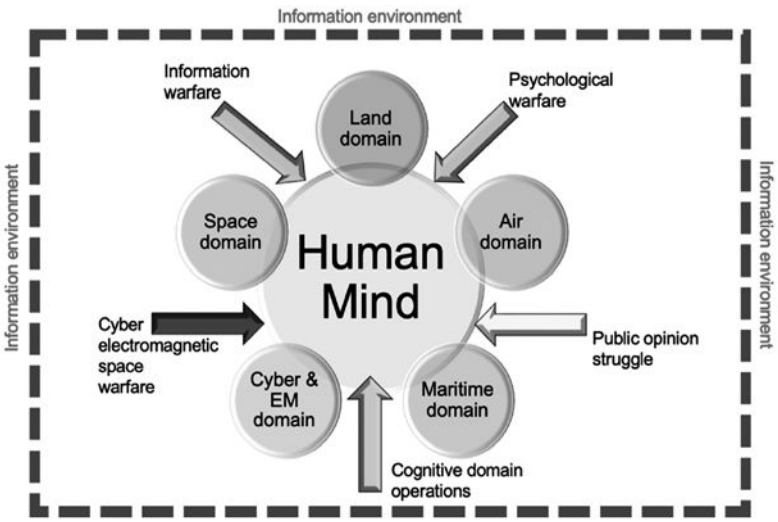
On reviewing various literature of US, Chinese, British and French origin, this article proposes that the human mind, both individually as well as collectively, is, in fact, the cognitive domain. The cognitive domain is central to all other domains of warfare and possesses varying degrees of overlap with the other domains. As a working definition, this article defines CW as warfare which targets the human cognitive domain, to alter or influence human behaviour, by

24. "In Their Own Words: Science of Military Strategy 2020", China Aerospace Studies Institute, 2022, p. 154, https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy/. Accessed on January 19, 2024.
25. Ibid., p. 236.
26. Ibid., p. 240.
27. Charon and Vilmer, n. 23, p. 27.
28. Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations", *China Brief,* vol. 19, no. 16, September 2019, https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/. Accessed on March 8, 2024.

leveraging information and propaganda, in the larger IE, through the ever-evolving tools and networks of the physical and cyber domains. The cognitive domain and CW are illustrated in Fig 1.

In view of the centrality of the human mind as the target, this article argues that CW, as an overarching term, subsumes PW, public opinion struggle, PsyW, IW, IO, CDO and CESW. This article shall endeavour to maintain a commonality of thought by replacing such usage of terms by the overarching term CW, while paraphrasing from scholarly works.

**Fig 1: Cognitive Domain and CW**




Source: Figure made by the author.

Having defined a possible conceptual framework for better understanding CW, we can now look at the *raison d'etre* and contours of contemporary Chinese CW.

## CONTOURS OF CHINESE CW

A Chinese policy option of CW would perhaps be driven by an interest or perhaps a policy compulsion. Such a policy option is likely to exhibit regional and global footprints. Chinese disinformation campaigns and media influence efforts in Taiwan are aimed at

discrediting as well as undermining Taiwan's elected government.[29] China also manipulates social media, using fake accounts to amplify the Chinese narrative, in multiple countries.[30]

***Raison d'Etre***

In case Chinese CW is indeed targeting democracies such as India, is there a Chinese compulsion to do so? The answer perhaps lies in the rationale behind Chinese interference in Taiwan. Puma Shen, an eminent Taiwanese scholar, argues that democracies such as Taiwan, which offer a democratic, stable and prosperous alternative to Chinese governance, are an existential threat to the CCP and, hence, to Chinese stability or the stated concept of national rejuvenation.[31]

The *raison d'etre* of Chinese interference in democracies is driven by the survival instincts of the CCP. Puma Shen argues that China's core national interest is to maintain China's stability and not the Chinese concept of national rejuvenation. In maintaining Chinese stability, the Chinese population, therefore, must find the CCP as the best option for China's governance and, hence, ensuring the belief of legitimacy as well as relevance of the CCP among the Chinese, becomes a priority for the CCP.[32]

Given the paucity of Chinese government literature on CW, the contours of Chinese CW can be drawn out from scholarly works and news reports on Chinese CW.

***Aims, Architecture and Audience of Chinese CW***

Chinese CW aims to control the human mind and associated thinking and decision-making capabilities, by leveraging a whole of government approach. Moreover, the Chinese wish to lead the narrative building process, so that the Chinese eventually decide upon the popular perception of the "winner and loser" in any event.[33] In order to achieve these aims, domestic and external Chinese

29. Cook, et. al., n. 3, p. 41.
30. n. 4, p. 123.
31. Ibid., pp. 14–15.
32. Ibid., pp. 14–15.
33. Josh Baughman, "How China Wins the Cognitive Domain",China Aerospace Studies Institute, 2023, pp. 3-4, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2023-01-23%20How%20China%20Wins%20the%20Cognitive%20Domain.pdf. Accessed on August 8, 2023.

operations in the cognitive domain are executed by various organs of the CCP and the government.

In China, at a political party level, the Propaganda Department, Chinese United Front Work Department (UFWD), International Liaison Department (ILD), and Chinese Youth League (CYL), which are a part of the CCP, are intimately involved in CW. The Chinese Propaganda Department controls domestic CW, the ILD maintains relations with political parties of other countries, the UFWD looks after both external and internal CW, while the CYL grooms future political leadership and mobilises the youth when required by the CCP.[34]

At the Chinese government level, the Chinese Ministry of State Security (MSS), and from a military perspective, the erstwhile Strategic Support Force (SSF) control influence operations in the electro-magnetic, cyber, information and space domains. In addition, to the Chinese political party and government level organisations, there are many Chinese technology companies, with links to the Chinese government and the Chinese military, which collect data, identifying suitable influence targets.[35]

The Chinese government's CW stakeholders have been tasked with four goals viz., (1) look after China's perceived reputation; (2) enhance China's global investment; (3) increase Chinese international influence; and (4) limit "any international speech or actions that are perceived to threaten the CCP's grip on power".[36] In attempting to achieve these goals, Chinese operations for influencing the cognitive domain are aimed at both domestic and international audiences i.e. (1) Chinese diaspora; (2) media; (3) diplomacy, including international organisations as well as norms; (4) economy; (5) politics; (6) education; (7) think-tanks; (8) culture and, among others; (9) social media as well as influencers.[37]

Global Chinese footprints of interference and CW, when analysed, should emerge in the form of certain categories and trends.

34. Charon and Vilmer, n. 23, pp. 15–16.
35. Ibid., p. 16.
36. Cook, et. al., n. 3, p. 4.
37. Charon and Vilmer, n. 23, pp. 17–18.

***Categories of Chinese Interference and Trends of Chinese CW***

Chinese interference in other countries falls into three categories: "(1) ideological interference; (2) establishing dependence; and (3) rule-making;"[38] Chinese ideological interference is executed via cognitive control over people, involving the media-cum-academia manipulation; the Chinese establish dependence by making nations dependent on the Chinese economy and technology, while Chinese rule-making refers to increasing leverage over international organisations, clout in diplomatic-cum-military relations, and enforcement of the pro-China perception in the rule of law.[39]

Chinese CW manifests along two trends: the first trend is where China attracts or seduces foreign audiences to a vibrant and positive Chinese image of strength, traditions and a Chinese way; while the second trend is where China slowly infiltrates into societies opposed to Chinese interests, via multiple intermediaries and thereafter progressively coerces the infiltrated society towards Chinese interests.[40]

In the case of Taiwan, in corroboration of the two trends of Chinese CW, firstly, persistent Chinese influence activities encourage pro-China perceptions among the Taiwanese youth and educationists; secondly, Chinese efforts create dependence on China in Taiwanese businesses, officials and political leaders, among other stakeholders.[41] Scholars identify a third trend in the Chinese attempts to separate the creation and distribution of propaganda, which renders Chinese CW indirect, covert, sophisticated and difficult to detect.[42]

The Chinese, having initially used Taiwan and Hong Kong as 'training grounds' for CW, have targeted several countries across the globe.[43] Aggressive Chinese CW, during the 2017 Doklam stand-off between India and China, attempted to create and drive a narrative to coerce Indian decision-makers, by exploiting the media spectrum.[44]

38. n. 4, p.15.
39. Ibid.
40. Charon and Vilmer, n. 23, p.16.
41. n. 4, p. 17.
42. Ibid., p. 21.
43. Charon and Vilmer, n. 23, p. 18.
44. Ibid., pp. 50–51.

Another report highlights Chinese cyber operations aimed at future election interference in the US.[45]

***Chinese CW in India***

In India, China targets the intellectual elite, including political parties, with long-term implications, while Chinese investments in the entertainment, education sector and other critical sectors create economic dependence on the Chinese, thereby rendering India vulnerable to manipulation.[46] Chinese cooption of Indian academia, mushrooming of pro-China study groups and investments in India's prominent education technology companies reflect an established Chinese pattern of influencing and manipulating the impressionable youth.[47]

A US report on China's Global Media Influence claims that the Chinese insert paid content in Indian newspapers, attempt to coopt Indian journalists, carry out aggressive cyber activities against the Tibetan diaspora in India and engage with a wide Indian demographic base using vernacular content on social media.[48] The report rates Chinese influence attempts at 31 out of a total score of 85, while Indian resilience to Chinese influence has been rated at 40 out of a total score of 85.[49] In a Taiwanese report, India's vulnerability exposure to Chinese influence is ranked at a relatively lower score of 23 percent and Chinese pressure to change India's behaviour towards China ranks at 31 percent.[50]

Cyber security research reports highlight an increase in incidents of "suspected state-sponsored Chinese cyber operations targeting Indian organizations and companies", by nearly 120 percent from the

45. Seth G. Jones, et. al., "Competing Without Fighting: China's Strategy of Political Warfare.",Centre for Strategic and International Studies, August 2, 2023, pp. 37-38, https://www.csis.org/analysis/chinas-strategy-political-warfare. Accessed on November 5, 2023.
46. N. C. Bipindra, *Mapping Chinese Footprints and Influence Operations in India* (New Delhi: Law and Society Alliance, 2021), p. 64, https://defence.capital/wp-content/uploads/2021/09/MAPPING-CHINESE-FOOTPRINTS-AND-INFLUENCE-OPERATIONS-IN-INDIA2.pdf. Accessed on November 12, 2023.
47. Ibid., pp. 18–20.
48. Cook, et. al., n. 3, p. 6, p.35.
49. Ibid., p. 26.
50. "China Index 2022", November 15, 2022, https://china-index.io/country. Accessed on November 2, 2023.

year 2019 to 2020 and which further increased by 261 percent from year 2020 to 2021.[51] The report alludes to possible linkages between suspected Chinese sponsored cyber operations against the Unique Identification Authority of India (UIDAI), with the purpose of "identifying high-value targets such as government officials, enabling social engineering attacks, or enriching other data sources."[52]

The response to Chinese CW in India includes banning of Chinese apps, and deeper scrutiny of Chinese investments in India. In June 2020, amidst the Galwan stand-off with China, India banned 59 Chinese apps, including Tik Tok, over security concerns.[53] Additional apps as well as websites linked to China, were reportedly banned in 2023.[54] In July 2023, Chinese car maker BYD, reportedly shelved investment plans in Indian Electric Vehicles (EVs), over Indian security concerns.[55] Similarly in 2022, Chinese car maker Great Wall, also failed to obtain regulatory approvals for establishing a car business in India.[56] In 2022, assets of Chinese phone maker Xiaomi were frozen in India, due to illegal financial remittances.[57]

51. "China-Linked Group TAG-28 Targets India's 'The Times Group' and UIDAI (Aadhaar) Government Agency With Winnti Malware", *Recorded Future*, September 21, 2021, https://www.recordedfuture.com/china-linked-tag-28-targets-indias-the-times-group. Accessed on January 2, 2024.
52. Ibid.
53. "India Bans 59 Chinese Mobile Apps Including TikTok And Shareit", *Outlook*, June 29, 2020, https://www.outlookindia.com/website/story/india-news-india-bans-59-chinese-mobile-apps-including-tik-tok-and-shareit/355679. Accessed on January 2, 2024.
54. "India Bans 200-Plus Chinese Mobile Apps in Boon for Paytm", *Hindustan Times Tech*, February 8, 2023, https://tech.hindustantimes.com/tech/news/india-bans-200-plus-chinese-mobile-apps-in-boon-for-paytm-71675797420850.html. Accessed on January 4, 2024.
55. Sarita Chaganti Singh, "Exclusive: BYD Tells India Partner It Wants to Drop $1 Billion EV Investment Plan, Sources Say", Reuters, July 28, 2023, https://www.reuters.com/business/autos-transportation/byd-tells-india-partner-it-wants-drop-1-bln-ev-investment-plan-sources-2023-07-28/. Accessed on January 2, 2024.
56. Aditi Shah, "China's Great Wall Motor Shelves $1 Bln India Plan -Sources", Reuters, July 1, 2022, https://www.reuters.com/business/autos-transportation/chinas-great-wall-shelves-1-billion-india-investment-plan-sources-2022-07-01/. Accessed on January 12, 2024.
57. Aditya Kalra, "India Court Rejects Xiaomi's Challenge to $676 Million Asset Freeze", Reuters, April 21, 2023, https://www.reuters.com/technology/india-court-rejects-xiaomis-challenge-676-mln-asset-freeze-live-law-2023-04-21/. Accessed on January 12, 2024.

This part of the article identified the possible Chinese *raison d'etre*, aim, architecture, audiences and manifestation of contemporary Chinese CW. The article shall now propose a possible Chinese strategy for CW framed in an ends-ways-means construct.

***Chinese Strategy for CW and Policy Options***

On distilling existing research on Chinese CW into a construct of ends-ways-means, a possible Chinese strategy for CW emerges. The key aspects of the Chinese strategy, in brief, have been placed at Table 1.

**Table 1. Possible Chinese Strategy for CW**

| Ends | Ways | Means |
|---|---|---|
| • Stability of China.<br>• Limit or remove threats to CCP's legitimacy, role and relevance.<br>• Enhance China's global and domestic image.<br>• Enhance China's global investments.<br>• Increase Chinese international influence and leverage.<br>• Undermine democratic institutions. | • Indirect investments in critical sectors and coercion.<br>• Cyber operations and espionage.<br>• Media control and influence.<br>• Build relations with foreign politicians through lobbying, outreach and fund contributions.<br>• Monitoring Chinese dissidents and diaspora.<br>• Direct information manipulation.<br>• Spread disinformation. | • UFWD.<br>• MSS, ILD and CYL.<br>• Chinese Cyber Militia and erstwhile PLA SSF.<br>• Chinese diplomats.<br>• Chinese state owned media.<br>• Chinese entertainment industries.<br>• Social media influencers.<br>• China controlled troll and content farms.<br>• Confucius Institutes and similar pro-China centres<br>• Coopted, coerced or manipulated foreign media, youth, intellectuals and diaspora. |

| | | |
|---|---|---|
| | • Censorship of internet and media.<br>• Cyber bullying and trolling of journalists. | |

Source: Author's compilation, based on a review of contemporary literature on Chinese CW.[58]

Chinese strategy is clearly long-term and strategic in nature, therefore, the policy response options by democracies, including India, should be similarly nuanced and carefully calibrated. A long-term view, to safeguard the very concept of democracy itself, against an ideological autocratic onslaught, is perhaps the need of the hour.

## CONCLUSION

Warfare in the cognitive domain centres around the human mind, which, in turn, has a significant overlap among the other domains. Various kinds of warfare and operations targeting the human mind, can arguably be subsumed under the overarching term of CW. China practises CW globally with the possible strategic intent of undermining democratic countries and the potential to fracture societies by weaponising information.

Security concerns drive India's responses to Chinese CW. India's increasing scrutiny over Chinese investments through regulatory frameworks and banning Chinese apps, are some of the responses highlighted in this article. The Chinese CW strategy seamlessly aligns with the Chinese strategy of winning without fighting and merits further research in possible policy actions as well as a counter-strategy by India and other democracies. Identifying Chinese CW strategy is the first step to deter or counter this strategy.

58. n. 4, pp. 14–17;. Charon and Vilmer, n. 23, pp. 15–16.