



CENJOWS

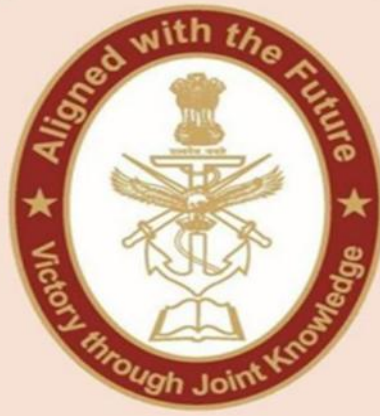
ISSUE BRIEF

IB/14/25

INDIA'S JOINT STRATEGY TO COUNTER PAKISTAN'S MALIGN PROPAGANDA DURING 'OPERATION SINDOOR'

MR CHANDER SHEKHAR

CENTRE FOR JOINT WARFARE STUDIES



CENJOWS

India's Joint Strategy to Counter Pakistan's Malign Propaganda during 'Operation Sindoor'.



Mr Chander Shekhar is an Associate Fellow at CENJOWS

Abstract

This issue brief explores as to how Pakistan's malign propaganda affects India and how India can counter this type of new emerging threat in the digital age, which developed following the Pahalgam terror attack in 2025. In peacetime and wartime both, information plays a crucial role in receiving the true and right message to the citizens of the nation. Malign Propaganda has drastically spread over social media networks during the 'Operation Sindoor', and it is part of an expansion of the security arena from traditional to nontraditional domains, while also sparking an information battle. It underscores the need to recognise "truth" as a strategic resource as it defends the cognitive sovereignty of the nation. Through a careful dissection of real-time responses, digital countermeasures and civil-military synergy, the brief reveals the operational and doctrinal depth of India's narrative defence architecture. The enemies try to divert the mind and try to destabilise the national peace. Pakistani media and other various agencies try to destabilise India through fake news. Operation Sindoor may well serve as a global model for future democracies confronting disinformation

threats. This paper highlights India's countermeasures against fake news through a joint and synergistic approach.

Introduction

Fake information on social media tries to shape the narrative by targeting a particular personality, organisation, state and country. Operation Sindoor was officially launched by the Indian Armed Forces on May 7, 2025, for targeting terrorist infrastructure and camps in Pakistan and Pakistan-occupied Jammu and Kashmir following the Pahalgam terror attack.¹ Soon after the launch of Operation Sindoor, there was a rapid increase in the spread of fake news in India from various sources.² Fake news has become one of the most potent threats to national integrity as it is increasingly reflected in social media platforms. In a digital age where a morphed video can trigger riots and a deepfake can derail military strategy, states must arm themselves with digital resilience. The aftermath of fake news on social media rapidly escalated against India³, disturbing national security. In response, we initiated a joint effort to counter the rising wave of hostile misinformation campaigns and to build digital resilience. The operation was designed with both defensive and offensive elements in the information spectrum and was executed by synchronising efforts of the armed forces, cyber intelligence units, civilian ministries and tech-sector allies. India's national security architecture has proven the value of cooperation and strategic vision in an era of multi-domain conflict, where threats change more quickly than boundaries.⁴



Figure 1: Fake news has circulated on social media. Source: PIB Fact Check Unit⁵

The importance of such a mission arose when intelligence agencies tracked disinformation patterns and behaviour targeting troop movements along the Western border, and Pakistan also attempted to divert the armed forces' minds through the social media platform. In one alarming case, Artificial Intelligence (AI) and Machine Learning (ML) generated audio mimicking the Indian Army Chief, falsely urging battalion retreats. While it was quickly exposed, it revealed the urgency of a consolidated framework to tackle such digital intrusions.⁶ Operation Sindoor was more than a countermeasure. It was a blueprint for future psychological and cyber conflict prevention. It's a turning point to counter Kashmir terrorism and redefine jointness not just in terms of physical operations but in the information and ideological space.⁷ Even Pakistani supporters in Bangladesh supported Pakistan in its attempts to spread disinformation to distract the minds of India. For example, a Maj Gen Fazlur's (retd) from Bangladesh circulated fake news suggesting that Bangladesh would attack the northeast region with the support of China if India launched a war against Pakistan.⁸ However, after cross verification, the Bangladesh Ministry of Foreign Affairs firmly refuted Maj Gen Fazlur's (retd) statement.⁹ This initiative reflects a broader evolution in India's strategic planning from merely countering and tackling kinetic threats to safeguarding public cognition. It integrates multiple layers of governance, technology and grassroots communication, offering an actionable model for other democracies confronting similar hybrid threats.

Cognitive Warfare in the Digital Age

Disinformation is no longer an accidental byproduct of a connected society; it is an engineered tool of psychological subversion. Countries such as Russia and China have institutionalised influence operations as a part of their warfighting strategies.¹⁰ India, faced with a complex security environment ranging from proxy terror, insurgency, to grey-zone tactics, had to respond with equal doctrinal seriousness. Operation Sindoor was the Indian response to "cognitive warfare," where the battleground is the perception of truth among its people.¹¹

The campaign applied cognitive load theory to develop rebuttals. Instead of dense official statements, Operation Sindoor crafted short explainer videos and infographics. This change in communication psychology helped ensure messages penetrated digital

fatigue and algorithmic walls. It also ensured misinformation fatigue didn't lead to apathy, a condition more dangerous than outrage.¹²

Rise of Joint Digital Command

The Joint Digital Commands formulated for countering malicious information and fake news represent a proactive and strategic evolution in national security and information warfare. For the first time, India operated with a real-time digital warfare cell under the Integrated Defence Staff (IDS).¹³ This ad-hoc Joint Digital Command (JDC) multi-agency, cross-sector digital task force or military unit is specifically designed to combine the capabilities of the tri-services' media wings, the Ministry of Defence's Cyber Security Operations Centre and strategic partnerships with CERT-IN and NIC.¹⁴ In Operation Sindoor, alerts were triggered within a few minutes of malignant information spikes on any social media platform. Artificial Intelligence and intelligence model classifiers rated content by potential national security impact, triggering escalated responses where necessary¹⁵ after full coordination with cybersecurity, intelligence, social media and tech platforms to ensure a unified approach to national and international response. Below, I have provided India's major cyber agencies to countering the fake propaganda and provide cybersecurity during the Operation Sindoor.

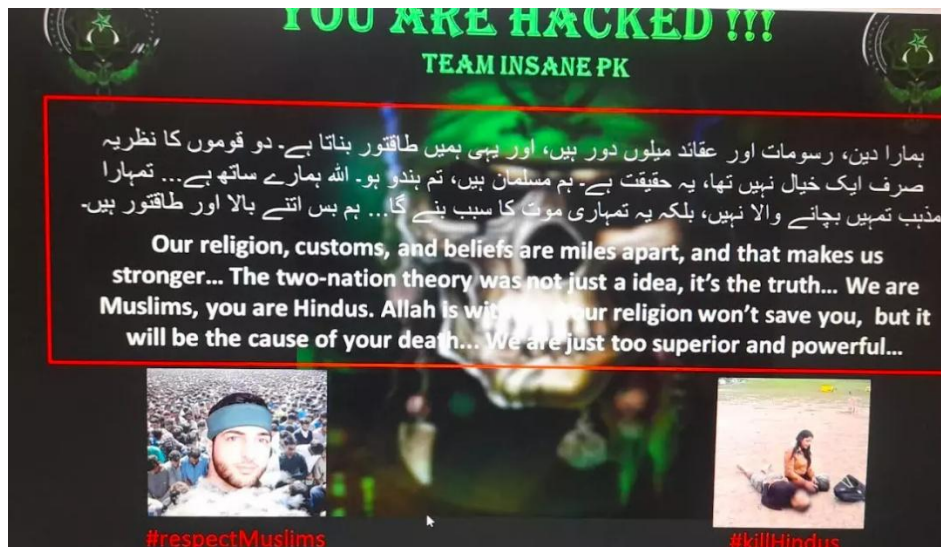


Image 2: Citizen visitors to the public site encountered a banner reading “YOU ARE HACKED, TEAM INSANE PK” above a disturbing image linked to April 22’s terror attack in Pahalgam, Jammu & Kashmir, alongside a photograph of Hizbul Mujahideen commander Burhan Wani. Source: <https://www.deccanchronicle.com>¹⁶

- **The Defence Cyber Agency (DCyA):** The Defence and Cyber Agency is India's tri-services agency within the Indian Armed Forces, jointly responsible for handling cybersecurity threats. DCyA operated as the key sentinel over India's cyber borders, aggressively detecting and neutralizing incoming threats, and enabling real-time response for coordination across air, land, and digital fronts. In the Operation Sindoor, DCyA actively participated and conducted many operations for the secure and sustain the situation during the conflict time because many cyber threats have raised after the operations Sindoor in India.
- **Indian Cybercrime Coordination Centre (I4C):** Cyberspace cuts across global boundaries, and handling Cybercrime requires coordination amongst different stakeholders in different jurisdictions at all levels. Cybercrime is one of the fastest-growing forms of transnational crime. The Indian Cybercrime Coordination Centre (I4C) comes under the Ministry of Home Affairs (MHA). During Operation Sindoor, I4C plays an important role in focusing on all the issues related to cybercrime. It provides the right information through coordination between various Law Enforcement Agencies and the stakeholders, I4C driving change in India's overall capability to counter Cybercrime in India.¹⁷
- **CERT-IN (Indian Computer Emergency Response Team):** The CERT-In deals with cybersecurity threats such as hacking and phishing to maintain the functioning. It strengthens the security-related defence of the Indian internet-related sector. The CERT-In has come under Section 70B of the Information Technology (Amendment) Act 2008. It functions as the national agency of India to perform the functions in the areas such as cyber data collection, analysis and dissemination of information on cyber incidents, cyber alert, issuing guidelines, advisories, vulnerability notes and white papers related to information security practices, procedures, preventions, response and many more.¹⁸

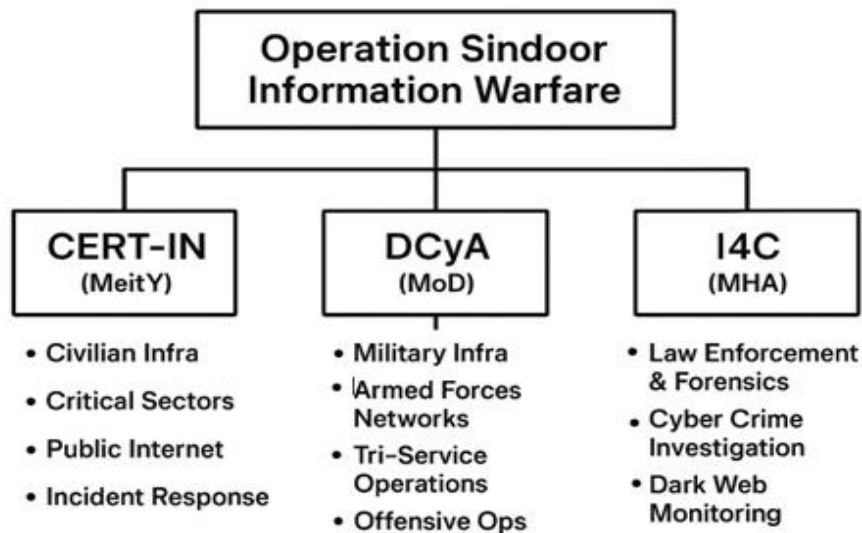


Figure 3: India's agencies for combating digital warfare. Source: Author

They all played as guardians of the Indian digital front and provided the perfect example of architects of integrated cyber defence to jointly counter the fake propaganda during Operation Sindoor. Joint Digital Command's success lies in its fusion model of military precision with having civilian interface. Private sector participation ensured the technological agility, while military doctrine guaranteed discipline in messaging. Jointness is a game-changer for India. This structure, if institutionalised, could serve as India's peacetime command for digital and perception warfare in any future operation.¹⁹

Why India Required Joint-Digital Command?

The border defines the physically delimited line between two nations. If the enemy attacks, it is responded to due to the capacity of the Indian Armed Forces and Paramilitary forces. Similarly, we must establish a joint digital command, as in the digital age, there are no physical boundaries, and both civilians & the military are being targeted by enemies. Therefore, a joint command must be created to have synergy to effectively respond to these threats. Wrong information on social media has increased public anxiety on both sides of the border, and information has no borders, so it is not easy to identify and stop it in the physical domain. Each nation has accused the other of such attacks. In today's digital age, the threat of misinformation and fake news has emerged as a key weapon in hybrid warfare, where hostile actors exploit all online

platforms to spread disinformation, create confusion and weaken public trust in democratic institutions during peacetime as well as during conflict time.²⁰ This new emerging challenge has been evident in efforts to manipulate information, divide societies, support radicalisation, disrupt public health responses and divert the minds of youth and masses. The same situation was seen in some incidents during the CAA riots, the COVID-19 pandemic and recently in the India-Pakistan dispute.²¹ The speed, scale and sophistication of these campaigns that are often powered by artificial intelligence, automated terror organisations and bots make them difficult to identify and detect for countermeasures through conventional means. Recognising these new risks, Operation Sindoor marked a significant step forward by demonstrating the strategic value of coordinated digital response mechanisms along with a set narrative through the joint press conference. The operation underscored the urgent need for a Joint Digital Command, a unified and agile entity capable of defending the information space, countering fake news in real time and safeguarding national security in an era where information is both a target and a weapon. In the disputed region of LOC, people became confused about the information, and they took some unnecessary actions due to fear.²²

Civil-Military Fusion Against Disinformation

In Operation Sindoor, the ability to mobilise civilian resources alongside the military was demonstrated. State education boards were roped in to send fake-news-awareness templates through schools, to make them understand about the right information and for remaining stay alert. The Ministry of Information and Broadcasting (MIB) plays an important role in creating vernacular content using regional influencers, while ex-servicemen organisations were trained to identify and report suspect digital narratives in border villages to counter disinformation to calm the situation.²³

This bottom-level approach of inclusion proved to be a critical strength. For instance, in Jammu's Rajouri district, a community radio campaign led by local teachers helped deconstruct misinformation that claimed Indian bunkers were being vacated and many more to stay calm in that disputed region.²⁴ The proactive community in the Jammu and Kashmir response helped maintain order and troop morale. Civil-military fusion thus ensured that India's ideological borderlines remained intact even during military pressures, ensuring everything was fine.²⁵

A Timeline of Tri-Service Briefings and Unified Press Conferences:

To counter the malign information and disinformation, the joint tri-services conducted many press conferences during Operation Sindoor, showcasing India's Synergised Information Warfare Approach. Press briefs are mentioned in the table below:

May 7, 2025	Operation Sindoor and Launched Announced	Launch of precision strikes on terrorist targets in POK and Pakistan, aimed at preventing escalation.	PIB India
May 8, 2025	MEA Briefing	Clarified that India did not target the Pakistan military; it focused only on terrorist camps and stations	MEA India
May 9, 2025	Tri-Service Joint Briefing	Satellite visual for proof of successful strikes and drone wreckage showing. Civilian safety emphasised.	DD News YouTube
May 10, 2025	MOD Technical Briefing (Army, Navy, Air Force)	Commodore R N Nair, Col Sofiya Qureshi, Wg Cdr Vyomika Singh explained op targets and rules of engagement.	PIB India / MEA Briefing Portal
May 11, 2025	Post-Strike MOD Wrap-up Briefing	Summarised operation results: no Indian casualties; highlighted deterrence value.	DD India
May 12, 2025	Tri-Service DGMOs conducted a press conference	Assured readiness, showed maps with verified targets, and confirmed mission success.	PIB India YouTube
May 13, 2025	PM Modi's Address to Armed Forces (from Adampur Airbase)	PM commended precision and synergy, which raised morale.	MyGov India
May 15, 2025	Joint India-Pak DGMO Confidence-Building Briefing	India confirmed it will maintain alertness but supports de-escalation and conveyed via official channels only.	MEA India

Figure 4: India's Joint Countermeasure during Operation Sindoor. Source: Author

Details of Fake News and Propaganda Undermining India's Internal Security via Social Media Platforms with a Focus on Pakistan-Backed Narratives:

The list of all malign information and coordinated fake propaganda generated and originating or amplified by Pakistani sources on social platforms like X, YouTube, Facebook and other platforms are mentioned in the succeeding paragraphs. Intended to destabilise India's national security, Pakistan incites communal tension to undermine public trust in national institutions. Through this data report, people can understand the degree of malicious information and the comparison between false and true information for better clarity in their minds.

- **Pakistan Shot Down an Indian Air Force Rafale (IAF) Jet during 'Operation Sindoor':** During the conflict, Pakistani media showed and circulated images claiming that Pakistan had successfully shot down an IAF's Rafale jet during Operation Sindoor. India's agencies clarified that the image and data were from a 2021 MiG-21 crash in Punjab, not a Rafale jet in Operation Sindoor.²⁶
- **Alleged Pakistani Strike on Delhi Airport through a short video:** A fake clip was circulated by Pakistani sources, claiming to show a Pakistani missile successfully striking Delhi's Airport. India's agencies clarified that the clip and data were fake, stating the footage was from a gas station explosion in Aden, Yemen, in August 2024²⁷. They had shown the strength of Pakistan through this clip.
- **Advanced Infographic Used: CNN Report on Indian Faces Heavy Losses:** They used the malicious information with CNN's logo and claimed that India suffered more economic loss as compared to Pakistan during Operation Sindoor. Again, Indian agencies confirmed the infographic was totally fake and was part of a propaganda campaign.²⁸
- **Artificial Intelligence (AI) Originated Fake News: Pakistan Deputy PM used and cites Non-Existent Article:** The Deputy Prime Minister of Pakistan, Ishaq Dar, cited a fabricated article from *The Daily Telegraph* praising the Pakistani

Air Force. Pakistan's own media outlet, *Dawn*, fact-checked and confirmed the article was fake.²⁹

- **Fake Alleged Destruction of Indian Army Post, Though Video:** The Pakistani Army destroyed an Indian Army post by the "20 Raj Battalion." The fake video was circulated by Pakistani social media, but PIB clarified that no such unit exists in the Indian armed forces, and the video was staged propaganda.³⁰
- **Indian Air Force Pilot Captured in POK:** Fake reporting by Pakistani social media, which claimed that an IAF female Air Force pilot was captured in POK. The Indian government confirmed that this was a fabricated story made by Pakistan with no factual basis.³¹
- **Shown Video Game Footage and Simulated Military Victory during Operation:** The fake Pakistani state media shared wrong footage from the video game Arma 3, presenting to the media that it was real military action, showing Pakistani air forces downing an IAF's jet. The International UK Defence Journal has confirmed the footage was from a video game.³²
- **Successful destruction of India's S-400 Air Defence System:** Again, Pakistani social media claimed that they destroyed India's S-400 air defence system. During the joint press conference, this information was countered stating that the system was intact and operational.³³ Pakistan spread fake propaganda to show victory over India.
- **High Explosion at Surat Port by Pakistan:** A Fake and malicious video claimed a Pakistani attack caused a high explosion at Surat port in Gujrat. The footage didn't match the Surat location and was an unrelated incident.³⁴

Navigating the Challenges to Counter the Malign Propaganda

During the Operation Sindoor, the country not only tackled physical threats but also the invisible warfare of malign propaganda from the side of Pakistan. For countering these narratives, swift, coordinated action, ground reality, resilience, and strategic communication were required to positively impact social media. By empowering communities with facts, strengthening digital vigilance and fostering unity, misinformation can be dismantled. In this battle of perception, clarity, fact, figure, and credibility are the strongest weapons. Some challenges faced by India during Operation Sindoor in terms of information war and malign propaganda are covered below:

- **Speed of Virality and Counter Response:** Actual event velocity at which misinformation spreads on platforms like WhatsApp, Telegram, Instagram, and X far outpaces institutional response mechanisms. By the time an official release clarification is made, fake narratives often reach millions of views, reactions and comments, hardening public perception. This asymmetry creates a reactive rather than proactive communication posture, allowing adversarial actors to dictate the narrative tempo.³⁵
- **Information Fatigue and Psychological Saturation in Opinions:** The overload of information leads to reduced attention spans, delayed reactions and in some cases, complete disengagement with the masses. Cognitive exhaustion makes individuals susceptible to confirmation bias and emotional manipulation by false narratives.³⁶
- **Issue of Linguistic and Cultural Penetration:** Countermeasures failed to account for India's vast and multiple linguistic diversity. Disinformation created in Urdu, Bhojpuri, Telugu, or Manipuri often went unchecked due to the lack of early monitoring tools in those dialects and local monitoring. Moreover, cultural references and local idioms used in disinformation campaigns resonated more effectively than generic rebuttals, reducing the credibility of official messages released by the government.³⁷

- **International Platform Compliance and Jurisdictional Barriers:** International digital social media platforms like X, YouTube and Meta platforms hesitated or delayed action on flagged content due to legal ambiguity about India's jurisdiction over their servers and data. This gap and loophole provided a time window for malicious content to trend and achieve virality before takedown requests were fulfilled.³⁸
- **Need to Update Legal and Doctrinal Gaps:** The India Information Technology Act, 2000,³⁹ needs to be updated as per the emerging challenges in its ability to tackle 21st-century information warfare and cybersecurity measures. There were no provisions for developing the latest algorithmic disinformation, memetic warfare, or cognitive manipulation through media. Enforcement agencies lacked clear guidelines on arrest, evidence collection and digital prosecution.⁴⁰
- **AI and Deep Fake Escalation:** They first make authentic accounts and during the vulnerable time activate to deploy synthetic media tools to produce hyper-realistic deep fake videos of political leaders, military officers and public figures. These videos were circulated during respected peak hours to manipulate public emotions affecting minds. Detection tools were often slower, requiring human verification due to limitations in automated authenticity checks.⁴¹
- **Foreign Amplification of Fault Lines:** Pakistan-based bot organisations, Chinese APT groups, and other foreign actors masqueraded as Indian citizens online, injecting divisive content on caste, religion and regional identity. They leveraged polarising hashtags and exploited existing grievances, often achieving viral traction through micro-targeting and paid trends, to highlight the fake information.⁴²
- **Scarcity in Media Credibility and International Reach:** Our response to global media narratives has been slower than required. Before we could counter false claims, distorted inputs had already been amplified by various agencies across international media networks. Pakistani research agencies and scholars had published or released pre-planned papers on targeting

Operation Sindoor. These changed the views, with biased and misleading information through fake media channels, as to change the perspective of targeting India's image.⁴³ These types of negative efforts are part of a broader strategy to change the mindset of global media stakeholders and build false narratives at the international level. Pakistan is a terrorism-based country, as Pakistan has the 2nd rank in the global terrorism index report as of 2025.⁴⁴

Recommendations

- **Real Time Monitoring and Digital Quick-Reaction Units (DQRUs):** To response in the real time and close the time gap between virality and response, India need to be established dedicate DQRUs within the Ministry of Home Affairs and the Ministry of Defence, with the help of the Ministry of Information & Broadcasting, to upload the information on time. These units are empowered to detect emerging trends on media, initiate takedown notices and publish counter-narratives within 10–15 minutes of a fake item going live. Trained analysts, cyber forensic teams and social media experts worked in real-time coordination.
- **Language and Sentiment-Aware AI Engines:** Defence and security Artificial Intelligence (AI) models were retrained using datasets that included 16 official languages as well as other local slang and emotion recognition cues. This model helped the system detect not just the factual inaccuracy of a post but also its sentiment polarity, anger, fear, and sarcasm to allow tailored counter-responses. These engines were integrated with social listening tools and telecom surveillance units in all districts.⁴⁵
- **Develop Memetic Warfare Cells:** Identifying and recognising the power of memes, satirical videos, and short emotional clips need to be created. During Operation Sindoor, there was a need to establish creative cells composed of cultural experts, meme-makers and digital storytellers. Their task should be to produce highly shareable content that emotionally resonates with local populations, especially for youth, while subtly debunking hostile narratives during dispute time.

- **Joint Fact-Check Battalions/Units with Civil Society:** The government needs to develop a programme for increasing credibility through partnerships with independent fact-checkers, media houses, retired intelligence officers and tech-savvy veterans. These battalions/Units need to work 24x7, sharing verified information via dashboards, SMS alerts and radio broadcasts. The collaborative model earned higher public trust than isolated government statements.
- **Legislative Overhaul:** The outdated IT Act needed to be updated by the new Digital India Act, which specifically categorised cognitive attacks, deepfake production and bot-driven malicious information as criminal offences. Provisions included fast-track courts for cybercrime, penalties for platform non-compliance and protective clauses for whistleblowers in the narrative space.
- **Workshops for Counter Propaganda:** To address the counter propaganda, we need to conduct workshops across schools, military academies and government authorities as well as in local societies. These modules should focus on digital hygiene and sanitation, recognising manipulated information, emotional regulation during information storms and tools for validating online content. Local influencers and micro bloggers need to be incentivised to spread digital literacy.

The One-week trend of Fake News and Real News during ‘Operation Sindoor’ From 07-05-2025 to 14-05-2025

As the Open-source AI data highlighted the information of Operation Sindoor through a graphical representation, it also generated a graph through its own data-based network and the information landscape from 07-05-2025 to 14-05-2025. If we check the one-week open trend on the AI Model of fake news, it represents the three lines which show the fake news in yellow, real news updates in orange and fact checks in pink colour.

Artificial Intelligence (AI) represents the flow of data, and checks resulted in a spike in fake news immediately after the operation began.⁴⁶ This trend highlights India's effective counter-disinformation joint strategy, where timely press briefings and

coordinated agency responses helped counter the misinformation and maintain narrative control with India. This data was collected automatically through the Open network analysis, and AI has generated this graph, so that it is a clear representation of India's efforts to counter Pakistan-based malign Propaganda and fake news.⁴⁷ It is the answer to the fake news, which harms national security, and real news updates are used for countermeasures to safeguard India's narrative. Fact-checkers are quite slow, but it helps to take dependable action against fake news data.

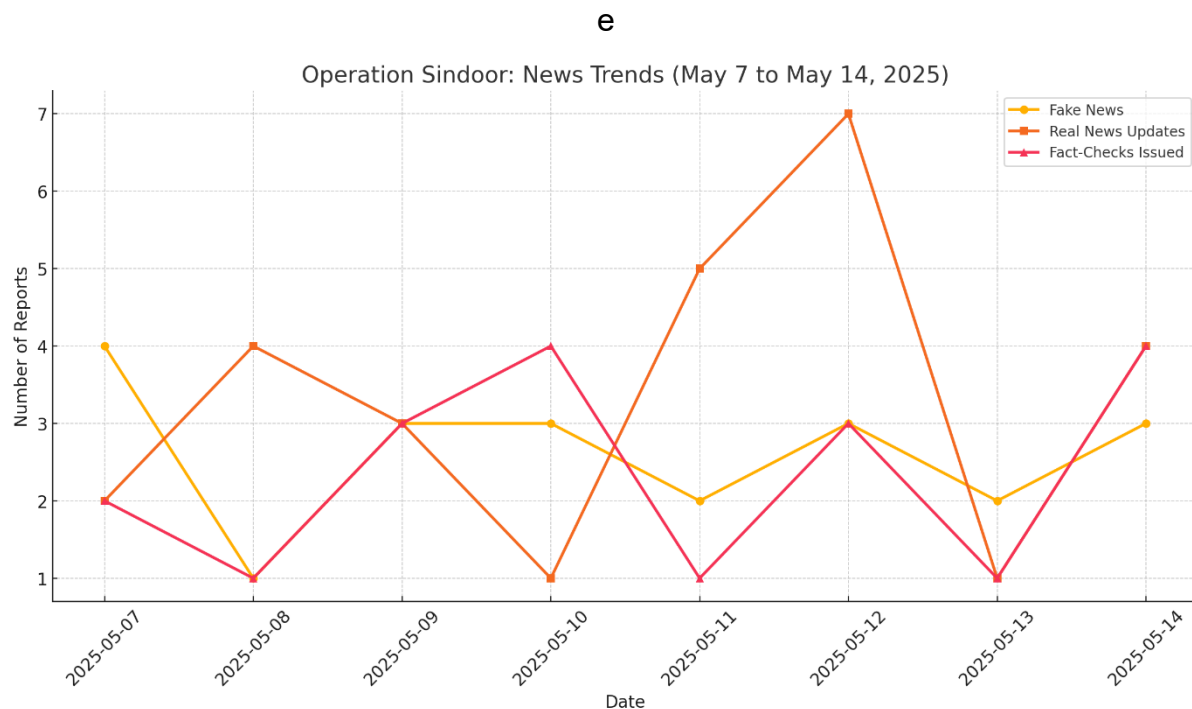


Figure 5: One Week of Fake News Information Graph. Source: AI

Conclusion

DCyA, I4C and CERT-IN played the major role in counteracting and neutralising the cyber threats and securing the digital network of India. The other fact-checker units also played a major role in Operation Sindoor because India's Operation Sindoor is not just a military action, but India's frontal assault against terrorist acts. India's Joint Strategy to Counter Pakistan's Malign Propaganda during 'Operation Sindoor' set the remarkable example of synergy and a joint warfare approach in the digital age. In the multiple warzone situation, India maintained internal peace. Through joint coordination, digital strategies and a nationalist ideological approach, India created a template for the modern narrative generation. India's joint efforts towards Operation

Sindoor required a greater preparedness to increase the credibility in the world news, for which we need to build resilience in the social media network.

Disclaimer

The views expressed in this monograph are solely those of the author and do not necessarily reflect the opinions or policies of CENJOWS. The author affirms that this work is an original piece of scholarly research, has not been published or submitted for publication elsewhere (in print or online), and that all data, facts, and figures cited are appropriately referenced and believed to be accurate to the best of the author's

Endnotes

¹ Press Information Bureau (PIB), “Operation Sindoor Launched by Indian Armed Forces,” May 7, 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2127370>.

² “Social Media Platforms Buzz with high Fake Posts on Operation Sindoor,” *The Economic Times*, May 9, 2025, <https://economictimes.indiatimes.com/news/india/social-media-platforms-buzz-with-fake-posts-on-operation-sindoor/articleshow/120969228.cms>.

³ Fake News Alert: Government Fact-Checks Pakistani Propaganda on Operation Sindoor,” *The Times of India*, May 10, 2025, <https://timesofindia.indiatimes.com/india/fake-news-alert-government-fact-checks-pakistani-propaganda-on-operation-sindoor/articleshow/120992221.cms>.

⁴ Press Information Bureau (PIB), “Operation Sindoor: Multi-Domain Strategy Against Hybrid Threats,” May 10, 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129453>.

⁵ <https://x.com/PIBFactCheck/status/1920455206481113205>

⁶ “Fake Audio Mimicking Army Chief Sparks Panic,” *The Economic Times*, May 9, 2025, <https://economictimes.indiatimes.com/news/india/social-media-platforms-buzz-with-fake-posts-on-operation-sindoor/articleshow/120969228.cms>.

⁷ International Centre for Counter-Terrorism, “Operation Sindoor: A Turning Point for India in Addressing Terrorism in Kashmir,” May 2025, <https://icct.nl/publication/operation-sindoor-turning-point-india-addressing-terrorism-kashmir>.

⁸ “Ex-Maj Gen Fazlur’s Remarks on India Personal: MoFA,” *New Age Bangladesh*, May 11, 2025, <https://www.newagebd.net/post/foreign%20affairs/263805/ex-maj-gen-fazlurs-remarks-on-india-personal-mofa>.

⁹ “Moffa, Denies Bangladeshi General’s Claims about Attack Plans,” *Bangladesh Sangbad Sangstha (BSS)*, May 11, 2025, <https://www.bssnews.net/news/269054>.

¹⁰ Var India, “Cognitive Warfare in the India-Pakistan Conflict: The Invisible Battlefield of 2025,” May 21, 2025, <https://www.varindia.com/news/cognitive-warfare-in-the-india-pakistan-conflict-the-invisible-battlefield-of-2025>.

¹¹ Centre for International and Homeland Security (CIHS), “India Needs Cognitive Warfare Plan,” May 14, 2025, <https://cihs.org.in/india-needs-cognitive-warfare-plan/>.

¹² Times of India, “‘Yachna Nahin, Ab Rann Hoga’: How Army Used Powerful Music and Visuals to Deliver Their Message Post Operation Sindoor,” May 25, 2025, <https://timesofindia.indiatimes.com/india/yachna-nahin-ab-rann-hoga-how-army-used-powerful-music-and-visuals-to-deliver-their-message-post-operation-sindoor/articleshow/121380656.cms>.

¹³ Press Information Bureau(PIB), "Operation SINDOOR: Forging One Force," May 18, 2025, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129453>.

¹⁴ Operation Sindoor: CERT-In Boosts Cyber Defences Across Critical Indian Sectors Amid DDoS Surge," NPAV Blog, May 12, 2025, <https://blogs.npav.net/blogs/post/operation-sindoor-cert-in-boosts-cyber-defences-across-critical-indian-sectors-amid-ddos-surge>

¹⁵ "Operation Sindoor: CERT-In Issues Advisory on DDoS Threats to Critical Sectors After Pahalgam Terror Attack," Money control, May 7, 2025, <https://www.moneycontrol.com/technology/operation-sindoor-cert-in-issues-advisory-on-ddos-threats-to-critical-sectors-after-pahalgam-terror-attack-article-13016041.html>.

¹⁶ <https://www.deccanchronicle.com/nation/pak-hackers-deface-army-college-of-nursing-website-1875152>

¹⁷ Ministry of Home Affairs, Government of India. *Indian Cyber Crime Coordination Centre (I4C)*. Accessed June 9, 2025. https://www.cybercrime.gov.in/Webform/Crime_Statistics.aspx

¹⁸ Indian Computer Emergency Response Team (CERT-IN). *Indian Computer Emergency Response Team*. Ministry of Electronics and Information Technology, Government of India. Accessed June 9, 2025. <https://www.cert-in.org.in>

¹⁹ "Operation Sindoor: Jointness Was the Game Changer," India Today, May 23, 2025, <https://www.indiatoday.in/magazine/up-front/story/20250602-operation-sindoor-jointness-was-the-game-changer-viewpoint-by-it-gen-vipul-shinghal-2729365-2025-05-23>.

²⁰ "India Battles Disinformation War After Successful Operation Sindoor," *The Times of India*, May 10, 2025, <https://timesofindia.indiatimes.com/india/india-battles-disinformation-war-after-successful-operation-sindoor/articleshow/120985948.cms>.

²¹ Sedova, Katerina, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan. "AI and the Future of Disinformation Campaigns." *Centre for Security and Emerging Technology*, Georgetown University, 2021.

²² Operation Sindoor: Here Are Key Takeaways from DGMOS' Press Conference," *Business Standard*, May 12, 2025, https://www.business-standard.com/external-affairs-defence-security/news/operation-sindoor-key-takeaways-from-dgmos-press-conference-125051100704_1.html

²³ Press Information Bureau(PIB), "Operation Sindoor: Pakistan's False Propaganda Debunked by I&B Ministry's Fact Check Unit," *The New Indian Express*, May 7, 2025, <https://www.newindianexpress.com/nation/2025/May/07/operation-sindoor-false-propaganda-by-pakistan-debunked-by-ib-ministrys-fact-check-unit>.

²⁴ Operation Sindoor: Govt Debunks Claims of Suicide Attack at Army Brigade in Rajouri," *Firstpost*, May 9, 2025, <https://www.firstpost.com/india/operation-sindoor-india-pakistan-air-strikes-13886873.html>.

²⁵ Rouf Bhat and Syeda Afshana, "Fake News in Kashmir: A Case Study," *Research Review International Journal of Multidisciplinary* 4, no. 3 (2019): 502–506.
https://www.researchgate.net/publication/333016835_Fake_News_in_Kashmir_A_Case_Study

²⁶ Press Information Bureau (PIB). "Did Pakistan shoot down Rafale jet during Operation Sindoor? PIB fact check says no." *The Times of India*, May 8, 2025. [Did Pakistan shoot down Rafale jet during Operation Sindoor? PIB fact check says no | India News - The Times of India](#)

²⁷ Press Information Bureau (PIB). "PIB Fact Checks Fake Video Claiming Pak Strike On Delhi Airport." *YouTube*, May 9, 2025. [India-Pakistan War | PIB Fact Checks Fake Video Claiming Pak Strike On Delhi Airport | WION](#)

²⁸ Press Information Bureau (PIB). "Fact check: Govt debunks fake infographic about Indian losses in Op Sindoor." *Business Standard*, May 12, 2025 [Fact check: Govt debunks fake infographic about Indian losses in Op Sindoor | External Affairs & Defence Security News - Business Standard](#)

²⁹ NDTV. "Pak Minister Ishaq Dar Cites Fake News To Praise Air Force, Gets Fact-Checked At Home." *NDTV*, May 16, 2025. [Operation Sindoor, India-Pakistan Tensions: Pak Minister Ishaq Dar Cites Fake News To Praise Air Force, Gets Fact-Checked At Home](#)

³⁰ Press Information Bureau (PIB). "PIB fact check debunks fake video alleging Indian post destroyed by Pakistani Army." *The Economic Times*, May 9, 2025. [The PIB fact check debunks fake video alleging Indian post destroyed by Pakistani Army - The Economic Times](#)

³¹ Press Information Bureau (PIB). "Entry to airports banned, ATMs closed, Indian Air Force's Female pilot captured and 2 other such news going viral; government says fake news." *The Times of India*, May 9, 2025.

³² Allison, George. "Pakistani Govt shares game footage as real military action." *UK Defence Journal*, May 9, 2025. [2025 India–Pakistan conflict - Wikipedia](#)

³³ Press Information Bureau (PIB). "PIB Fact Check debunks false claims made by Pakistan." *YouTube*, May 9, 2025. [Stolen - Official Trailer | Prime Video India](#)

³⁴ Press Information Bureau (PIB). "PIB Fact Check debunks false claims made by Pakistan." *YouTube*, May 9, 2025. [PIB Fact Check unit has debunked false claims made by Pakistan | DD India](#)

³⁵ Mohamed R. Shoaib et al., "Deepfakes, Misinformation, and Disinformation in the Era of Frontier AI, Generative AI, and Large AI Models," *arXiv preprint*, November 29, 2023, <https://arxiv.org/abs/2311.17394>

³⁶ Johnny Botha and Heloise Pieterse, "Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security," *International Conference on Cyber Warfare and Security*, 2020,

<https://www.researchgate.net/publication/341454354> Fake News and Deepfakes A Dangerous Threat for 21st Century Information Security.

³⁷ Singhal, Srishti, Kruthi Shah, and Ponnurangam Kumaraguru. "SpotFake+: A Multimodal Framework for Fake News Detection in Low-Resource Languages." *arXiv preprint arXiv:2102.11276*, 2021. <https://arxiv.org/abs/2102.11276>.

³⁸ Policy Circle. "Safety or Censorship: India's Social Media Regulation Dilemma." *Policy Circle*, March 2025. <https://www.policycircle.org/policy/indias-social-media-regulation-dilemma/>.

³⁹ Blythe, Stephen E. "A critique of India's Information Technology Act and recommendations for improvement." *Syracuse J. Int'l L. & Com.* 34 (2006): 1.

⁴⁰ Aseem Chandra Paliwal and Afkar Ahmad, "Emerging Technologies and Future Challenges in Indian Cyber Law," *ResearchGate*, January 18, 2024. <https://www.researchgate.net/publication/377473599> EMERGING TECHNOLOGIES AND FUTURE CHALLENGES IN INDIAN CYBER LAW.

⁴¹ Ravuri, S., & Vinyals, O. (2023). "Warning: Humans cannot reliably detect speech deepfakes." *Proceedings of the National Academy of Sciences*, 120(30), e2300421120. <https://doi.org/10.1073/pnas.2300421120>

⁴² Press Information Bureau. "PIB Debunks Pakistan Misinformation Campaign Against India: The Lies & the Real Truth." *The Economic Times*, May 9, 2025. <https://m.economictimes.com/news/india/pib-debunks-pakistan-misinformation-campaign-against-india-the-lies-the-real-truth-heres-what-you-need-to-know/articleshow/120986838.cms>.

⁴³ Janjua, Raja Abdul Ahad. "FOUR DAYS TO THE BRINK: THE 2025 INDIA-PAKISTAN AIR WAR." *Available at SSRN* 5252595 (2025).

⁴⁴ Institute for Economics & Peace. *Global Terrorism Index 2025: Measuring the Impact of Terrorism*. Sydney: Institute for Economics & Peace, March 2025. <https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf>.

⁴⁵ Government of India. *Defence and Security AI Integration Report*. Ministry of Home Affairs, Ministry of Defence, and Ministry of Information & Broadcasting. Accessed June 13, 2025. <https://www.example.gov.in/defai2024.pdf>.

⁴⁶ **Press Information Bureau (PIB) – Fact Check Division**
Press Information Bureau. "PIB Fact Check Archive: May 2025." *Government of India*. <https://pib.gov.in/factcheck.aspx>.

⁴⁷ **Ministry of Information and Broadcasting (MIB)**
Ministry of Information and Broadcasting. "Daily Media Monitoring Brief: Operation Sindoor (May 2025)." *mib.gov.in*, Government of India. <https://mib.gov.in>.