International Journal of Sociology and Political Science
www.sociologyjournal.in
Online ISSN: 2664-7745, Print ISSN: 2664-7737
Received: 15-04-2025, Accepted: 16-05-2025, Published: 31-05-2025
Volume 7, Issue 2, 2025, Page No. 35-38

Digital propaganda and national security: India's battle against disinformation

Dr. Charu Mathur
Associate Professor, Department of Political Science ARSD College, University of Delhi, Delhi, India

Abstract
Over the past decade, there has been a swift technological evolution, which has heralded an era that boasts about unrivalled connectivity and innovation in cyberspace. This has led to modifications and alterations in 'cyberspace dynamics.' As the internet, social media, or digital media become central to our lives, information warfare has quietly emerged as a major threat to a country's independence, internal peace, and social unity.

"In today's world, conflicts are not just fought on battlefields but also through messages, images, and false information." State and non-state actors are employing sophisticated information warfare tactics to undermine governments, sway public opinion, and create internal discord (Baloyi Errol, 2017). This study has tried to assess how numerous social and digital media channels, like Instagram, Telegram, Facebook, Twitter, and TikTok, are used strategically during wars and conflict. For a diverse democracy like India, which is rapidly advancing in the digital sphere, these challenges have grown increasingly urgent. India is facing challenges in the Information Warfare space regularly, be it concerning the collusive nature of transborder war and Hybrid Warfare, or the spread of radicalism and terrorist ideology (Bakshi B, 2018) [5].

Digital propaganda signifies all those manipulative uses of digital technology to achieve particular political and military goals by producing false and fake information to instill fear among the people of the opponent state and wean away more friends in the international arena. As information becomes an instrument or a weapon, India finds itself navigating a precarious landscape where state and non-state actors exploit digital tools to spread disinformation and destabilize internal harmony.

The issue discussed in this Article is important both academically and strategically. Recent incidents like the Terrorist attack on Pahalgam and 'Operation SINDOOR' resulted in national unrest in which disinformation played a crucial role. The agitation also highlighted the failure of security agencies to counter the wrong narrative. The discussion on information warfare focuses on key areas like national security, political stability, and social unity to provide a well-rounded understanding. Its main goal is to offer practical ideas for policymakers, civil society, and security agencies to create effective and timely strategies against information warfare. Making use of ideas like hybrid warfare, digital autonomy, and cognitive security in the Indian situation will also lead to better understanding of Political Science and International Relations. The campaign during Operation SINDOOR applied a wide range of means including public diplomacy, findings of research think tanks, public opinion surveys and mobilization of traditional and social media, to set up the correct narrative.

This paper aims to amplify India's ability to detect and counter misinformation and propaganda by improving monitoring systems and establishing quick response strategies. It will provide useful knowledge to policymakers on the impact of information warfare on elections, social harmony, and political governance. Additionally, it will suggest how to develop a strategic framework to integrate information security into national defence policies, ensuring a coordinated response to emerging threats. By raising public awareness and improving media literacy, the research aims to reduce vulnerability to false information and promote resiliency among citizens. Addressing these areas will strengthen India's resilience against information warfare, contributing to greater political and social stability.

However, most current research either looks at cybersecurity from a technical angle or views disinformation as a separate issue. There is still a major gap in examining information warfare in a way that connects it to India's unique context, specifically how it affects internal security and social harmony together. This study aims to fill that gap. The knowledge acquired will contribute to practical policy recommendations aimed at boosting India's ability to withstand information warfare. The aim is to offer to strengthen democratic institutions, maintain social harmony, increase citizens' resilience and protect national sovereignty from new information threats by suggesting a balanced strategy that combines legal, technical, and social solutions.

"World War III is a guerrilla information war with no division between military and civilian participation."

Keywords: Information warfare, hybrid warfare, disinformation, national security, misinformation

Introduction

'Information Warfare' has transformed the idea of information security by making information both the primary target and the main tool of conflict. Unlike traditional warfare fought on land, sea, air, or in space, this form of battle takes place in the virtual realm of information space, giving it a unique and modern dimension (Bakshi B, 2018) [5]. Information warfare has been a prominent topic in international security discussions. Misinformation, propaganda, and cyber strategies are tactically used to disrupt political systems and influence public perception. Like traditional war, Information Warfare is very powerful and can cause long-term damage. However, unlike the former, the latter is potentially bloodless, cost-effective, and not a military-specific phenomenon (Taddeo M, 2011) [20].

Information warfare is not only about spreading misinformation. But also shaping narratives with carefully curated propaganda. Former British PM Winston Churchill

said during Tehran Conference (1943), "In wartime, truth is so precarious that she should always be attended by a bodyguard of lies." Every side in war carefully guards information considered sensitive. But it goes far beyond protecting sensitive military or strategic information.

Information's influence on warfare appears so imminent that one wonders how "information warfare" differs from warfare itself (Libicki & Shapiro, 1999) [15]. Information Warfare emphasizes 'C3I – Command, Control, Communication and Intelligence'. During war, countries use propaganda to influence the national and international audience. Due to time constraints, aggressive tactics discredit unbiased information and sow doubt. Once it reaches social media platform, it has a deep impact on public consciousness, shaping beliefs and actions. Its impact lingers, influencing societies and creating both intended and unintended consequences (Fitzgerald & Brantly, 2017) [9].

Use of Information Warfare in Geopolitical Rivalries

'Information warfare involves targeting a state's information systems, processes, and resources to weaken its political, economic, and social structures.' The goal is to destabilise society through large-scale psychological influence or "mass brainwashing," ultimately pressuring the targeted state to act in favor of the aggressor's interests (Ajir and Vailliant, 2018) [2].

'Misinformation', usually being sensational in nature, spreads faster than facts. In tense situations like a war or an armed conflict, misinformation can travel like missiles- fast and destructive. In the era of live coverage, rumours can beat the speed of light.

"Additionally, being in the digital age, warfare transcends traditional battlegrounds. Alongside military operations, a fierce information war has been ongoing online. For instance, following the commencement of 'Operation SINDOOR', India found itself targeted by an aggressive campaign launched by Pakistan, full of lies and misinformation. Pakistan's social media handles, like Twitter became infested with coordinated efforts aimed at discrediting India. Trending Hashtags were #IndianFalseFlag, #PahalgamDramaExposed, #ModiExposed and others, which tried to show the world that the attack was planned by India itself. The aim was to distort the truth, mislead the global public and reclaim lost narrative ground through a storm of misinformation. However, India has been proactively responding and dissipating misinformation with facts, transparency, showcasing strong digital vigilance. Rather than reacting emotionally, a composed and methodical approach to information warfare was undertaken:

- **Highlighting operational success**: Operation SINDOOR's effectiveness was communicated with precision, focusing on strategic outcomes rather than sensationalism.

- **Discrediting sources**: Indian authorities have exposed the manipulation tactics used by Pakistan-based accounts, many of which are now under scrutiny by international social media platforms.

- **Promoting media literacy**: Campaigns to educate citizens on how to identify fake news have helped create a more resilient digital environment."

Information technology has become deeply integrated into modern societies, making it a potential tool for harming a nation's stability and security. Cyberattacks targeting critical information systems and infrastructure can increase tensions and even lead to full-scale war. (Colarik & Janczewski, 2012) [8].

Arquilla and Ronfeldt use the terms 'Cyberwar' and 'Netwar' in their article 'Cyberwar is Coming!'. According to them, "Cyberwar and Netwar revolve around information and communication matters. Through the deeper level, they are forms of war about knowledge; about who knows when, what, where and why, and how secure a society or military is regarding its knowledge of itself and its adversaries" (Arquilla, 1993) [3]. They argued that netwar can disrupt or modify what targeted people know or think. Netwar can influence the opinion of the public or elite, it can also involve propaganda and psychological campaigns or interfere with computer networks or databases to promote dissidents. They also stated that the information has set off as a strategic resource that can prove valuable and influential.

Digital Platform and Data Manipulation

Social media has become a key platform for spreading misinformation and carrying out propaganda campaigns, frequently utilizing doctored images and altered videos. The strategic use of disinformation as an instrument of war embitters international relations, creates distrust among the public towards its leaders and institutions, and tarnishes opposing political ideologies (Baloyi, 2024) [6].

Social media enables propaganda by amplifying narratives aligned with existing beliefs. Key players include true believers, a cyber team crafting targeted content, and automated bots boosting visibility. Together, they command trends using videos, memes, and fake news, influencing populations through coordinated efforts across social platforms, online news, and traditional media channels (Prier, 2017) [19].

Cyber operations have become a powerful tool for shaping public perception and influencing opinions. By manipulating online spaces, individuals can be exposed to propaganda without their awareness, often through misleading websites or deceptive content. False narratives can be amplified by artificially boosting certain information while suppressing others. Automated accounts can steer online discussions, making certain viewpoints appear more popular than they are. Additionally, leaked information—sometimes mixed with fabricated details—can be used to discredit opponents or create confusion. As traditional media gives way to unfiltered social media, misinformation spreads more rapidly, making it harder to distinguish truth from falsehood (Libicki, 2017) [14].

In today's highly connected and digital world, people are constantly exposed to online content, making them vulnerable to manipulated realities. Advanced technologies now allow for easy alteration of images, videos, and documents, enabling the creation and spread of fake news. Unlike traditional propaganda, perception management involves tailoring messages to influence public attitudes and behavior through interactive communication. Tactics such as distortion, fabrication, deception, conspiracy theories, and online harassment are often used in information warfare to shape opinions. Social media platforms like Instagram and 'X' accelerate the spread of unverified content, making perception management a powerful tool in the digital age (Babacan & Tam, 2022).

India's National Security and Information Warfare

In the journal article 'Challenges to Internal Security of India', Arunkumar and Sakthivel wrote "Perhaps no other country in the world confronts as many threats with as much intensity at the same time".

McAfee wrote the 2007 Annual Virtual Criminology Report, which said that, "international cyber spying would be the greatest danger to national security in 2008". It said that more than 120 countries were already on the web espionage bandwagon.

India's civilian institutions have their own firefighting agencies while the armed forces have their own insulated platforms to counter cyber-attacks. Unlike nuclear energy, a marked division between civilian and military use of cyberspace is difficult to establish (Arunkumar & Sakthivel, 2017) [4].

'Hacktivism', a blend of "hacking" and "activism," refers to the use of digital tools and techniques to support political or social causes. It often draws from the traditions of protest, resistance, and anti-globalisation movements. Hacktivists use these methods to raise awareness about issues, highlight conflicts, or promote specific messages online (Gawel, 2024) [10]. The 2020 Indian farmers' protest saw the rise of hacktivist groups such as Anonymous India and the Red Rabbit Team

Information operations activities in the propaganda category can cause political and societal division in a target country as they seek to influence public opinion and play on the vulnerabilities inherent to many states.

India's Policy and Challenges

'Indian policymakers have mostly ignored the problem of cyber-security. India lacks the strong cyber-security mechanisms needed to combat the rising threat of cyber-terrorism, of which India is a major victim.' (Naha, 2022) [17].

In addition, approved projects like the National Critical Information Infrastructure Protection Centre (NCIIPC) and National Cyber Coordination Centre (NCCC) of India have been formed. The Government has aimed at ensuring open, safe, trusted and accountable internet for its users. The Indian Computer Emergency Response Team (CERT-In) is a national agency for cybersecurity incidents. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) to ensure coordination amongst different agencies. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre

Establishing a CWD is the need of the hour to ensure a well-coordinated and future-ready approach to cyber defence. Modern militaries have enhanced their command and control systems through network-centric warfare, relying heavily on advanced information networks. As cyber threats grow more sophisticated, every nation must be prepared to defend against cyberattacks and, if necessary, carry out countermeasures. For India to effectively respond to such threats, there is a pressing need to establish a Cyber Warfare Doctrine that aligns with its core national principles. Such a doctrine should be rooted in three key areas: political, legal, and military. A well-founded CWD, built on these pillars, is essential to ensure long-term national preparedness and resilience in the digital age. Ministry of Electronics and Information Technology '(MeitY)' has notified 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Even though awareness about the dangers of information warfare is growing, there remains a lack of detailed academic research focused on how information warfare affects India across multiple dimensions - particularly the intersection of national security, political stability, and social harmony. We don't really know how disinformation spreads in the country's unique pluralistic and political landscape, or which legal, institutional, and educational tools work best to tackle these challenges. There's also a lack of research on how these threats shape public opinion, influence policy making, and impact the long-term strength of democratic institutions.

To effectively respond to information warfare, it is important to first understand the existing gaps in knowledge. To structure and plan successful policies it is pertinent to understand how Information warfare works in India. Recognising insights into the tactics, goals, and impact of such threats can help in improving education efforts, updating existing legal measures, improving counter measures and raising public awareness. As these challenges become more sophisticated and frequent, bridging these gaps is crucial not only for academic purposes but also for making informed decisions that support internal security. Through this method, the aim is to identify key patterns, understand their impact on India's security and society, and suggest practical steps that can help the country respond more effectively to these challenges.

The impact of information warfare on public opinion, political stability, and social harmony is challenging to measure.

The role of information warfare in India in amplifying the political incidents highlights major weaknesses in the country's information system, such as the spread of false information, fractured political division, and manipulation of public opinion. These issues are made worse by the absence of strong countermeasures and low media literacy and a lack of digital resilience among citizens. To tackle these challenges, India needs an all-inclusive strategy, which includes improving digital literacy, strengthening regulations for online platforms, encouraging collaboration between the government and tech companies, and raising public awareness about disinformation. A war is not just armed conflict for physical control of a geographical territory; it's also about shaping larger public opinion with carefully curated propaganda.

References

1. Abdyraeva C. Information Warfare Operations in the Cyber Domain. In The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends, 2020, 20–28.
2. Ajir M, Vailliant B. Russian Information Warfare: Implications for Deterrence Theory. Strategic Studies Quarterly,2018:12(3)70–89.
3. Arquilla J, Ronfeldt D. Cyberwar is Coming! RAND, 1993.
4. Arunkumar C, Sakthivel P. Challenges To National Security In India. World Affairs: The Journal of International Issues,2017:21(1):114–121.
5. Bakshi Bipin. Information Warfare: Concepts and Components. Information Warfare Concepts and Components,2018:5:178-185.
6. Baloyi Errol, Mahlasela Oyena, Siphambili Nokuthaba, Stegmann Mayan. Social Media as a Strategic

Advantage during Cyberwarfare: A Systematic Literature Review. International Conference on Cyber Warfare and Security,2024:19:19-25.
7. Biały B. Social Media—From Social Exchange to Battlefield. The Cyber Defense Review,2017:2(2):69–90.
8. Colarik A, Janczewski L. Establishing Cyber Warfare Doctrine. Journal of Strategic Security,2012:5(1):31–48.
9. Fitzgerald Chad, Brantly Aaron. Subverting Reality: The Role of Propaganda in 21st Century Intelligence. International Journal of Intelligence and Counterintelligence, 2017.
10. Gawel H. Hacktivism. Internet Policy Review, 2024, 13(2).
11. Kalita P. China could be instigating Manipur unrest: The Times of India, 2024.
12. Kohler Kevin. Estonia's National Cybersecurity and Cyberdefense Posture, 2020.
13. Kumar A, Anekant V. Challenges to Internal security of India (3rd ed.). McGraw-Hill Education (India) Private Limited, 2020.
14. Libicki MC. The Convergence of Information Warfare. Strategic Studies Quarterly,2017:11(1):49–65.
15. Libicki M, Shapiro J, marshall aW. Conclusion: the changing role of information in warfare. In z. M. Khalilzad & j. P. White (eds.), Strategic Appraisal: The Changing Role of Information in Warfare (1st ed., pp. 439–454). RAND Corporation, 1999.
16. Mint. India most targeted country by religiously motivated hacktivists, 2023.
17. Naha Alik. Emerging Cyber Security Threats India's Concerns and Options, 2022, 170-200.
18. Parmar SD. Cybersecurity in India: An evolving concern for national security. The Journal of Intelligence and Cyber Security, 2018.
19. Prier J. Commanding the Trend: Social Media as Information Warfare. Strategic Studies Quarterly,2017:11(4):50–85.
20. Taddeo Mariarosaria. Information Warfare: A Philosophical Perspective. Philosophy and Geography, 2011.
21. Tarapore A. Mitigating the risk of a China–India conflict. Australian Strategic Policy Institute, 2021. http://www.jstor.org/
22. https://www.academicapress.com/
23. https://www.livemint.com
24. https://timesofindia.indiatimes.com
25. https://www.researchgate.net/
26. https://www.theprint.in
27. https://www.rand.org
28. https://papers.academic-conferences.org/
29. https://orcid.org/