INFORMATION WARFARE ON INDIA: FIGHTING AN INVISIBLE WAR

Maj Vishnu RJ

Abstract

Information Warfare (IW) is emerging as a critical threat to the national security of India especially since it is exploiting the fault lines in a huge and diverse population. It aims to gain an upper hand over the enemy by creating confusion, degrading the societal structure and destroying the resolve of the targeted country. A nation is destabilised using a multitude of techniques including cyber-attacks, misinformation and psychological operations. The complex and multifaceted nature of IW presents a tricky battlefront in which any potent opponent is tempted and confused to act, thereby eschewing a set-piece mechanical response. Social media, news platforms and digital networks are being extensively used to disseminate false narratives, incite social unrest and undermine public trust in national institutions. The disruption of technology has introduced new soldiers for IW in the form of deepfakes, bot armies and other intelligent machines to this digital battlefield. There is an urgent requirement to address this invisible war waged on India to safeguard its sovereignty and democratic values. This study explores the concept of IW along with its effect on the contemporary battlefield to understand its effects on a nation. The study also suggests certain countermeasures and recommendations, especially given a dual front IW by China and Pakistan

INTRODUCTION

Indian epic Mahabharata mentions this famous incident where misinformation was used to deceive Guru Dronacharya into believing his son Ashwatthama was dead instead of the elephant with the same name. This act by Yudhishitra led to the death of Dronacharya and shifted the momentum of the Epic Mahabharata Battle in Pandavas' favour. From ancient strategists like Kautilya and Sun Tzu to modern thinkers like David Petraeus emphasised on the concept of 'Winning a war without fighting'. It involves the use of wisdom, strategy and diplomacy to force the opponent to surrender.[1] The WWI too saw an extensive exploitation of the information domain. Great Britain, then a global communication hub, caused a communication blackout for Germany by cutting off telegraph lines which was the mainstay of military communication. Similarly, the command-and-control structure of Iraq was collapsed by the US-led coalition in the first Gulf War. They deactivated the SPOT satellite system to obscure Saddam Hussein's observations before deploying tactical diversionary manoeuvres by US ground forces. In more recent times, Russia used hybrid warfare in Ukraine to effectively annex Crimea even without firing a shot. IW when used to their full potential can significantly influence the battlefield by deceiving, weakening and degrading the enemy's resolve. These non-violent manoeuvres are more powerful and destructive than conventional military strategies like fire and manoeuvres. However, to influence a foreign audience effectively, one must be well-versed in their language, culture and history. In the twenty-first century, a multitude of technologies are interacting in various planes making IW a decisive tool in modern battlefields particularly for weaker actors due to its accessibility and low cost.

PHILOSOPHICAL PERSPECTIVE OF IW

Information Operations defines IW as the “integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own”.[2]

IW covers a multitude of actions to gain a competitive advantage over the enemy by influencing ideas and perceptions. It involves a constant

integration of information, physical, psychological and cognitive domains on the foundation of data, technology and communication networks. The existing established beliefs and customs are progressively destroyed to exhaust the spirit of a nation. Traditionally, this was made possible through a calculated mix of disinformation, misinformation and propaganda. Along with radio communication came Electronic Warfare (EW) and growing reliance on computers paved the way for cyber warfare within the realms of IW. The integration of cyber, cognitive and space domains is further complicating the effects of IW.

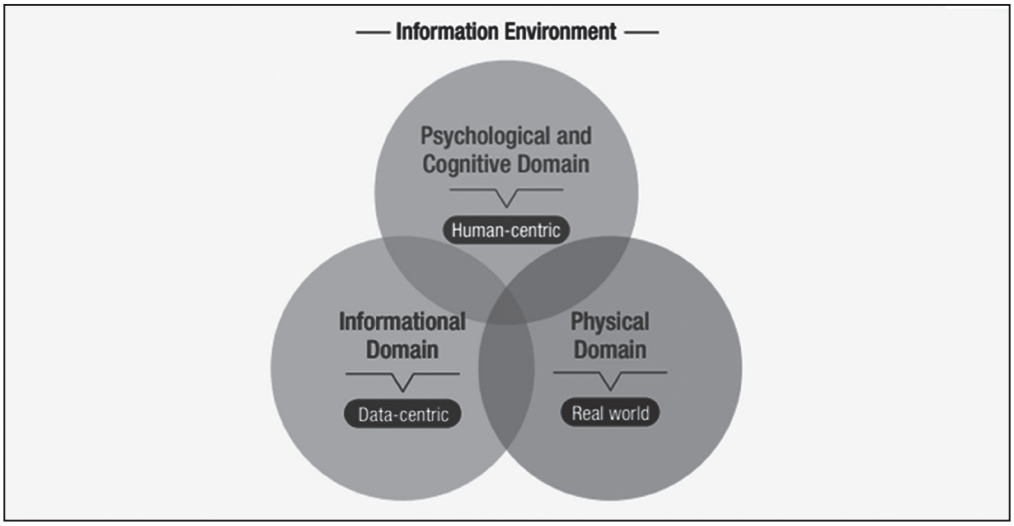

Figure 1: Interactions in the information environment. **Source:** Shinji 2023, 28.[3]

- **Information is Power.** There is a continuous interaction between a person with his working environment and his understanding of an event is influenced by the information available to him along with his personal beliefs. It will be highly empowering for him to have accurate information at the right time as it helps him shape his decisions, influence opinions and drive changes. Thus, sustained misinformation and propaganda can easily obscure the truth and progressively influence the belief system of a person. The impact of IW is often enhanced by shaping the response of an audience through controlled narratives in microtargeted content.[4]

These sensationalised media are subconscious biases leading to reactions rather than thoughtful responses. The COVID-19 pandemic highlighted that information overload can cause confusion and chaos. The world was exposed to too much information which was a combination of correct information, misinformation and disinformation that occurs during a disease outbreak. The WHO defines this as infodemic'.[5]

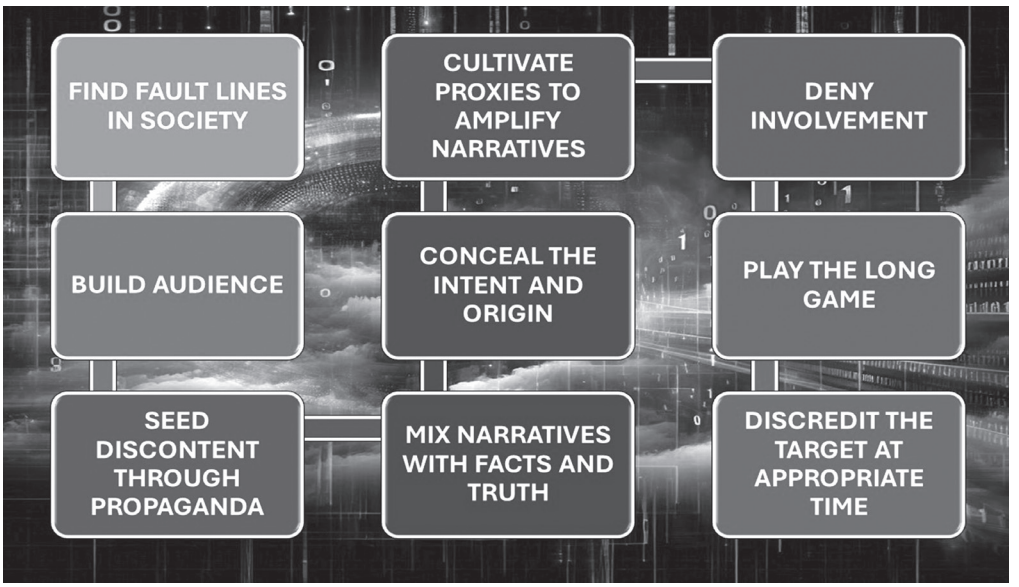

Figure 2: Operation of IW to achieve the result. **Source:** Author

- **IW in the Digital Era.** Disruptive technologies are transforming IW by increasing the speed, influence and impact of information dissemination. It enables IW operations in the complete spectrum of warfighting by integrating multiple domains in both time and space. Even though cyberspace has evolved as a powerful medium for shaping consciousness and social values the nature of influence continues to transform with the evolution of technologies like AI and Big Data. Social media and digital communication are now primary means of global influence and countries are leveraging on them to shape public opinion. Digital tools have increasingly evolved to become more effective, efficient and intelligent. This is increasing the complexity and frequency of IW in the modern battlefield.

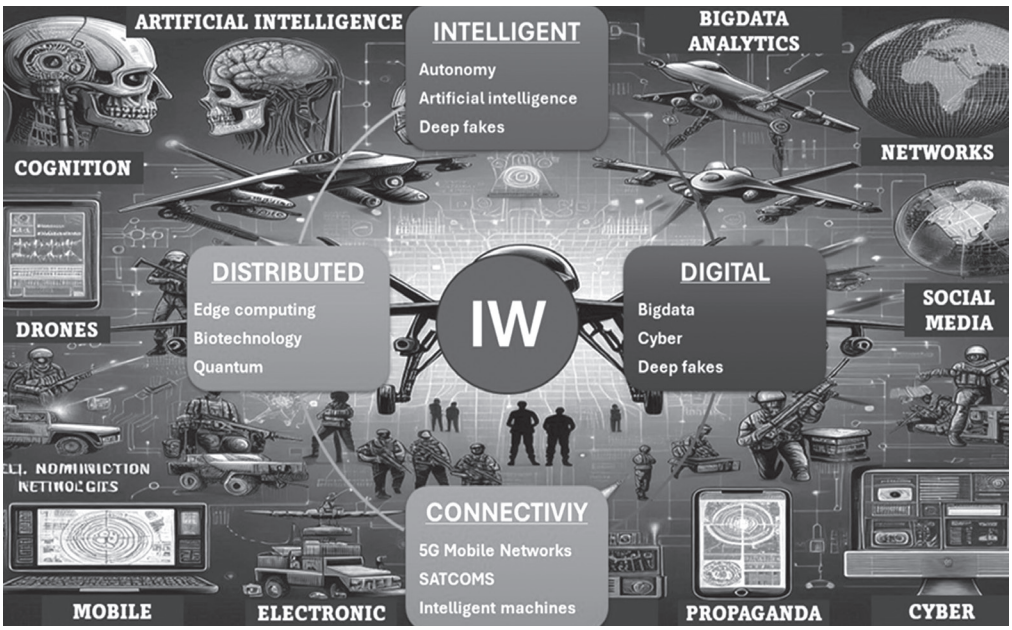

Figure 3: Interpretation of technologies involved in IW. **Source:** Author

- **IW Altering Traditional Warfighting Concepts.** While conventional warfare focuses on fire and manoeuvre, IW emphasises the strategic use of information on the backbone of technology to outmanoeuvre adversaries. This is making it a vital component of modern military strategy. The U.S. Department of Defence has been integrating IW into its operations to counter threats from state and non-state actors.[6] Recently, there has been a rise in computational propaganda and AI-generated content to manipulate public opinion for political activism and public mobilisation. However, the impact of these digital contents varies with each generation highlighting the complexity of new-gen IW. Gen Z favours reliable news sources and uses social media as their main news platform. Even though they view each content sceptically and expose falsehoods by fact-checking information. They are still struggling to identify misinformation. The exposure to false stories on a large scale and huge rate is making them more susceptible to IW. Countries like China and Russia have been leveraging IW to achieve their geopolitical goals without engaging in direct military conflict.[7,8] Big Tech companies like Meta and "X" are significantly influencing

content management on their platform to alter the information as per their interest.

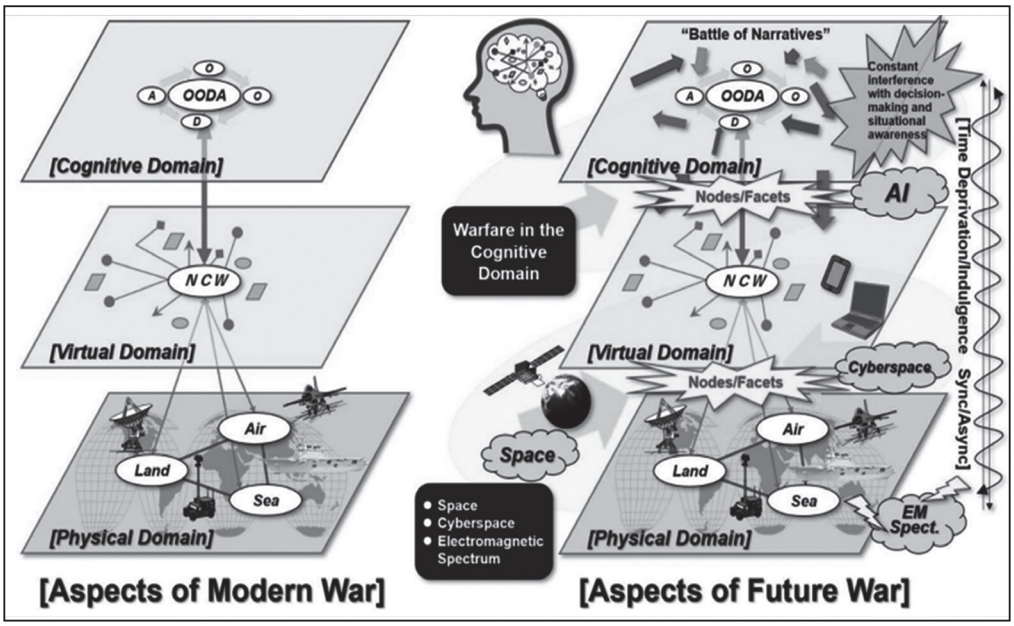

Figure 4: Complexities of the future under the umbrella of IW.
Source: Kazumi 2021.[9]

- **Ethics and IW.** IW has a complex relationship with the 'Just War Theory'. While IW can justify initiating war Jus ad Bellum through narrative building and propaganda, it contradicts the ethical conduct of war Jus in Bello and post-war justice Jus post-Bellum. These operations involve information manipulation, identity theft, infringement of privacy and security breaches thereby lacking ethical justification and morality. It often causes political and social dilemmas in a country by meddling in its internal affairs. Constant exposure to manipulated information can have psychological effects on the countrymen of the targeted nation, including increased anxiety, fear and a sense of helplessness.[10] Information manipulation can harm human psychology and give an unfair advantage to the powerful nation. Balancing national security with individual privacy rights

is a dilemma. Technology is outpacing the existing International conventions. These laws and guidelines lack codes of ethics for IW.

- **Human-Machine Integration and Evolution of CDO.** The lethal blend of humans with disruptive technologies like AI, affective computing, biometrics, neurotechnology and cyber technology is revolutionising global intelligence. Intelligent machines are used to gauge and envisage human behaviour using sentiment analysis and predictive algorithms. Based on these algorithms, the bots create and spread deep fakes, fake news and other misleading content to influence perceptions and behaviours. The recent conflicts amply demonstrate the evolution of traditional IW to CDO which is the ultimate form of IW. CDO is an inclusive multi-dimensional attack and defence strategy involving political, economic, military, diplomatic and public opinion tactics. CDO leverages information and technology by integrating disruptive technologies with IW to target cognition. It begins at the conscious level to affect how people perceive a nation, disrupt societal understanding, control reactions by exploiting psychological vulnerabilities and is referred to as 'Cognitive Hacking'.[11]

- **IW for Effect-Based Operations (EBO).** EBO aims to achieve the end state with minimal force and emphasises strategic effects. It aims to reach definite effects rather than merely destroying enemy forces. This process involves analysing the relationships and influences in the adversary's system to predict their responses and actions. This approach starts by defining the strategic effect and plans backwards to identify necessary tactical actions to achieve this effect. This philosophy enables the tactical intertwining of IW with EBO to achieve the desired 'effect'. Strategic communication is used to shape public opinion to accomplish this end state. Thus, enabling an intersection between EBO and Cognitive Domain Operations (CDO) at the strategic plane by directly targeting cognition.

- **Digital Colonisation (Kwet 2019).**[12] Domination of less powerful regions by powerful nations or corporations using digital technology is often called Digital Colonisation. The powerful tech companies are extracting, exploiting and controlling data from developed countries to

cause economic and social dependency, unlike historical times when colonisation was for exploiting natural resources. The companies like Google, Amazon and Meta dominate the digital landscape and collect vast amounts of data from developing countries.[13] While India is the country with the biggest amount of Facebook users, of the location of Facebook's fifteen data centres, ten are in North America, four in Europe and one in Asia.[14] These countries not only overshadow local cultures and social values leading to a loss of local identity but also set up data centres and infrastructure to benefit their home countries.

IW TECHNIQUES

World nations have taken massive strides to develop techniques and procedures to incorporate IW into the new age of warfighting. Propaganda and Psychological Operations are widely used to manipulate global judgment about a nation through planned radical, economic, military and socio-political activities. These actions are directed towards organisations and individuals of the targeted country to create emotions, attitudes, understanding, beliefs and behaviour.[15] The information revolution revolving around Internet-enabled platforms and technologies effectively degraded the natural resiliency of democratic processes to manipulative IW.[16] This gave way to the cyber-based influence technique based on a continually iterative and time-sensitive process where it is crucial not only to message first but also to maintain a sustained rate.[17] Military Deception is another vital tool that can integrate traditional warfighting tactics with cyber capabilities. It hampers the decision-making of the enemy and forces him to misallocate resources.

OPSEC on the other hand provides a foundation for identifying and protecting critical information by balancing security with operational efficiency to assist military planners in prioritising and safeguarding critical data. This is achieved through information security, information assurance, physical security and operations security.[18] EW shapes the information environment electronically on the backbone of advancements in various disruptive technologies and is often integrated with PSYOP, Military Deception and Computer Network Operations. This integration

helps to create a comprehensive strategy to influence, disrupt, or deceive adversaries.[19] The digitalised IW is also using social media platforms supported by intelligent machines to influence and achieve strategic objectives. Automated bot accounts are launching coordinated campaigns to amplify specific messages to make them appear more credible. During the Russo-Ukraine conflict, Ukraine has effectively managed to gain global sympathy by sharing real-time updates, videos and memes.[20] Perception management on the other hand monopolises on achieving strategic objectives by influencing how people perceive reality. It alters basic human emotions using carefully crafted messages by targeting emotions like fear and anger.

Figure 5: Stages of OPSEC**. Source:** Author

IMPACT OF IW ON NATIONAL SECURITY

IW significantly impacts geopolitics by influencing political processes, destabilising adversaries and shaping the global perception of an event, a conflict or a nation. Russia has been an expert in using IW effectively to undermine the democratic process for various states, especially the US. They used race-related issues to target African Americans through social media, hacking, and disinformation. In 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency

used social media to conduct an IW campaign designed to spread disinformation and societal division in the US.[21] These tailored messages can alter the socio-political condition of the targeted country by addressing the specific audience to create new fault lines or exploit old ones. During the Russo-Ukraine conflict, Kyiv used a mix of emotion, political interests and even humour to counterattack Moscow online to create a herd effect as users across the world shared Zelensky speeches, satirical Darth Putin quips and videos made by Ukrainian citizens.[22] Russia countered this by employing influence-for-hire firms to target far-right and far-left groups with tailored messages that indirectly supported their narrative which led to declining global support for Ukraine and increasing criticism of Western support for the war. Over the past year, Russia has aimed to weaken Ukraine's resolve and create internal discord by discrediting its civilian and military leaders. Ukraine was portrayed as an unstable nation by amplifying the internal conflicts using social media. The Kremlin's propaganda apparatus established the largest known influence operation on TikTok to disseminate rumours about Ukrainian political corruption.[23] On the other hand, the US and British acting in cooperation, announced details of a purported Russian plot to install a pro-Moscow regime in Kyiv and named a pro-Russia former member of the Ukrainian parliament as Putin's preferred puppet.[24] Strategic competition has evolved from the traditional binary view of peace and war to an extensive continuum of competitions that stays below armed conflict.

Strategic Communications (StratCom) are often used by nations to demonstrate their national goals and interests. It protects one's narrative from hostile foreign narratives to ensure the alignment of political goals with national interests. NATO has built its capacity and capability by creating the first military StratCom doctrine in March 2023. This forms the foundation for organising and conducting these operations in a new era. These operations use concealed actors, methods and goals to disseminate messages rapidly and repetitively to blur the line between reality and fiction through cross-media reinforcement by influencers. The use of familiar topics or seemingly verified evidence creates a mix

of lies and partial truths to shape public judgment. This process is known as “information laundering”.[25]

CHINA-PAK IW ONSLAUGHT ON INDIA

India may encounter concurrent conflicts with both China and Pakistan potentially involving both overt military assistance and covert support between the two nations. IW is a major front where they can collaborate to create division within Indian society and discredit India globally. Beijing is already conducting a large-scale misinformation campaign using multiple social media platforms such as ‘X’, Facebook, Instagram and YouTube against New Delhi by spreading fake news and propaganda online to undermine India’s global reputation. Since 2020, China’s intensified disinformation strategy and Chinese diplomats have assumed a more aggressive posture in supporting and guarding Beijing’s interests against criticism. This broader IW approach is often termed as 'Wolf Warrior Diplomacy'. China’s misinformation factories are manufacturing numerous fake news against India’s G20 presidency, the Manipur conflict, Buddhism & the Dalai Lama and are even spreading lies to fuel tension between India and Canada.[26] China has been making multiple micro-aggressions such as not sending a delegation to the Y20 forum hosted by India, disputing India’s use of the theme 'Vasudhaiva Kutumbakam' and the release of maps claiming Indian territories as Chinese. They have been running false claims about the conflict in Manipur, accusing India of running concentration camps for minorities and suggesting that Northeast Indian states should secede from India.[27]

Pakistan too has been involved in numerous disinformation campaigns by spreading fake news and divisive content against India. Channels and websites from Pakistan, including the Naya Pakistan Group have been posting divisive content on sensitive topics. These websites with over 3.5 million subscribers and 5.5 billion views have been trying to spread discontent in Kashmir, the Indian Army and minority communities. They aimed to undermine the election process in India by highlighting issues like the farmers’ protest and the Citizenship Amendment Act. Kashmir

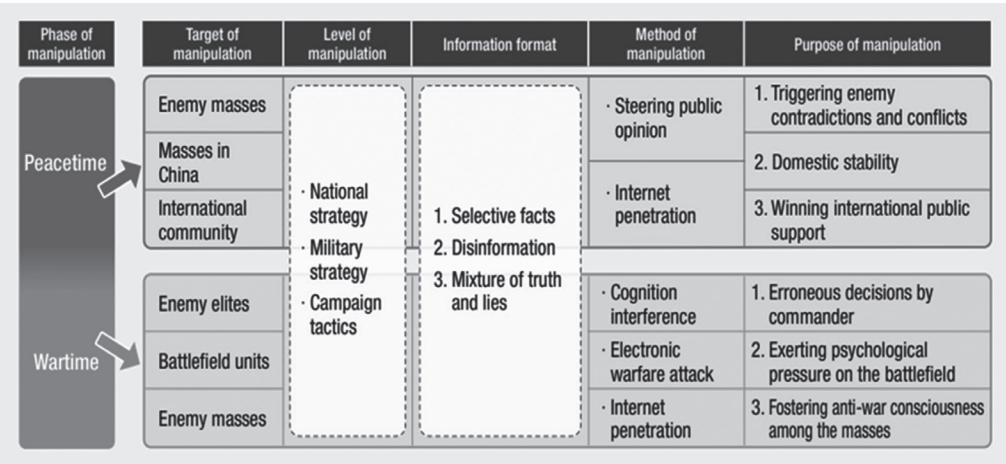

Figure 6: Line of Operations of PLA IW. **Source:** Shinji 2023, 49.[28]

has seen a huge spike in disinformation campaigns especially after the abrogation of Article 370 in 2019. This involves false claims about resource shortages and administrative problems in the region post the abrogation. In 2021, the Ministry of Information and Broadcasting ordered the blocking of twenty YouTube channels and two websites sponsored by Pakistan for spreading anti-India propaganda and fake news.[29]

SOCIO-POLITICAL IMPLICATIONS OF CHINA-PAK IW

- **Political Impact.** They exploit identity politics such as inequality and wealth disparity in India by disguising propaganda as genuine information causing widespread scepticism and cynicism. This causes the population to undermine the government, divert their attention from nation-building and incite political violence. Continuous disinformation will erode public trust in institutions including judiciary, media and scientific communities.
- **Social Impact.** IW exacerbates the social and political divide in society to cause heightened polarisation and social unrest within India. It fosters mistrust and suspicion among diverse groups by exploiting sensitive issues like religion, ethnicity and identity causing anxiety, stress and a sense of helplessness. This undermines the

efforts of the government and other institutions to create inclusive and resilient communities.

- **Diplomatic Issues.** Coordinated disinformation narratives are launched by these nations to diplomatically isolate India by portraying her negatively in global fora. The aim is to cause a rift between India and its allies by creating suspicion about India's intentions. Indian diplomats will face difficulties in garnering support on agendas like terrorism and regional security on global forums like the UN.
- **National Security Concerns.** Coordinated IW can disrupt essential services, damage the economy and expose sensitive information to endanger operational stability and threaten national security. Advanced AI technologies especially language models have enhanced China's ability to conduct sophisticated IW. The deepfake videos are undermining governance and public confidence by creating realistic but fake videos of politicians and celebrities. This is often termed as 'infocalypse'.[30]

WORK-IN-PROGRESS FOR INDIA AND ARMED FORCES

With the disruption in technology and social media, information is being highlighted as an important joint function in military operations leading to greater advocacy and integration of information into military plans. The major lessons for India are as given below:

- **Bolstering Cybersecurity.** The digital era necessitates an enhanced use of cyber assets to cope with the speed of technology. The critical networks, infrastructure and systems are thus vulnerable to cyber-attacks and their protection will be crucial for fighting against IW. They can be protected by enhancing the security of digital infrastructure and implementing robust cybersecurity measures.

BOLSTERING CYBERSECURITY	
Government Networks	Conducting frequent security audits and vulnerability assessments. Implement strong encryption protocols using Multi-Factor Authentication. Role-based access controls to limit access to sensitive information.
Security of Critical Infrastructure	Ensure system resilience and swift recovery by implementing redundancy. Updating incident response plans and fostering public-private collaboration for threat intelligence sharing and best practices.
Security of Private Sector Systems	Conduct regular cybersecurity training, deploy endpoint security solutions and implement data loss prevention. Deploy comprehensive endpoint security solutions to safeguard devices connected to the network.
General Cybersecurity Measures	Regular software update and segment networks to protect against vulnerabilities and contain malware spread. Utilise advanced threat detection systems, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS).
Futureproofing	2FA add an extra layer of security to prevent unauthorized access. RPKI secures internet routing by verifying IP addresses. IPv6 addresses modern security features like IPsec, ensuring long-term internet growth and secure communications.

Figure 7: Measures to bolster cyber security. **Source**: Ratiu 2024[31] Clark 2023[32]

- **Promoting Media Literacy.**The major component of the IW setup is the cognitive and psychological domain. Humans are both the target as well as the resource in this scenario. The humans operating in this setup must critically evaluate the information and understand it before giving a suitable response. Thus, educating the public on this aspect is crucial in this digital age. Key aspects are given in Figure 8.

PROMOTING MEDIA LITERACY	
Media Literacy Programs	Incorporate media literacy into school curriculums to teach students how to analyse and evaluate information from an early age. Conduct community workshops and seminars to educate adults on recognising disinformation.
Identifying Disinformation	Promote the use of fact-checking websites and tools to verify the accuracy of information. Encourage individuals to critically evaluate the information they encounter by assessing the evidence provided and identifying potential biases.
Understanding Information Sources	Educate individuals on evaluating the authority and reliability of various sources. Government must promote transparency in media by advocating for clear authorship and accountability for published content.
Making Informed Decisions	Advocate for comparing multiple sources to gain a comprehensive understanding of a topic and use logical reasoning skills to evaluate the validity of arguments and evidence.
Reducing Impact of False Narratives	Initiate awareness campaigns to highlight the dangers of disinformation and the importance of media literacy. They must encourage discussions to build collective understanding and resilience against false narratives.
Building a Resilient Society	Collaboration between educational institutions, government bodies and media organizations to improve media literacy. Emphasis must be given for continuous learning.

Figure 8: Media Literacy. **Source:** Compiled by the author

- **Collaborative International Efforts.** India must advocate and facilitate agreements to simplify secure intelligence exchange between allied nations. Sensitive information must be shared over

established protocols while ensuring data protection and privacy. Joint intelligence centres must be set up with trusted allies for real-time information sharing on emerging threats. This will facilitate the quick identification of IW threats and their mitigation. Alliances like QUAD must collaborate to find transformative solutions for combating IW threats and share best practices to foster global cybersecurity guidelines.

- **Investing in Technology and Innovation.** The government must invest in home-grown advanced technologies and innovations to enhance the ability to detect and counter IW. AI-enabled algorithms can be effectively used to monitor and analyse data by detecting patterns of various IW techniques. These intelligent platforms can facilitate real-time alert systems to enable rapid coordinated responses. Cheap open-source secure cybersecurity tools must be created and made available to the common man to protect his data. Pilot programs to evaluate these technologies in real-world scenarios to gain valuable insights should be implemented and refine the approach before large-scale deployment.
- **Joint Inter-Service Network.** Indian Armed Forces could collaborate with the private technology companies to build a robust network setup which is both cyber and EMP-hardened. These networks must possess adequate redundancy and survivability to function in all environments. It must consider a proactive approach based on the Chinese Net Force model[33] that is more offensive rather than the existing more defensive 'CERT' concept to respond to cyber-attacks.
- **Building and Retaining a National Force for IW.** Immediate response is vital in IW to prevent considerable damage and maintain national harmony. Indian Armed forces must build a dedicated national force with strong IW capability to enhance the global standing as a formidable force. It must take cues from the recently established Cyber Command while laying the foundation for this new force. This force must be facilitated on the foundations of a strong legal and ethical framework, homegrown technologies, international collaboration

and a trained workforce.[34] An evolutionary approach must be taken that can start with the integration of the current IO resources from the three Services into a newly formed IO Command Headquarters. Additional specialist units could be raised subsequently in a phased manner to gradually boost its capabilities.[35]

Building and Retaining a National Force for IW	
Cyber Espionage	Gather intelligence on potential threats by infiltrating adversaries networks.
Disinformation Campaigns	Craft and disseminate false information to mislead adversaries and disrupt their operations.
Strategic Planning	Developing and executing offensive IW strategies to weaken adversaries.
Threat Detection	Identifying and monitoring cyber threats, misinformation and espionage activities.
Counter Intelligence	Preventing and neutralizing espionage efforts by foreign entities aimed at compromising national security.
Incident Response	Coordinating rapid responses to cyber-attacks and misinformation campaigns to mitigate their impact.
Analysis and Reporting	Providing detailed analysis and reports on IW threats and trends to help decision-making.
Collaboration	Working with other national and international agencies to share intelligence.
Training and Development	Educating and training personnel in IW tactics, techniques, and procedures to enhance overall capabilities.
Oversight and Accountability	Monitor intelligence activities to ensure that they adhere to legal standards and respect civil liberties. Implement internal policies and directives that provide guidelines and procedures for its operations.

Figure 9: Measures to Build a National Force for IW. **Source:** Author

- **Incorporation of IW Concepts in Military Training.** Incorporating IW into military training is crucial for preparing the armed forces for the digital battlefield. This comprehensive training must include dedicated courses on cyber defence, offensive cyber operations and information strategies. It should also include war games, simulations and joint exercises using cyber ranges and the latest IW tools.[36]
- **Whole-of-Government Approach.** The whole-of-government approach includes collaborative efforts across various tools of governance including military, intelligence, academia, civilian agencies and law enforcement. This strategy emphasises inter-agency collaboration, robust information sharing and unified strategies including establishing legal standards, fostering public-private partnerships and engaging in international cooperation.[37] Dedicated funds must be arranged through long-term legislative appropriations

and diversified sources like grants and public-private partnerships. The government must establish partnerships formalised through agreements like MOUs and joint ventures with tech companies and cybersecurity firms. IW strategies must be assessed through regular review of performance matrices and insights must be communicated for necessary alterations by the government.

CONCLUSION

Information had evolved to become both a weapon and a battleground. The new age of digital battlefields is necessitating innovative cognitive combat tactics. IW along with other domains of warfighting had embraced the nuances of disruptive technologies, generational changes, cognitive developments, etc to achieve this effect. This new age IW revolves around the concept of altering the perception of a population through cognitive shaping to achieve political goals. It should be understood that this invisible war is not just a matter of national security but also protection of democratic principles. The study has emphasised the multifaceted and disrupting nature of IW. Adversaries are exploiting digital platforms, social media, deep fakes, bot armies, etc to spread false narratives, incite social unrest and erode trust in national institutions. Effective countermeasures must be developed by India based on the understanding of these newage IW tactics. To safeguard its sovereignty and democratic values, India must develop homegrown disruptive technologies, improve cyber resilience and promote media literacy. This must include digital literacy, strengthen digital infrastructure and foster international cooperation. Combat stages in this approach involve monitoring web-connected devices, mapping information spaces and evolving rapid responses. India must form dynamic and proactive future strategies based on vigilance, rapid response and multinational cooperation. This will ensure the societal cohesion and the integrity of the democratic processes in the digital age.

★★★

Maj Vishnu RJ is an alumnus of the Defence Services Staff Collage, Wellington, the National Defence Academy, Khadakwasla and Sainik School Kazhakootam. He is a serving officer in the Regiment of Artillery and is currently posted as an Instructor Cl 'A' at School of Artillery, Deolali.

NOTES

1 *Amanda Penn, Subdue the Enemy Without Fighting: 5 Rules (Sun Tzu), SHORTFORM, 15 November 2019, Accessed: 28 August 2024, URL: Subdue the Enemy Without Fighting: 5 Rules (Sun Tzu) | Shortform Books.*

2 *Brunetti-Lihach Nick, Information Warfare Past, Present, and Future, Real Clear Defense, 14 November 2018, Accessed: 28 August 2014, URL: Information Warfare Past, Present, and Future | RealClearDefense.*

3 *Shinji Yamaguchi, et al, China's Quest for Control of the Cognitive Domain and Gray Zone Situations, National Institute for Defense Studies, Japan,2023,28.*

4 *Gavin Wright, Microtargeting, TechTarget, September 2023, Accessed: 28 August 2014, URL: What is microtargeting? | Definition from TechTarget.*

5 *Sarah Gibbens, A guide to overcoming COVID-19 misinformation, National Geographic, 22 October 2020, Accessed: 28 August 2014, URL: The 'infodemic' of COVID-19 misinformation, explained (nationalgeographic.com).*

6 *Roger C. Molander, Andrew Riddile, Peter A. Wilson, Strategic Information Warfare: A New Face of War, RAND, Research Published 1996, RAND, Accessed: 28 August 2024, URL: Strategic Information Warfare: A New Face of War | RAND.*

7 *Christopher H. Chin, et al, When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force, National Defense University Press,04 May 2023, Accessed: 28 August 2024, URL:When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force > National Defense University Press > News Article View (ndu.edu).*

8 *Brunetti-Lihach Nick, Information Warfare Past, Present, and Future, The Strategy Bridge, 14 November 2018, Accessed: 28 August 2024, URL: Information Warfare Past, Present, and Future (thestrategybridge.org).*

9 *Kazumi Naganuma, Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality, NIDS, 30 March 2021, Japan.*

10 *Ramjee Divya and Jensen Benjamin, Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs, Center for Strategic and International Studies (CSIS), 20 December 2023, Accessed: 28 August 2024, URL: Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs (csis.org).*

11 *Baruchin Rotem, How Modern Hackers Exploit Human Psychology With Cognitive Hacking, Cyabra, 05 August 2024, Accessed: 28 August 2024, URL: Everything You Need To Know About Cognitive Hacking (cyabra.com).*

[12] *Kwet Michael, Digital colonialism is threatening the Global South, Al Jazeera, 13 March 2019, Accessed: 28 August 2024, URL: Digital colonialism is threatening the Global South | Science and Technology | Al Jazeera.*

[13] *Jindal Divyanshu, The War On Conscience: India In The Age Of Cognitive Warfare, India Foundation, 2023, 07.*

[14] *Hicks Jacqueline, 'Digital colonialism': why some countries want to take control of their people's data from Big Tech, The Conversation,26 September 2019, Accessed: 28 August 2024, URL: 'Digital colonialism': why some countries want to take control of their people's data from Big Tech (theconversation.com).*

[15] *Congressional Research Service, Defense Primer: Information Operations (congress.gov), Updated 18 December 2018, 01.*

[16] *Whyte Christopher, Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, Journal of Cybersecurity, 14 September 2020, Accessed: 28 August 2024, URL: Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare | Journal of Cybersecurity | Oxford Academic (oup.com)*

[17] *Collins Liam and Cook Chaveso, PSYOP, Cyber, and Info War: Combating the New Age IED, Modern War Institute At West Point, 04 June 2021, Accessed: 28 August 2024, URL: PSYOP, Cyber, and Info War: Combating the New Age IED - Modern War Institute (westpoint.edu).*

[18] *C. A. Theohary, Defense Primer: Information Operations, Congressional Research Service,18 December 2018, Updated: 28 August 2024, URL: Defense Primer: Information Operations (congress.gov), 01.*

[19] *C. A. Theohary, Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues, Congressional Research Service, 17 March 2009, Accessed: 28 August 2024, URL: Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues (congress.gov), 28.*

[20] *Daniel Johnson, The real reason Ukraine's information war is so successful, Task & Purpose, 29 March 2022, Accessed: 28 August 2024, URL: The real reason why Ukraine's information war is so successful (taskandpurpose.com).*

[21] *The Select Committee On Intelligence, United States Senate on Russian active measures campaigns and interference in the 2016 U.S. Election, Report Of The Select Committee On Intelligence, Volume 2, 2016, Accessed: 28 August 2024, URL: Report_Volume2.pdf (senate.gov).*

[22] *Ramjee Divya and Jensen Benjamin, Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs, Center for Strategic and International Studies, 20 December 2023, Accessed: 28 August 2024, URL: Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs (csis.org).*

[23] *The Digital Forensic Research Lab, Undermining Ukraine: How Russia widened its global information war in 2023, Atlantic Council, 29 February 2024, Accessed: 28 August 2024, URL: Undermining Ukraine: How Russia widened its global information war in 2023 - Atlantic Council.*

[24] *Boot Max, Why the U.S. Ramped Up Its Information War With Russia, Council on Foreign Relations, 10 February 2022, Accessed: 28 August 2024, URL: Why the U.S. Ramped Up Its Information War With Russia | Council on Foreign Relations (cfr.org).*

[25] *Arjomand Noah, Information Laundering and Globalized Media — Part I: The Problem, Center For International Media Assistance, 20 August 2019, Accessed: 28 August 2024, URL: Center for International Media Assistance (ned.org).*

[26] *Sagar Pradip R., How China has unleashed a misinformation war on India, India Today, 18 October 2023, Accessed: 28 August 2024, URL: How China has unleashed a misinformation war on India - India Today.*

[27] *Shinji, China's Quest for Control of the Cognitive Domain and Gray Zone Situations,33.*

[28] *Shinji, China's Quest for Control of the Cognitive Domain and Gray Zone Situations,49.*

[29] *PIB, India dismantles Pakistani coordinated disinformation operation, PIB, 21 December 2021, Accessed: 28 August 2024, URL: Press Release:Press Information Bureau (pib.gov.in).*

[30] *Huminski Joshua, Deep Fakes: The Coming Infocalypse, Diplomatic Courier, 29 August 2020, Accessed: 28 August 2024, URL: Deep Fakes: The Coming Infocalypse (diplomaticourier.com).*

[31] *Ratiu Ramona, Securing the Future: Enhancing Cybersecurity in 2024 and Beyond, ISACA, 12 February 2024, Accessed 02 September 2024, URL:Securing the Future: Enhancing Cybersecurity in 2024 and Beyond (isaca.org)*

[32] *Clark Anthony, 3 Strategies for Ensuring the Security of Your Digital Infrastructure, ARIN, 27 October 2023, Accessed 02 September 2024, URL:3 Strategies for Ensuring the Security of Your Digital Infrastructure - American Registry for Internet Numbers (arin.net).*

[33] *Wuthnow Joel, China's New Info Warriors: The Information Support Force Emerges, Texas National Security Review, 24 June 2024, Accessed on: 05 September 2024, URL: China's New Info Warriors: The Information Support Force Emerges - War on the Rocks.*

[34] *Blannin Patrick, The Good Operation: Notes on a Whole-of-Government approach to National Security, Modern War Institute at Westpoint, 05 April 1028, Accessed: 05 September 2014, URL:The Good Operation: Notes on a Whole-of-Government approach to National Security - Modern War Institute (westpoint.edu).*

[35] *Panwar, Grey Zone Operations In The Infospace Dimension: Imperatives For India.*

[36] *Kick Jason, Cyber Exercise Book, Germany, MITRE, 11.*

[37] *Statements and Releases, Addressing the Collective Challenges of our Time: Implementing the U.S. Strategy to Prevent Conflict and Promote Stability, The White House, 01 April 2022, Accessed on: 05 September 2024, URL: Addressing the Collective Challenges of our Time: Implementing the U.S. Strategy to Prevent Conflict and Promote Stability | The White House.*