

Disinformation and Misinformation During Operation Sindoor

Shuvam Sharma¹, Dr. Ranjan Sharma²

¹ICSSR Doctoral Fellow, Department of National Security Studies, Central University of Jammu, J&K - 181143,

²Assistant Professor, Department of Strategic and Regional Studies, University of Jammu, J&K

Abstract

During the India-Pakistan conflict of May 2025, modern warfare extended beyond conventional tactics, with nations using armed drones and missiles against each other. Simultaneously, disinformation was used as a weapon in the digital realm. This study examines the disinformation and misinformation campaigns conducted by Pakistan against India during this conflict, arguing that in the digital age, control over narratives is as critical as physical combat.

The study reveals that Pakistan launched a coordinated information war across various social media platforms. The tactics included using fake images, AI-generated content, old videos, and even video game footage to create false narratives and shape perceptions. While India's initial digital response was reactive, it quickly adapted with a strategy of proactive transparency and centralized information control. However, the conflict also exposed India's vulnerabilities to internal divisions, the weaponization of public statements, and the misrepresentation of remarks made by leaders. The paper concludes that the conflict underscores the urgent need for a comprehensive national strategy for India to counter information warfare.

Keywords: Information Warfare, Propaganda, Media, National Security, Counter-Narrative

INTRODUCTION

The terrorist attack targeting tourists in Pahalgam, Jammu and Kashmir (J&K), on April 22, 2025, resulted in the loss of 26 civilian lives. This incident immediately escalated tensions between India and Pakistan, prompting both nations to mobilize their military forces. In response to the attack, India subsequently launched "Operation Sindoor" on May 7, 2025. In the midnight of 6 - 7th May, the Indian armed forces struck nine terrorist launch pads across Pakistan and Pakistan-occupied Jammu and Kashmir (PoJK). After the attack, India announced that its response was deliberate, precise, and strategic, without crossing the international border (IB) or the Line of Control (LoC) (M. GoI, 2025). Indian armed forces struck terrorist infrastructure in Pakistan, this strategic move significantly heightened tensions between the two nuclear-armed neighbor states. Pakistan retaliated for the strike with ceasefire violations along the IB and LoC in Poonch, Rajouri, Baramulla, Kupwara, and Jammu, launching indiscriminate shelling on civilian areas that resulted in considerable loss of life and property. This was followed by a series of missile and drone attacks across J&K, Punjab, Rajasthan, and Gujarat, including both military and civilians installations. Indian armed forces swiftly neutralized these threats using air defence systems and responded with aggressive counterattacks. A ceasefire was agreed upon

between the two nations on 10 May and took effect at 1700 hours on the same day (GoI, 2017). However, the conflict was not limited to conventional physical battlegrounds. In this digital era, warfare has expanded into a complex “5th dimension of conflict”, the information domain (Bakshi, 2018). This new battlefield is pervasive and continuous, with information superiority emerging as a decisive factor in conflict. The “battle of the mind” is increasingly fought over digital media, making the security of our “infospace” critically important. The flow and storage of information have rapidly shifted from traditional media to digital forms, diminishing the relevance of print, radio, and television. Consequently, physical security measures are no longer sufficient to protect critical infrastructure from digital manipulation and disruption. Information security must be viewed through a dual lens; this involves taking aggressive action against an adversary’s information while simultaneously securing one’s own. The battle of digital information is unique in its permeability to hostile attacks, often with a sense of anonymity (Bakshi, 2018).

During the conflict, Pakistan launched a coordinated information war against India, flooding social and mainstream media with fake news, AI-generated clips, and mislabeled war footage, all disseminated through mainstream media as well as social media platforms including YouTube, Instagram and X. The primary objective of this digital assault was to sow confusion, distort the reality of India’s military operations, and manipulate international perceptions. This study will analyze the various forms and campaign of misinformation and disinformation spread during operation Sindoor, also examining their impact and addressing the effects of cognitive warfare. By analyzing relevant documents and media sources, the study aims to conceptualize the specific forms of information warfare used during conflict.

1. Research Methodology

This study employs a qualitative, document-analysis methodology to investigate the phenomenon of disinformation and misinformation during Operation Sindoor (May 6–10, 2025). The research utilizes a systematic framework to analyze content and identify the forms of information warfare employed by Pakistan against India during the conflict. The study is based on primary and secondary data, which were collected from diverse channels spanning the official, mainstream, and digital media spheres. The time frame for collection focuses on the period immediately preceding, during, and following Operation Sindoor (April 22, 2025, to September 2025).

Conceptual and Theoretical Framework

The conceptual framework of this study situates Operation Sindoor within the broader domain of information warfare and its subcategories: misinformation, disinformation, and malinformation. The framework integrates theories of cognitive warfare (Reding & Wells, 2022; Yu & Ho, 2022) and inoculation theory (Katharina Kiener-Manu, 2019) to explain the mechanisms of information manipulation and its societal consequences.

Core Constructs

Information warfare (IW): is a modern component of conflict that has evolved with technology, enabling faster and wider dissemination of information (Bingle, 2023). Despite its acknowledged importance, there is no single, universally accepted definition of IW. The term’s basic elements are highly debatable, with some experts viewing “information” quantitatively as raw data, while others see it qualitatively as the ideas or narratives that unite groups. Likewise, views differ on whether IW applies to conventional state-on-state warfare, irregular warfare, or a blend of both (Bingle, 2023).

According to the U.S. Department of Defense, IW is the integrated use of “Information Related Capabilities” to influence, disrupt, or usurp an adversary's decision-making while protecting one's own.

This occurs within the “Information Environment,” which is divided into three parts:

1. Physical: The tangible infrastructure, such as command and control systems and key decision-makers.
2. Informational: The methods for collecting, processing, and disseminating information.
3. Cognitive: The minds of individuals who receive, transmit, and respond to information (Bingle, 2023).

The U.S. Air Force and Army take a more nuanced approach, defining IW as a way to affect human behavior rather than just technical capabilities. The Air Force, for instance, sees all its actions from social media posts to the presence of an armed aircraft, as a form of communication that can shape an adversary's decision-making (Bingle, 2023). The Army also balances quantitative and qualitative views, but with a stronger focus on people and interpersonal contact (Bingle, 2023). NATO defines IW as an operation to gain an information advantage by controlling one's own information space, protecting access to it, and disrupting the opponent's information systems and flow (NATO, 2020). The primary goal of IW tactics, such as disinformation and propaganda, is to alter a target's perception to achieve a desired outcome (Katharina Kiener-Manu, 2019). Overall, IW is understood as the collection, manipulation, and distribution of information to gain a strategic advantage, disrupt decision-making, and erode trust in institutions.

In recent years, interest in information warfare has grown considerably, especially in light of recent conflicts such as those between Russia and Ukraine, Israel and Iran, and India and Pakistan. Nations are increasingly striving to advance their own narratives, both domestically and internationally, by leveraging state-controlled traditional media alongside social media platforms.

The Role of Cyber warfare

Cyberspace and emerging technologies have become critical domains for information warfare. This not only includes direct cyber attacks aimed at dismantling an opponent's information infrastructure but also encompasses social cyber attacks, commonly referred to as cognitive warfare. These attacks aim to shape specific worldviews that align with the objectives of the aggressor. The magnitude of this threat has led some experts to categorize “cyber-enabled information warfare” as an existential risk, with potential consequences comparable to those of nuclear war and climate change (Nataliya Stepanova & Ross, 2023). While misinformation itself is not a novel phenomenon, its influence has been exponentially intensified by social media platforms, which facilitate the rapid and widespread dissemination of false information (Nataliya Stepanova & Ross, 2023).

Cognitive Warfare

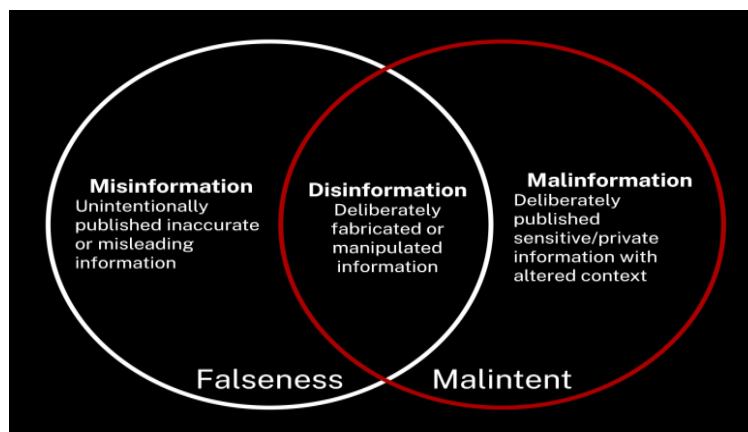
Cognitive warfare is a strategic effort to influence perceptions and behaviors by exploiting information and disinformation (Reding & Wells, 2022; Yu & Ho, 2022). While similar to IW, which primarily uses information to disrupt an adversary, cognitive warfare focuses on influencing how individuals and the public evaluate an issue or event. It operates in the cognitive domain, using a combination of information, misinformation, and disinformation to achieve social influence (Yu & Ho, 2022).

Misinformation: Cambridge Dictionary defined term misinformation as “wrong information, or the fact that people are misinformed”. According to the American Psychological Association (2025),

misinformation refers to false or inaccurate information, often resulting from errors in conveying facts. Menicocci et al. (2024) further clarify that misinformation refers specifically to “false or inaccurate information shared unintentionally.” The United Nations High Commission for Refugees similarly describes misinformation as false or inaccurate information, also providing examples such as rumors, insults, and pranks (UNHCR, 2022). Whereas, Polger (2021) characterizes misinformation as “unintentional mistakes,” which may include inaccurate photo captions, dates, statistics, translations, or instances where satire is misinterpreted as factual. This type of erroneous information is accidental and not intended to be harmful. United Nations refers misinformation to the accidental dissemination of inaccurate information (United Nations, 2021).

Disinformation: The term disinformation lacks a universally accepted definition, as its meaning is shaped by diverse contexts such as public health, electoral processes, and armed conflicts (United Nations, 2021). The American Psychological Association (2025) defines it as false information intentionally presented to mislead by deliberately misstating facts. It is fundamentally characterized as the deliberate creation and distribution of false information with the intent to harm, manipulate, or generate profit (Karami et al., 2021). Disinformation often involves malicious content, including hoaxes, spear phishing, and propaganda, which can spread fear and suspicion (UNHCR, 2022). It can also manifest as fabricated audiovisual material or the intentional spread of conspiracy theories and rumors (Polger, 2021). Both state and non-state actors can use disinformation, negatively impacting human rights, undermining public policy, and escalating social tensions during conflicts and emergencies (United Nations, 2021).

Malinformation: The term malinformation refers to genuine information that is shared with malicious intent to cause harm (Polger, 2021). It is truthful content that is often deliberately taken out of its original context, or a private detail released without consent, with the sole purpose of attacking an individual, group, or country. Examples include publishing private information like “revenge porn” or exaggerating factual content for propaganda purposes (Polger, 2021; Princeton Public Library, 2024).



Source: Library.csi.cuny.edu. <https://library.csi.cuny.edu/misinformation>

While misinformation is the unintentional sharing of false or partially false information, disinformation is a more malicious form that involves sharing false information with the deliberate intent to cause harm or profit. Moreover, disinformation is a warfare strategy used to create confusion, disrupt political processes, and manipulate public discourse. It is disseminated rapidly across various platforms, including social media, mainstream media, and non mainstream media. Social media, in particular, enables real-time, large-scale dissemination of disinformation, reaching a wider audience more quickly

than other online channels.

This strategic use of information is a key component of IW, which involves the deliberate spread of misinformation, propaganda, and manipulation. “The goal of IW is to influence public opinion, disrupt social systems, and undermine trust in institutions.” IW tactics can be used to disrupt an adversary’s decision-making process by creating “information shocks” that lead them to make mistakes (Pandey et al., 2024).

Types of Misinformation and Disinformation:

Type	Description
Fabricated Content	Entirely false information or stories.
Manipulated Content	Authentic information or media that has been deliberately altered for a deceptive purpose, like a misleading headline.
Imposter Content	Content created to impersonate a legitimate source, often by using its branding or design.
Misleading Content	The presentation of information in a way that creates a false impression, such as treating an opinion as a fact.
False Context	Combining accurate information with deceptive contextual details to present a misleading narrative.
Satire and Parody	Fictional, often humorous content that is not intended to deceive but can be misinterpreted as true.
False Connections	The use of headlines, visuals, or captions that are unrelated to the actual content they accompany.
Sponsored Content	Material that is paid for by an advertiser but is designed to appear as unbiased editorial content.
Propaganda	Content strategically created and disseminated to influence attitudes, values, and knowledge in favor of a specific agenda.
Error	A factual mistake made by a legitimate news organization in its reporting.

Source: Created by the Authors

In the digital age, the nature of misinformation has changed, enabling its rapid spread through new methods. The recent Russia-Ukraine war demonstrated the development of novel information warfare tactics, with future strategies expected to become even more sophisticated (Hung, 2022). While the internet provides vast access to information, its reliability must be verified, as false information poses a significant threat to its credibility. Misinformation is particularly dangerous in cross-border conflicts, where it can be weaponized to manipulate public opinion, erode social cohesion, and worsen tensions between nations by influencing individual perceptions and behaviors (Menicocci et al., 2024).

In the contemporary digital landscape, the Internet has become a primary domain for information warfare, enabling the swift and widespread acquisition, defense, and disruption of data (NATO, 2020). The low cost, extensive reach and high speed of disinformation campaigns make social media a critical tool for this purpose. These platforms also provide valuable data on target audiences, allowing for more precise and effective manipulation. Key tactics employed in internet-based information warfare include:

1. Troll factories: Organizations that use fake social media profiles to post comments aligned with a client’s agenda.
2. Bots: Automated programs designed to send messages, often triggered by specific keywords, to amplify a particular narrative.
3. Fake news: Misleading messages intentionally created to deceive media consumers (NATO, 2020).

Social Media Manipulation

A growing number of tactics are used to manipulate narratives on social media which includes:

1. **Sockpuppeting** is the use of a fake online identity to deceive others. Unlike a pseudonym, a sock puppet pretends to be an independent third party to praise, defend, or support a person or organization. This tactic is used to manipulate public opinion or bypass bans.
2. **Sealioning** is a form of harassment characterized by persistent requests for evidence or repeated questions. The perpetrator maintains a pretense of civility and sincerity while engaging in an incessant, bad-faith attempt to debate.
3. **Astroturfing** is the practice of masking the true sponsors of a message to make it appear as if it originates from a grassroots movement. This is often done by political, religious, or corporate organizations to gain credibility by concealing their financial motives.
4. **Catfishing** is a type of fraud in which a person creates a fake online identity to deceive a victim, often for financial gain, to compromise their information, or for other malicious purposes. It is commonly associated with romance scams on dating websites. (UNHCR, 2022)

The advent of artificial intelligence (AI) has led to the emergence of synthetic media, a new form of digital manipulation. Synthetic media involves the AI-driven production and modification of data and multimedia to alter original meanings or mislead audiences. This technology poses a significant threat, as it can accelerate the spread of fake news, erode trust, and even automate creative jobs.

Types of Synthetic Media

1. **Deepfakes** are a form of synthetic media that uses AI to replace a person's likeness in an image or video with someone else's. While content manipulation is not new, deepfakes employ powerful machine learning to create highly deceptive and realistic visual and audio content. They have been used in various malicious activities, including revenge porn, hoaxes, and financial fraud, prompting efforts from industries and governments to detect and limit their use.
2. **Speech synthesis** is a form of synthetic media capable of artificially generating human speech. This technology, also known as a "speech synthesizer," creates voices by either combining fragments of recorded speech or by modeling the human vocal tract to generate a completely synthetic voice.

2. Transmission Channels

Social Media: Social media platforms, such as X (formerly Twitter) and WhatsApp, have become primary channels for information warfare, enabling false information to spread faster than factual content (Stepanova & Ross, 2023; Prier, 2017). While these platforms facilitate the sharing of truthful information, they are also significant sources of disinformation (intentional false information) and misinformation (unintentional false information). This dual nature places social media on the "front line" of information conflict (Karami et al., 2021).

Mainstream Media: Traditional media, including both state-controlled and independent outlets, can either amplify or correct misinformation. The spread of disinformation and misinformation is a significant threat to quality journalism and professional ethics (Media Defence, n.d.). While not new, this problem has become more acute as digital technology allows false information to spread rapidly, particularly in polarized environments, where it can overwhelm credible news and obscure the truth.

Impacts

1. **Journalists:** Media outlets are not just reporters of conflict; they are also targets of information warfare. Journalists face the challenge of verifying information related to international events, as messages may be part of a disinformation campaign. Hacking attacks on websites that oppose a state's information warfare activities are also a concern (NATO, 2020).

2. **Media Users:** Users of both traditional and digital media are often targets of information warfare. They are becoming increasingly aware that they are being subjected to disinformation campaigns aimed at influencing their perception of reality. As distrust in official sources grows, many users are turning to alternative sources, including civil media. To counter propaganda, users must actively seek to escape their “information bubble” or “echo chamber” by diversifying their sources and consuming information not filtered by social media algorithms (NATO, 2020).

Waves of Disinformation during the Conflict

False narratives can significantly influence public behavior (Katharina Kiener-Manu, 2019). When these narratives are amplified through various channels, they generate further waves of misinformation and disinformation. This self-sustaining cycle fueled the information warfare environment during the conflict between India and Pakistan in May 2025. Operation Sindoor demonstrates how digital platforms are becoming critical battlegrounds for narrative control, where the strategic use of emotionally charged content is vital for boosting user engagement, escalating geopolitical tensions, and ultimately influencing strategic outcomes.

1. Fake Claims and narrative of Downed Indian Jets:

During Operation Sindoor, a coordinated disinformation campaign was launched by Pakistan, initially claiming that three Indian jets had been shot down (ET Online, 2025). This narrative quickly escalated, with the Pakistani Inter-Services Public Relations (ISPR) office officially asserting that the Pakistan Air Force (PAF) had shot five Indian fighter jets. When asked for evidence by CNN, Pakistan's Defense Minister, Khawaja Muhammad Asif, vaguely stated, “It is all over social media” (ET Online, 2025). This claim was amplified by Pakistani news outlets and by international media sourcing Pakistan outlets. Even US President claimed that five fighter jets were shot down before the two side’s ceased hostilities, though he did not specify which side's aircraft were downed or what the jets were (Asian News International, 2025).

Pakistani Air Vice Marshal Aurangzeb during media briefing increased the number of downed Indian aircraft to six, supporting his assertion with an audio clip of what he alleged was intercepted communication between Indian pilots. This led to a widespread “6-0” social media campaign, which was even mirrored by a Pakistani cricketer during a cricket match to mock the Indian crowd. The false narrative gained further international attention when, in July, U.S. President Donald Trump claimed, “The war with India and Pakistan was the next level that was going to be a nuclear war... They already shot down 7 jets...” In September, Pakistan’s Prime Minister echoed this claim at the UN General Assembly, stating, “Our falcons took flight and turned 7 Indian jets into scrap” (Asian News International, 2025).

To support these false claims, old and unrelated images of crashed aircrafts were shared on social media. India’s Press Information Bureau (PIB) swiftly debunked these posts on X (formerly Twitter). For example, a viral photo of a supposed downed Rafale jet was identified by PIB Fact Check as a 2021 MiG-21 crash in Moga, Punjab (ET Online, 2025).

The Indian Air Chief Marshal A.P. Singh, during the 16th Air Chief Marshal L.M. Katre Lecture on August 10, 2025, confirmed that India had shot at least five Pakistani jets during the conflict, along with a large aircraft most probably a surveillance aircraft. He further stated that India had destroyed at least two F-16s on the ground inside hangars at Shahbaz and Jacobabad airfields (Asian News International, 2025). An Austrian military aviation analyst, Tom Cooper, also supported these claims, stating that

based on evidence, Pakistani even had lost more aircrafts on the ground. The United States also refused to provide details of the Pakistan Air Force active F-16 fleet.

2. Propaganda by Pakistan:

In an attempt to provoke communal unrest and disrupt Indian unity, Pakistan's Director-General of ISPR, Lieutenant General Ahmed Sharif Chaudhry, made several unsubstantiated claims. Among these was the fabricated narrative that India had fired six missiles at the city of Amritsar, a claim that was later proven false. Additionally, Gurpatwant Singh Pannun, an Indian-designated terrorist, used social media to urge Indian citizens to share information on military movements with his organization, "Sikhs for Justice," in exchange for money. He asserted that this information would assist Pakistan's military offensives and support the creation of Khalistan. This action further substantiated India's prior claims that Pannun acts as an agent of the Pakistani government. Pakistan also claimed that Indian missiles had landed in Afghanistan, a claim that was denied by the Afghan government.

In a separate instance, Pakistan's Army Chief, Asim Munir, publicly stated that in a future conflict, Pakistan would initiate an attack from the eastern direction (Mahjar-Barducci, 2025). This was likely a strategic maneuver to compel India to divert its air assets, thereby weakening its defenses on the western border. During his visit to the U.S., he issued a nuclear threat, stating, "We are a nuclear nation, if we are going to go down, we'll take half the world down with us" (Mahjar-Barducci, 2025). This statement was likely intended to pressure the international community into supporting Pakistan's military buildup under the pretense of preventing global instability.

3. False Claims of Airbase Strikes:

Both India and Pakistan claimed to have struck each other's air bases during the conflict. Pakistan asserted that it had rendered multiple Indian air bases in J&K, Punjab, Rajasthan, and Gujarat, including key bases at Adampur, Bhuj, Jammu, Pathankot, Srinagar, Udhampur and claimed to make them non-functional. Following the ceasefire, Pakistan's Director General of ISPR claimed to have struck 23 Indian military installations. However, these claims were refuted by the actions of Indian officials. The day after the ceasefire, the Indian Prime Minister visited the Adampur air base, while the Defence Minister visited the Srinagar air base, visually confirming that the facilities remained operational. Furthermore, there is no credible evidence like satellite imagery available which shows strikes on Indian bases. However, India asserted that limited damage was sustained at Adampur, Bhuj, Pathankot, and Udhampur air force stations including the medical and school premises (GoI, 2025).

In contrast, India provided satellite imagery to support its claims of striking Pakistani air bases. The strikes were so effective that some Pakistani bases, including the Rahim Yar Khan air base, remained inactive for months due to extensive damage. India also successfully struck Sargodha, Pakistan's most strategically significant and heavily guarded air base. Indian Air Chief Marshal A. P. Singh stated that "Sargodha...we've grown up in our Air Force, dreaming about day like this..... I got a chance and we took on the air field," (Asian News International, 2025) that is striking Sargodha. He also stated that India had hit a total of 11 Pakistani air bases (Asian News International, 2025).

4. False Claims about Soldiers Involving Indian Fighter Pilot Shivani Singh:

AI-generated and fabricated images and videos were circulated on social media, falsely claiming that India's first female Rafale pilot, Shivangi Singh, had been captured in Pakistan after her jet crashed. This disinformation fueled sensationalism until the Indian Directorate General of Air Operations (DGAO) clarified that "All pilots are at home" (TOI, 2025). Following the ceasefire, Pakistan's DG ISPR also confirmed that no Indian pilot was in its custody, ending the controversy.

Meanwhile, a report from the Pakistani news channel SAMAA TV inadvertently published a list of 155 Pakistan Army personnel who received awards for their service during India's Operation Sindoor. The report, which included names, ranks, and provinces, was quickly removed; sparking accusations that Islamabad was concealing its battlefield casualties. The leaked document, however, circulated online, revealing that many names were prefixed with "Shaheed" (martyr), indicating lot of casualties faced by Pakistan military during operation.

5. Staged Videos:

Fabricated videos were circulated on social media to falsely claim that a Brigade Headquarters in Poonch had been destroyed by Pakistan. These videos depicted Indian soldiers in a demolished building, accompanied by a burning Indian flag and a person chanting "Ram-Ram" to simulate a realistic scenario and spread disinformation. In a separate incident, a video falsely claiming that the Indian Army had surrendered by raising a white flag at Chora Post went viral and was endorsed by Pakistan's Minister Attaullah Tarar (ET Online, 2025), further fueling the disinformation.

During the conflict, many falsified videos, including footage of Israeli airstrikes against Palestinians, video game visuals, and clips of firecrackers were widely shared, misrepresented as strikes by Pakistani sides on Indian army bases. Some Pakistani television news anchors even contributed to the spread of fake content.

Claims of hitting military Installations

Pakistan also claimed to have hit India's S-400 air defense system and struck the BrahMos missile manufacturing facility in Haryana. Pakistani officials even circulated an image, asserting it showed the destruction of an S-400 at Adampur Airbase. However, neither satellite imagery nor independent verification ever confirmed these claims. The Inter-Services Public Relations (ISPR) issued a statement declaring that the S-400 was neutralized by hypersonic missiles from a JF-17 platform, but the recovery of a CM AKG-400 missile in an open field completely undermined Pakistan's assertions.

Despite Pakistan's claims, a Pakistani journalist, Najam Sethi, acknowledged during a television interview that his country lacks sophisticated air defense systems like the S-400 or Iron Dome. He conceded that India had demonstrated the accuracy of its missile technology by successfully striking Pakistani air bases and "offices of freedom fighters." The Indian Air Chief confirmed India's successful strikes, including the destruction of two command and control systems at Murid and Chaklala, at least six radars, two Surface-to-Air Guided Weapon (SAGW) systems at Lahore and Okara, and runways at Rahim Yar Khan and Sargodha. The Air Chief also noted the destruction of three hangars housing UAVs at Sukkur, an AW&CS at Bholari, and F-16s at Jacobabad (Asian News International, 2025).

Ceasefire Controversy

While a ceasefire between India and Pakistan was declared on May 10, 2025, at 17:00 IST, its origins became a subject of controversy and competing narratives. U.S. President Donald Trump publicly claimed credit for brokering the ceasefire, stating on social media platform X stating that he had stopped a major conflict. During a bilateral meeting with the President of the Republic of Korea, he further asserted, "You (India and Pakistan) want to trade? We are not doing any trade or anything with you if you keep fighting; you've got 24 hours to settle it" (Asian News International, 2025). Pakistan's Prime Minister further solidified this narrative during his September 2025 address to the UN General Assembly, where he gave Trump credit for the mediation and nominated him for the Nobel Peace Prize.

In contrast, the Indian government maintained that the ceasefire was initiated by Pakistan's Director General of Military Operations (DGMO), who contacted his Indian counterpart to propose it. India also confirmed receiving offers of mediation from the U.S. and Saudi Arabia but reiterated its position that the conflict was a "bilateral issue" (Asian News International, 2025). Despite this, the narrative of U.S. mediation gained traction, damaging India's diplomatic position and fostering a perception of external pressure. This underscores the power of competing public narratives in modern interstate conflicts.

Words Become Weapons

During the conflict, public statements by military officers and political figures were often taken out of context and weaponized to fuel misinformation. This phenomenon was evident when Director General Air Operations A.K. Bharati's statement that "losses are the part of combat" was misinterpreted by adversaries as an admission of losses, which was then used to confirm social media disinformation.

A similar controversy arose from remarks made by Chief of Defence Staff General Anil Chauhan at the Shangri-La Dialogue. When asked about potential Indian jet losses, he stated that India had "rectified" its tactics after losses on May 7th to gain an advantage over Pakistan. He also described Pakistan's claim of shooting down six Indian jets as "absolutely incorrect" but did not provide specific numbers for India's losses (Bureau, 2025a). Despite his nuanced comments, international media outlets, including Al Jazeera, reported that a high-ranking Indian official had confirmed jet losses. Remarks by the Indian defence attaché in Indonesia, Captain Shiv Kumar, at a seminar in Jakarta, was reported to have said, "We did lose some aircraft and that happened only because of the constraint given by the political leadership to not attack the military establishment or their air defence system" (PTI, 2025). A statement that Indian Embassy later clarified was taken out of context. The Opposition Congress party cited these reports to accuse the government of misleading the country, while Pakistani media used the remarks as "proof" of losses, highlighting how even minor misrepresentations can be used to advance an adversarial narrative.

In addition to official military statements, remarks from Indian politicians were also weaponized. Pakistan's DG ISPR exploited old videos of former J&K Governor Satya Pal Malik and Rahul Gandhi to promote the false narrative that the Indian government had orchestrated the 2019 Pulwama attack for political gain (Express Web Desk, 2023).

These events highlighted the critical need for Indian politicians and military officers to exercise caution in their public statements. Irresponsible remarks, even if politically motivated, can inadvertently aid enemy propaganda and distort the truth. The incident also underscored the importance of responsible political discourse in matters of national security, as careless rhetoric provides fertile ground for adversarial disinformation campaigns. This situation underscores the necessity for digital responsibility and vigilance from both political leaders and the officers. In the age of information warfare, every statement and social media post carries strategic weight, capable of influencing narratives far beyond borders.

Misinformation - The Role of Indian Media during the Conflict

Indian media played a dual role during the conflict. While many trusted news outlets worked to keep the public well-informed and maintain morale, certain national media channels spread misinformation that compromised their credibility. False reports of "Indian Navy attacks on Karachi Harbor" and "Indian Army advances 60 km into Pakistan" were circulated without verification. Some media houses even reported the arrest of a Pakistani Prime Minister, damaging both trust and reputation. Prominent news platforms, in the race for breaking news, often published unverified information under disclaimers like

“local sources” or “expected”. Some news portals deleted their reports from their platforms after they were found to be false or lacking verification from credible sources. These premature reports were swiftly picked up by international media and Pakistani digital platforms to reinforce their propaganda narratives, adding layers of complexity to India’s efforts in countering disinformation.

Similarly, local social media based news channels frequently posted unverified content during the conflict. As the Indian air defense shot down multiple drones and missiles during the conflict, the resulting explosions and scattered debris were often photographed and shared online. These posts, while immediate and unfiltered, inadvertently revealed critical infrastructure and military installation locations. Pakistan and Pakistani social media users quickly exploited these visuals to falsely claim successful strikes on key Indian targets. This exposure of sensitive locations during a conflict not only amplified disinformation campaigns but also highlighted the need for responsible reporting and digital awareness. Furthermore, social media users also posted unverified content during the conflict. Numerous rumors of attacks, blasts, infiltrations, and terrorist activities also spread across social media during the days of conflict, contributing to confusion and panic. During conflict, exercising caution and ensuring verification are crucial for safeguarding national security and upholding public morale.

Countering Mis and (dis)information

Katharina Kiener-Manu proposed a solution to counter misinformation and disinformation, drawing upon inoculation theory, which involves building public resilience (katharina.kiener-manu, 2019). This approach provides individuals with the tools to resist propaganda by exposing them to small amounts of false information and educating them on deceptive tactics. This method reduces susceptibility and encourages individuals to question the veracity of information and the legitimacy of its sources. Inoculation theory has been empirically supported in its application to highly politicized topics and can be effectively applied to both misinformation and disinformation (katharina.kiener-manu, 2019).

The international community, led by the United Nations, has also expressed significant concern over disinformation. The UN Secretary-General has submitted a report based on best practices from member states and other entities, detailing legal frameworks and measures to combat the problem while protecting fundamental freedoms (United Nations, 2021). The majority of strategies to combat disinformation are increasingly focused on social, educational, and technical solutions to avoid infringing on the right to freedom of expression. Current efforts emphasize media and information literacy (MIL) campaigns and advocacy, rather than litigation (United Nations, 2021). However, this is expected to evolve as digital rights litigators become more involved in strategic test cases to mitigate disinformation while upholding free speech.

India’s Digital Response: Learning from the Past

During the initial phases of Operation Sindoor, India’s digital response lagged behind Pakistan’s aggressive disinformation campaign (Bureau, 2025). However, India quickly adapted a strategy of proactive transparency. During the first official briefing, the Indian military displayed real-time images and videos of the strikes, which served to preemptively counter false narratives that had emerged during the 2019 Balakot airstrike. This strategic move successfully limited the space for speculation and narrative manipulation.

Key Components of India’s Digital Response

India's counter-disinformation efforts were multifaceted:

1. **Centralized Coordination:** A 24/7 centralized control room was established for inter-departmental

and inter-disciplinary coordination which included representatives from all branches of the armed forces and the PIB. Its primary function was to provide real-time, authentic information to media stakeholders through periodic briefings, complete with audio-visuals and satellite imagery (Bureau, 2025).

2. **Fact-Checking and Debunking:** The PIB's Fact Check Unit actively monitored social and online media to identify and debunk fake news, manipulated content, and misleading narratives. This unit specifically focused on countering Pakistani propaganda and its fact-checked links were shared with social media platforms for appropriate action (Bureau, 2025).
3. **Governmental Directives:** The government urged the public and media to exercise caution and responsible reporting, requesting that they refrain from publishing military movements. Government also issued directives to social media platforms, such as YouTube, Instagram, and X to block access to approximately 8,000 accounts and over 1,400 URLs that were circulating "false, misleading, anti-India, and communally sensitive content" (Venugopal, 2025; Bureau, 2025).

Challenges and Vulnerabilities

Despite these efforts, India's restrained official stance, particularly by the Ministry of External Affairs and the Indian armed forces was exploited by Pakistan to push false narratives and portray India as the aggressor. This highlighted India's ongoing struggle to manage digital narratives on the international stage effectively. During Operation Sindoor, no platform or medium was protected from the rapid spread of misleading content, social media platforms, including YouTube, Facebook, Instagram and X served as primary medium for cross-border information warfare. While fact-checking organizations like the PIB Fact Check Unit played a critical role, but they also struggled to keep up with the sheer volume and speed of misinformation.

More concerning was the limited response from platforms. Despite the widespread circulation of false content, platform moderation systems were largely ineffective, with very few posts being flagged or removed across social media. This deficiency exposed significant weaknesses in existing content-moderation frameworks. X, specifically, became a central hub for both misinformation and disinformation. A study that examined 437 posts indicates that only 73 were flagged with community notes. (Centre for the Study of Organized Hate, 2025).

The recent conflict brought into focus the threat posed by emerging technologies like generative AI and high-fidelity simulation engines, which showcased their capability for real-time narrative manipulation. The conflict also exposed the prevalence of malicious online tactics. "Doxing," which is defined as the use of sensitive or private information to harass and expose individuals (Fortinet, n.d.), also became a prominent issue. A shocking example was the doxing of India's foreign secretary Vikram Misri and his daughter, whose personnel information was leaked online. This act is a direct violation of the fundamental right to privacy (Venugopal, 2025), emphasizing the new and dangerous forms of cyberbullying in modern conflicts.

Conclusion: Building Resilience Against Information Warfare

The 2025 Indo-Pakistan conflict serves as a stark reminder that modern warfare transcends physical boundaries, making the battle for perception as critical as armed conflict itself. The events of operation Sindoor underscore the urgent need for India to prioritize digital resilience and redefine its concept of national security in the era of Information Warfare.

This study reveals that India's digital response, particularly in shaping narratives and countering misinformation, was initially underplayed. This highlights the necessity for a dedicated and robust infrastructure capable of both defending against and using information as a strategic weapon. Disinformation, if left unchecked, can not only distort the truth but also sway public opinion and undermine national security. Therefore, a coordinated strategy involving the government, media, and civil society is essential to combat it effectively. This strategy must include the establishment of real-time fact-checking mechanisms, the enhancement of digital literacy, and the adoption of swift counter-narrative measures. As every social media post can serve as a potential weapon, citizen awareness and responsible sharing are equally important in safeguarding the nation's narrative and morale. The study concludes that in the digital age, securing a nation's infospace is paramount to its security.

References

1. American Psychological Association. (2025). Misinformation and Disinformation. American Psychological Association. <https://www.apa.org/topics/journalism-facts/misinformation-disinformation>
2. Asian News International. (2025, August 27). "Seven Jets Downed": Trump Doubles Down On India-Pak Conflict Claim. NDTV. <https://www.ndtv.com/world-news/seven-jets-downed-trump-doubles-down-on-india-pak-conflict-claim-9167765>
3. Bakshi, M. G. B. (2018). INFORMATION WARFARE: REDEFINING NATIONAL SECURITY. CENTRE for JOINT WARFARE STUDIES , XII(23). https://cenjows.in/wp-content/uploads/2022/03/1_Information-Warfare-Refefining_30-10-2018_Digital.pdf
4. Bingle, M. (2023, September 26). What is Information Warfare? - The Henry M. Jackson School of International Studies. The Henry M. Jackson School of International Studies. <https://jsis.washington.edu/news/what-is-information-warfare/>
5. Bureau, T. H. (2025a, May 31). India established decisive advantage after "losses" in the air on first day of Operation Sindoor: CDS. The Hindu. <https://www.thehindu.com/news/national/operation-sindoor-cds-anil-chauhan-says-india-suffered-initial-losses-in-the-air-declines-to-give-details/article69641180.ece>
6. Bureau, T. H. (2025b, July 30). Blocked 1,400 "anti-India" URLs during Operation Sindoor, says Government. The Hindu. <https://www.thehindu.com/news/national/blocked-1400-anti-india-urls-during-operation-sindoor-says-governement/article69874844.ece>
7. Centre for the Study of Organized Hate. (2025, January). Inside the Misinformation and Disinformation War Between India and Pakistan. Csohate.org. <https://www.csohate.org/2025/05/16/india-pakistan-digital-war/>
8. ET Online. (2025, May 8). Pakistan defence minister's live TV blunder: Khawaja Asif cites social media to claim Indian jets were shot down. The Economic Times; Economic Times. https://economictimes.indiatimes.com/news/new-updates/pakistan-defence-ministers-live-tv-blunder-khawaja-asif-cites-social-media-to-claim-indian-jets-were-shot-down-gets-fact-checked/articleshow/120983764.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
9. Express Web Desk. (2023, October 25). Rahul Gandhi interviews Satya Pal Malik, asks him about Pulwama, Adani and Manipur. The Indian Express. <https://indianexpress.com/article/india/rahul-gandhi-interviews-satya-pal-malik-asks-him-about-pulwama-adani-and-manipur-8998982/>

10. fortinet. (n.d.). What Is Doxing? What Does It Mean to Dox Someone? Fortinet. <https://www.fortinet.com/resources/cyberglossary/doxing>
11. GoI, M. (2025, May 10). Transcript of Special briefing on OPERATION SINDOOR (May 10, 2025). Mea.gov.in. <https://www.mea.gov.in/media-briefings.htm?dtl/39486/Transcript+of+Special+briefing+on+OPERATION+SINDOOR+May+10+2025>
12. GoI, P. (2025). Operation SINDOOR: India's Strategic Clarity and Calculated Force. Pib.gov.in. <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2128748>
13. Hung. (2022). Distorting Your Perception of Russia's Aggression: How Can We Combat Information Warfare? *Connections the Quarterly Journal*, 21(3), 77–101. <https://doi.org/10.11610/connections.21.3.28>
14. Karami, A., Lundy, M., Webb, F., Turner-McGrievy, G., McKeever, B. W., & McKeever, R. (2021). Identifying and Analyzing Health-Related Themes in Disinformation Shared by Conservative and Liberal Russian Trolls on Twitter. *International Journal of Environmental Research and Public Health*, 18(4), 2159. <https://doi.org/10.3390/ijerph18042159>
15. katharina.kiener-manu. (2019, June). Cybercrime Module 14 Key Issues: Information Warfare, Disinformation and Electoral Fraud. [Www.unodc.org](http://www.unodc.org). <https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html>
16. Mahjar-Barducci, A. (2025, September 11). Pakistan's Army Chief Sparks Alarm with Nuclear Threats on U.S. Soil - Australian Institute of International Affairs. Australian Institute of International Affairs. <https://www.internationalaffairs.org.au/australianoutlook/pakistans-army-chief-sparks-alarm-with-nuclear-threats-on-u-s-soil/>
17. Media Defence. (n.d.). Misinformation, Disinformation and Mal-information. EReader. <https://www.mediadefence.org/ereader/publications/modules-on-litigating-freedom-of-expression-and-digital-rights-in-south-and-southeast-asia/module-8-false-news-misinformation-and-propaganda/misinformation-disinformation-and-mal-information/>
18. Menicocci, S., Lupo, V., Ferrara, S., Giorgi, A., Serra, E., Babiloni, F., & Borghini, G. (2024). Fake-News Attitude Evaluation in Terms of Visual Attention and Personality Traits: A Preliminary Study for Mitigating the Cognitive Warfare. *Behavioral Sciences*, 14(11), 1026. <https://doi.org/10.3390/bs14111026>
19. Nataliya Stepanova, & Ross, B. (2023). Temporal Generalizability in Multimodal Misinformation Detection. <https://doi.org/10.18653/v1/2023.genbench-1.6>
20. NATO. (2020). *Media-(Dis)Information-Security*. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
21. pandey, rashmikiran, Pandey, M., & Nazarov, A. (2024). Modeling Information Warfare in Scale-Free Networks: Analysis of Propagation and Counter-Propagation Dynamics. Research Square (Research Square). <https://doi.org/10.21203/rs.3.rs-3964006/v1>
22. Polger, M. A. (2021, November 16). CSI Library: Misinformation and Disinformation: Thinking Critically about Information Sources: Definitions of Terms. Library.csi.cuny.edu. <https://library.csi.cuny.edu/misinformation>

23. Princeton Public Library. (2024, October 23). Misinformation, Disinformation & Malinformation: A Guide - Princeton Public Library. Princeton Public Library.
<https://princetonlibrary.org/guides/misinformation-disinformation-malinformation-a-guide/>
24. PTI. (2025, June 30). Row over Defence attaché's remarks on "fighter jets lost" in Operation Sindoor; Indian Embassy steps in. The Hindu. <https://www.thehindu.com/news/national/indian-armed-forces-serve-under-civilian-political-leadership-embassy-says-defence-attach%C3%A9s-remarks-on-op-sindoor-misrepresented/article69753894.ece>
25. TOI. (2025, May 11). "All our pilots are back home": Air Marshal AK Bharti confirms as India strikes inside Pakistan. The Times of India; Times Of India.
<https://timesofindia.indiatimes.com/india/all-our-pilots-are-back-home-air-marshal-ak-bharti-confirms-as-india-strike-inside-pakistan/articleshow/121082943.cms>
26. UNHCR. (2022). Factsheet 4: Types of Misinformation and Disinformation.
<https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf>
27. United Nations. (2021). Countering Disinformation. United Nations.
<https://www.un.org/en/countering-disinformation>
28. Venugopal, S. (2025, May 13). Between Pahalgam attack and Operation Sindoor: India's social media war. The Hindu. <https://www.thehindu.com/sci-tech/technology/between-pahalgam-attack-and-operation-sindoor-indias-social-media-war/article69569944.ece>
29. Yu, M. T.-C., & Ho, K. (2022). COVID and Cognitive Warfare in Taiwan. *Journal of Asian and African Studies*, 58(2), 249–273. <https://doi.org/10.1177/00219096221137665>