Future Shift Labs

The New Frontline of War

Foreign Information Manipulation and Interference as Pakistan's Shadow Weapon Against India after Operation Sindoor

The New Frontline of War

Foreign Information Manipulation and Interference as Pakistan's Shadow Weapon Against India after Operation Sindoor

Prepared by

Future Shift Labs

Authors

Sunanda R. Marak

About Future Shift Labs

Future Shift Labs is a strategic research and policy think tank working to build a sustainable, equitable, and digitally resilient future by advancing responsible and ethical applications of artificial intelligence. Established in 2024, the organisation conducts in-depth research and analysis on emerging AI technologies and their societal impact, advocates for inclusive AI governance, and supports strategic consulting, training, and public engagement to strengthen institutional and community capacity. With a focus on fostering collaboration among researchers, policymakers, industry leaders, and civil society, Future Shift Labs seeks to position India as a global leader in digital diplomacy, ethical AI development, and international cooperation on emerging technology challenges

Publication Year: 2026

Future Shift Labs

Foreword

Mr. Nitin Narang

Founder, Future Shift Labs

The contest for influence has entered a new domain. One fought not with soldiers and steel, but with narratives, algorithms, and perception. This report by Sunanda R. Marak stands at the intersection of strategy, technology, and geopolitics, illuminating how Pakistan has operationalised disinformation as an extension of hybrid warfare against India.

At Future Shift Labs, our mission is to map the unseen; to decode the patterns shaping national security in the digital age. This study offers both depth and foresight, bridging the European FIMI framework with the Indian context. It exposes the structural anatomy of Pakistan's information manipulation network and its growing convergence with foreign state media and influence ecosystems.
Sunanda's work reinforces FSL's commitment to producing evidence-based, actionable insights for policymakers, journalists, and digital defenders. It reminds us that truth itself is now a contested domain; one we must vigilantly defend.

Foreword

Mr. Sagar Vishnoi

Co-Founder, Future Shift Labs

In an age where perception defines policy and pixels replace bullets, understanding information warfare is no longer optional; it is existential. This report dissects the anatomy of Pakistan's FIMI architecture with the precision of an intelligence map and the clarity of academic rigour.

By tracing how Islamabad leverages media, diplomacy, and digital ecosystems to distort narratives around India, Sunanda reveals not just tactics, but intent. Her analysis connects local incidents like the Pahalgam attack and Operation Sindoor to a global matrix of coordinated influence operations.

This publication is a milestone in FSL's pursuit of data-driven, independent research on cognitive and digital threats. It underlines our central conviction that national security today is as much about *information integrity* as it is about territorial sovereignty.

About the Author

Sunanda R. Marak

Senior Geopolitical Analyst

Sunanda R. Marak has completed Ph.D. in European Studies at Jawaharlal Nehru University (JNU), New Delhi. She holds a double Master's degree in International Relations and History. Her research delves into the European Union's cross-border cooperation policies, particularly focusing on Nordic-Baltic cooperation.

Her academic interests extend to South Asia, Southeast Asia, and China, where she examines intersections of geopolitics, governance, and digital influence. Professionally, Sunanda brings a diverse portfolio of experience; from teaching to working as a research analyst with prominent national and international think tanks.

At Future Shift Labs (FSL), she serves as a Senior Geopolitical Analyst, where her research centres on disinformation, misinformation, and influence operations within the broader context of the global information ecosystem. Her work reflects a commitment to bridging academic insight with real-world strategy in an era defined by cognitive warfare and information manipulation.

Index

Table of Content — Pages

Abstract

In the age of hybrid conflict, war is no longer confined to the battlefield, but it is within minds, through competing narratives, and across invisible lines of the information system. This report critically examines the evolving landscape of Foreign Information Manipulation and Interference (FIMI), focusing on how Pakistan operationalised disinformation as a strategic tool against India at the backdrop of Pahalgam attack and Operation Sindoor. This study explores how Pakistan leveraged foreign media and X influencers to amplify its messaging to the international community. Drawing on the EU's FIMI conceptual framework, the study analyses the architecture, objectives, and Tactics, Techniques and Procedures (TTPs) underpinning these state-led influence operations.

This study highlights three significant developments in Pakistan's state-driven disinformation campaign against India following *Operation Sindoor*. *Firstly,* Pakistan intensified its coordinated use of its official channels and state-controlled media to disseminate false narratives, deliberately targeting international audiences to delegitimise India's actions during *Operation Sindoor*. *Secondly*, the campaign exploited foreign media outlets and influential X personalities to amplify disinformation and misinformation, to distort narratives, cultivate confusion, undermine credible sources, polarise both Indian and global public opinion, and advance Pakistan's broader geopolitical agenda. Thirdly, Pakistan had deliberately weaponised "*Misinformation*" to maximise the impact of its disinformation operations, using false and distorted narratives, as well as AI-generated images and fabricated videos to manipulate public opinion and achieve its geopolitical objectives. A key finding of this report is the growing strategic convergence between Pakistan and countries like China, Turkey and Azerbaijan in their FIMI ecosystem. Moreover, the study also emphasises that with the integration of AI, algorithmic targeting, and real-time influence operations, Pakistan's FIMI has now evolved into a potent instrument of cognitive warfare.

The report concludes by underscoring the urgency of a comprehensive national response. It argues for a proactive, multi-pronged counter-FIMI strategy rooted in digital resilience, strategic communication, and the protection of India's democratic information space.

Introduction

The Gist: *The question of What, Where, Why and How?*

On 22 April 2025, news of a terrorist attack in Pahalgam triggered widespread shock, anger, and mourning across India, drawing significant global media attention. The attack was carried out by six terrorists, including two Kashmiris, at the popular tourist destination of Pahalgam in Kashmir, India. It was a premeditated strike, specifically targeting[1] Hindu tourists, who were identified and attacked before the perpetrators carried out the brutal killings. According to reports, the terrorists murdered 26 civilians mostly Hindus including one Christian and one Muslim. This attack was executed by "*The Resistance Front (TRF)"*, a proxy of Pakistan-based terror group Lashkar-e-Taiba (LeT).[2]

Following the attack, India issued a strong response. The Prime Minister-led Cabinet Committee on Security quickly approved the first set of punitive steps against Pakistan: cutting down the diplomatic ties, expelling the Pakistani military officers, suspension of the Indus Waters Treaty, and shutting down the Attari border post. At the same time, India also pulled back its defence, navy, and air advisers from the High Commission in Islamabad.[3] On 7 May 2025, between 1:05 AM and 1:30 AM, India launched "*Operation Sindoor*", striking nine terror targets in Pakistan and Pakistan-occupied Kashmir. These sites were identified as major epicentres for terrorist activity, used for recruiting, training, and indoctrinating militants, as well as planning cross-border attacks. The operation marked a swift and precise retaliation, hitting the enemy's critical infrastructure in a short, focused strike window achieving its strategic objectives.[4]

Despite's India's Director General of Military Operations (DGMO)[5] informing his Pakistani counterpart that the strikes were limited to terror targets and reaffirming India's willingness for dialogue, Pakistan responded aggressively on two fronts: militarily, by mobilizing its forces, and digitally, by unleashing a coordinated cyber offensive that combined disinformation, misinformation, and direct cyberattacks to counter *Operation Sindoor* which escalated into a massive narrative warfare.

History in Brief

Since its inception in 1947, Pakistan has consistently engaged in information warfare against India, aiming to shape narratives, distort facts, and influence public perception both domestically and internationally. While the patterns and mediums have evolved from traditional radio propaganda to sophisticated digital operations, the core objective has remained unchanged: to internationalise Kashmir, malign India's international image, undermine its democratic institutions, discredit India's political and military leadership, and erode social cohesion.

Historically, during the conventional wars between the two countries in 1947-48, 1965, 1971, and the Kargil conflict of 1999, Pakistan relied heavily on traditional means of propaganda. State-controlled radio, print media, and official spokespersons or diplomatic channels were central to its disinformation campaigns. These platforms were used to exaggerate Pakistani military successes, downplay setbacks, and circulate false or inflated claims about Indian losses. The objective was twofold: to boost domestic morale and to psychologically undermine Indian forces and public opinion.

Notably, under Operation Tupac launched in 1988, Pakistan established multiple radio stations along the India-Pakistan border to bombard the airwaves with anti-India propaganda. Beyond Jammu and Kashmir, these transmissions targeted India's national capital, New Delhi, as well as cities such as Jaipur, Kanpur, Meerut, and Aligarh, extending even into parts of Nepal.[6] The broadcasts were also conducted in Hindi, Bangla, and Gujarati, alongside several vernacular languages including Kashmiri, Balti, Shina, Pahari, and Urdu. This demonstrated a calculated effort of Islamabad to target diverse linguistic audiences in India and amplify the psychological impact of its messaging.

Today, Pakistan continues its information warfare campaign against India, albeit with modernized mediums and sophisticated strategies. With the emergence of social media platforms, online news portals, and messaging apps, the information warfare toolkit has expanded dramatically to include narrative construction, dissemination of disinformation and misinformation, fake news amplification, AI-generated content, deepfakes, bot networks, and proxy media outlets. This shift began with Pakistan's realisation that their media strategy against India in previous crises was often fragmented, reactive, and defensive. From the 2008 Mumbai attacks to the 2019 Pulwama incident, it is perceived that their communication apparatus frequently[7]suffered from credibility gaps, inconsistent messaging, and delayed responses. Therefore, in contrast to the backdrop of Pahalgam attack and Operation Sindoor we witnessed Islamabad's deliberate move towards coordinated and proactive information operations.

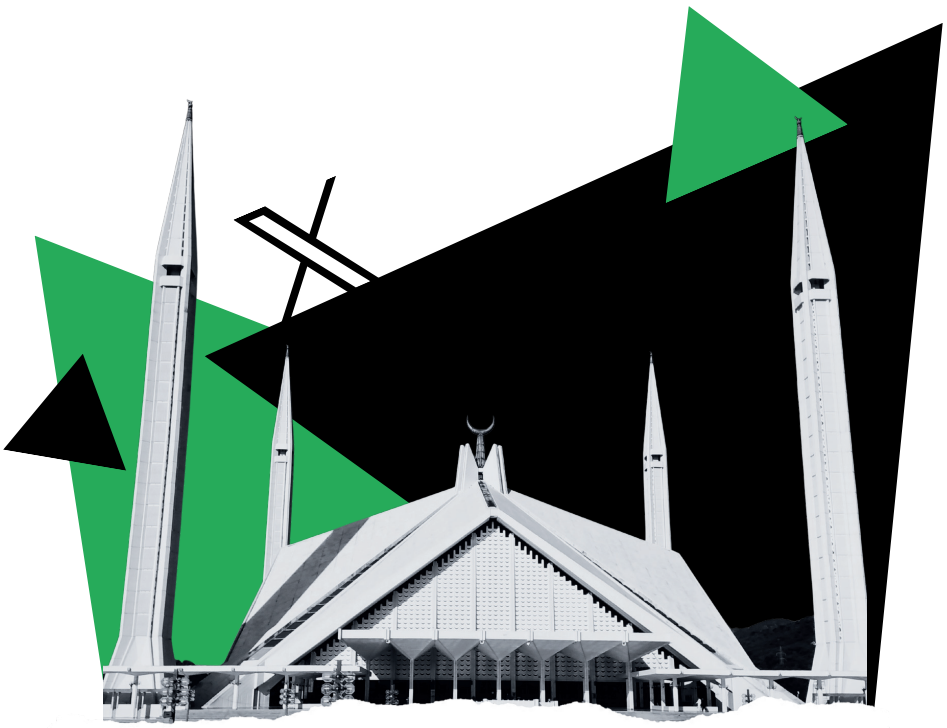
The primary objective of Pakistan's state-led disinformation campaign during Operation Sindoor was to manipulate perception of the international community against India, undermine India's democratic institutions, counter-terrorism efforts, attack military and political leadership, sow internal discord within India, and obfuscate the facts involving the incident. To achieve this, the campaign deployed a variety of tactics,[8] including the dissemination of fabricated news reports, circulation of doctored images and videos, and the revival of previously debunked internet hoaxes. This is Pakistan's calculated approach, one that treats the information domain as a battleground as real as the Line of Control. At the heart of Pakistan's FIMI machinery lies Islamabad's deep state, a convergence of its intelligence agency ISI, ISPR, MFA, Jihadi Mentality, Think Tanks, state controlled and aligned media, and non-State actors operating in both physical and digital realms.

In essence, while the battlefield of information warfare has shifted from radio waves to digital screens and algorithmic manipulation, Pakistan's strategic intent to use information as a weapon against India has remained a constant thread through decades of hostility.

Objective of study

The primary objective of this report is to critically examine the FIMI-based disinformation campaign orchestrated by Pakistan in the wake of the Pahalgam terrorist attack and India's subsequent *Operation Sindoor*. Specifically, this research seeks to:

1. *Analyse the architecture of Pakistan's FIMI ecosystem,* which includes the state institutions, state-linked media, affiliated think tanks and state-aligned social media networks beyond borders and assess how these actors coordinated in disseminating disinformation.
2. Map the strategic goals and objectives of Islamabad's FIMI operations, particularly its attempts to delegitimise India's counter-terrorism response and recast itself as the aggrieved party in the international arena.
3. Examine Pakistan's tactics, techniques, and procedures (TTPs), employed during the campaign, such as narrative construction, amplification strategies, use of visual manipulation, and deployment of historical false flag tropes.
4. Evaluate the role of foreign media and X influencers, and their nexus with Pakistan's FIMI ecosystem, emphasising how they amplified Islamabad's narratives, transnationalised the campaign, and embedded it within global information ecosystems.
5. Propose policy recommendations for the Government of India, aimed at countering FIMI-based disinformation, identifying malign actors, strengthening media resilience, and building international coalitions to expose malign influence operations



Research Methodology

This study adopts a qualitative, analytical, and exploratory research design to examine the architecture, objectives, and operational mechanisms of Pakistan's Foreign Information Manipulation and Interference (FIMI) campaigns against India, particularly during and after *Operation Sindoor* in 2025. This research employs the EU's FIMI framework as an analytical lens, but adapts it to the context of the India-Pakistan conflict. This methodology integrates open-source intelligence (OSINT), discourse analysis, and comparative framework mapping to ensure a comprehensive and evidence-based understanding of Pakistan's FIMI Disinformation operations.

The analysis relies on both primary and secondary data drawn from verified and triangulated sources to ensure accuracy and credibility. Primary sources included official state communications such as (e.g., Ministry of Foreign Affairs, military press releases), content from state-linked media (e.g., Radio Pakistan, *The Dawn*, TRT World, Global Times, Xinhua News Agency), and narratives amplified by specific state-aligned foreign social media accounts and think tanks. The scope of the study is strictly limited to the period immediately surrounding Pahalgam attack (22nd April 2025) to *Operation Sindoor* (7th -10th May 2025) to capture the real-time influence operations. Importantly, this study does not assess the military or tactical outcomes of *Operation Sindoor*; rather, it restricts itself to the information warfare domain, evaluating how Pakistan's FIMI campaign sought to delegitimise India's response, undermine its international credibility, and generate sympathy for Pakistan.

Secondary sources consist of the foundational academic and policy literature used for contextualisation and analytical framework development. These sources include: (a) Peer-reviewed journal articles and scholarly books on information warfare and strategic communications; (b) Official reports and taxonomies from international organizations, specifically the European External Action Service (EEAS) FIMI reports, which define the 5D model and the TTPs; and (c) Independent analyses and reports from global think tanks and reputable fact-checking organisations detailing the established structure and historical patterns of Pakistan's state-sponsored influence operations against India.

What is FIMI? Locating FIMI worldwide

This section delves into the conceptual understanding of the FIMI and the adopted countermeasures. FIMI which was originally constructed by the European Union (EU), but has been increasingly adopted by the other countries and international organisations.

The European Union (EU)

The acronym "FIMI", which stands for *Foreign Information Manipulation and Interference*, was first used by the European Union (EU) in 2015, when EU Member States urged the European External Action Service (EEAS) to tackle Russian disinformation campaigns following Russia's aggression against Ukraine.[9] It was further conceptualised, formally adopted and introduced into the official language of the EU in March 2022.[10] FIMI, which is often labelled as "disinformation", is identified as a growing political and security challenge for the EU and can be located in many high-level policy documents, such as the Action Plan against Disinformation (2018), the European Democracy Action Plan (2020), the European Strategic Compass (2022), and several Council Conclusions. Therefore, given its foreign and security policy dimensions, the High Representative, supported by the EEAS, assumes a leading role in addressing this issue in identifying, analysing, and responding to FIMI threats. Following this EEAS has published several FIMI Reports in 2023, 2024, and 2025 broadly by taking into account the evolving TTPs used by the malign actors. The EEAS designates Russia and China as its primary state-level threat actors, given their extensive involvement in coordinated disinformation and influence operations.

The EEAS defines “FIMI a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.[11] ”European Commission strategic communications further described that FIMI is an intentional and coordinated activity carried out by state or state-linked actors, aimed at manipulating the information environment in a deceptive, misleading, or coercive manner with the objective of undermining public trust, weakening democratic processes, and advancing geopolitical goals.

The core feature of FIMI is the deliberate use of manipulative tactics rather than the simple expression of opinions or the spread of propaganda. Unlike traditional propaganda mechanisms, FIMI seeks not merely to persuade but to confuse, divide, and destabilise, often by exploiting social or cultural tensions and eroding public trust in democratic institutions and independent media. Its methods include, beyond the distortion or fabrication of information, the artificial amplification of narratives through bots or fake accounts, the impersonation of trusted actors, and the coordination of cross-platform campaigns that exploit vulnerabilities in the open information ecosystem.[12] Therefore, FIMI is perceived as a multidimensional threat that lies at the intersection of national security, information integrity, democratic governance, and hybrid warfare**.**

The EU’s 1st EEAS FIMI Report[13] laid down the presumed objectives of FIMI on the basis of their observables and classified it into 5D’s (Dismiss, Distort, Distract, Dismay, and Divide). Each of these objectives is operationalised through specific TTPs (Tactics, Techniques, and Procedures), a modus operandi of a FIMI actor. This modus operandi of FIMI malign actors ranges from deploying diverse TTPs to launching an attack on the information space.

The EU’s 2nd EEAS FIMI Report[14] explains that TTPs are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. **“***Tactics*” are operational goals that malign actors are set to achieve, **“***Techniques***”** are actions which threat actors try to accomplish and **“***Procedures”* are specific combinations of techniques across multiple tactics/ or stages of an attack that indicate intent and may be unique for different threat actors.

TTPs are carried out in three executional phases: *Plan, Prepare and Execute.* To highlight, FIMI actors, in order to achieve their objectives, can go to that length that, in order to create legitimacy for certain claims, they chose to compromise trusted, real accounts to spread their message, while others chose to impersonate legitimate sources' information. These are the two different techniques used to achieve the same tactical objective of increasing the credibility of a claim. The next step of this tactic is to amplify content via other techniques.

Over the years, the European Union has developed a range of instruments enabling its institutions and Member States to counter-FIMI while upholding fundamental rights and freedoms. Central to this effort is the FIMI Toolbox, which provides a comprehensive and adaptable framework for addressing the multifaceted nature of FIMI.[15]Adopting a whole-of-society approach, the FIMI Toolbox is structured around four strategic pillars: Situational Awareness, Resilience Building, Disruption and Regulation, and External Action. Each of them was designed to strengthen Europe’s collective capacity to detect, deter, and respond to information threats.

The Rapid Alert System (RAS) represents the central component of the EU's comprehensive strategy to counter disinformation. It is established as one of the four pillars of the EU Action Plan against Disinformation, endorsed by the European Council in December 2018. The RAS facilitates swift information[16] exchange and coordinated responses among EU institutions and Member States. The RAS is based on open-source information and will also draw upon insights from academia, fact-checkers, online platforms and international partners. The EU FIMI Toolbox was further strengthened through the creation of the FIMI Information Sharing and Analysis Centre (FIMI-ISAC), a major step toward fostering a community-based, collaborative defence ecosystem. The FIMI-ISAC facilitates structured information[17] exchange, joint analysis, and coordinated responses among EU institutions, Member States, civil society, and other stakeholders, thereby consolidating a genuine network of FIMI defenders across the European information space. In addition to this, the EEAS FIMI Reports outline a series of analytical and operational frameworks integrated within its counter-measures toolbox, designed to strengthen the EU’s capacity to detect, analyse, and disrupt foreign information manipulation and interference activities. The EEAS Reports also provided an analysis of how the DISARM framework and Kill Chain perspectives could help develop countermeasures against FIMI.

Hence, to sum up, it is important to emphasise that FIMI disinformation operations are particularly dangerous to democratic societies because they target and exploit the openness of the liberal democratic political system. By leveraging constitutionally protected freedoms: speech, press, and political participation, the malign actors systematically transform democratic values into vectors of manipulation. Through the systematic dissemination of misleading content, conspiracy theories, and partial truths, they aim to flood the information space, disrupt rational discourse, induce apathy or polarisation and diminish societal cohesion. The purpose is just not to persuade but to erode, to exhaust citizens, corrode trust, and destabilize the epistemic foundations of democracy.[18]

Therefore, FIMI is not merely a pattern of behaviour rooted in intentional or coordinated activity, but a calculated and strategic approach to manipulate the global information environment. The threat arising from FIMI should not be viewed as a threat confined to the EU alone, but as a profound and evolving challenge to the global community, particularly to democratic nations where open information ecosystems are most vulnerable to manipulation. While the international community continues to refine its understanding and definition of FIMI, the activities of FIMI have long been in operation before the term gained formal recognition. Over the years, many countries have therefore begun to conceptualise FIMI within their own geopolitical contexts, adapting the framework to address region-specific vulnerabilities, security challenges, and media landscapes.

Taiwan

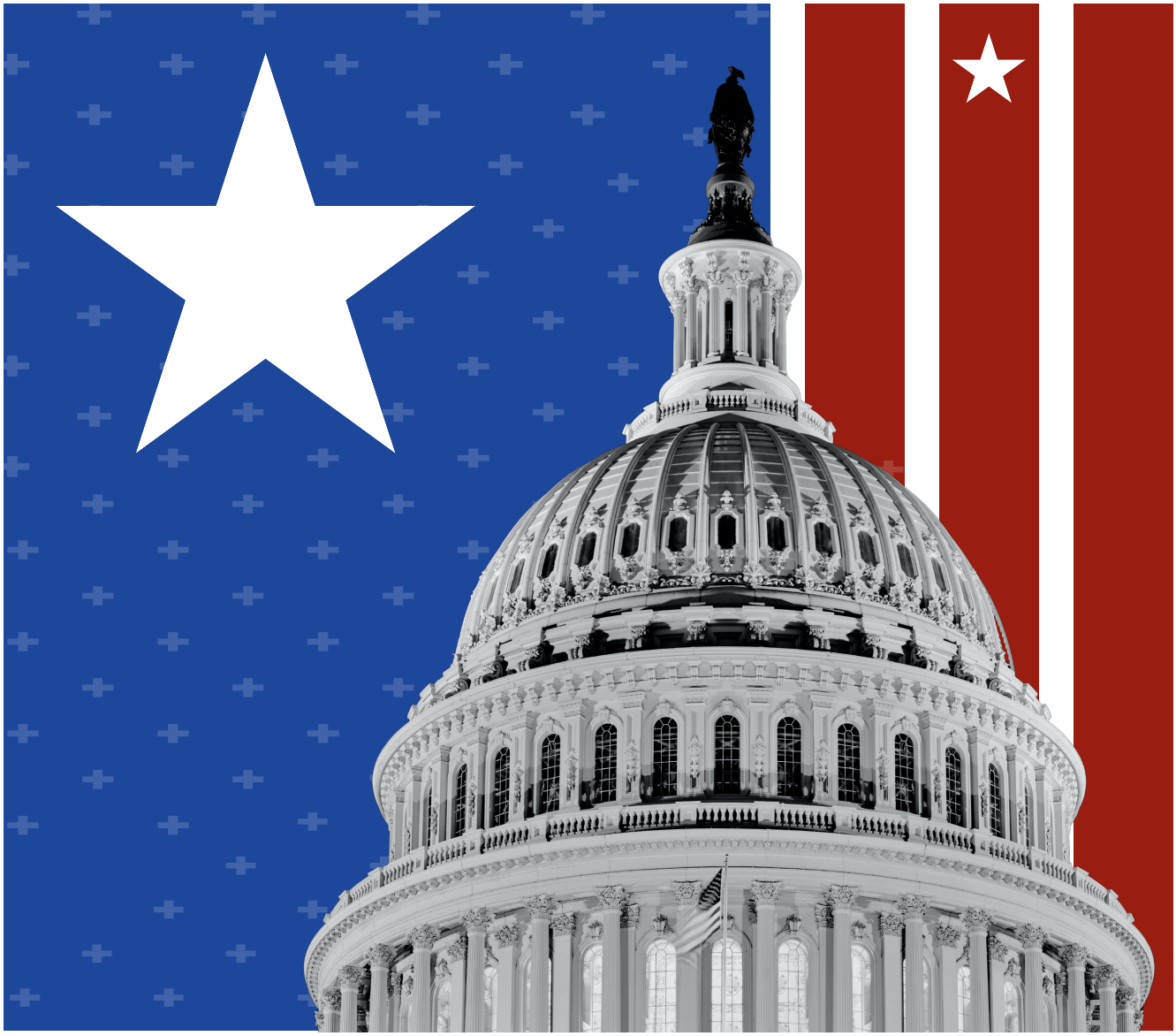
Taiwan conceptualises FIMI as a subset of cognitive warfare, situated within the broader framework of disinformation campaigns orchestrated by foreign actors.[19] Having experienced sustained and large-scale disinformation campaigns originating from the People's Republic of China (PRC),[20] Taiwan explicitly identifies the People's Republic of China (PRC) as the primary threat of FIMI targeting its democratic institutions and public opinion.[21] Its national-level response to FIMI began taking shape in 2017, with initial government initiatives and exploratory research. This effort was institutionalised in 2018 through the Executive Yuan's (EY) first central-level task force on countering disinformation, marking the government's formal entry into coordinated FIMI resilience. The Executive Yuan subsequently established a special task, led by Minister Luo Ping-Cheng, which introduced a structured approach to evaluating and addressing disinformation. This framework consisted of three evaluative elements: malicious intent, falsified content, and harmful outcome and a four-stage response model encompassing detection, debunking, containment, and discipline. This model laid the groundwork for Taiwan's comprehensive and institutionalised response to FIMI.[22]

In 2019, the Legislative Yuan advanced this agenda by enacting a "domain-specific legislation", including measures to curb external influence and enhance transparency in political communication. Taiwan's COVID-19 response in 2020 further solidified its capacity for rapid information verification and public communication. Since 2022, the government and parliament have progressively shifted their priority toward combating online fraud, recognising its growing intersection with foreign information manipulation activities. Interestingly, Taiwan's national response to countering FIMI is remarkable in both its scope and structure, encompassing multiple domains such as domestic affairs, foreign relations, national defense, economic development, agriculture, and public health and operating across central, local, and law enforcement levels. Among the key institutions spearheading this effort are the National Institute of Cyber Security (2023) and the Cognitive Warfare Research Centre (2024), both playing crucial roles in strengthening the nation's information resilience. In addition to this, the military Disinformation Rapid Response Unit was established in 2019 to strengthen public trust on the military, and fortify the psychological defence of military personnels.[23]

United States of America

Drawing an analysis from the Foreign Interference Taxonomy infographic provided[24] by the US Department Homeland Security (DHS) (2018), the US perceives FIMI, as a deliberate and coordinated actions by malign foreign governments or actors aimed at manipulating information environments to influence public opinion, sow discord, discredit democratic processes, bias policy development, or disrupt social, political, or economic stability. Their actions involve the abuse of both new and traditional media, cyber operations, and the strategic dissemination of false, misleading, or maliciously used authentic information, with the objective of undermining the interests and security of the US and its "allies"**.** Therefore, in 2016 US established, Global Engagement Center (GEC), to "recognise, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts" aimed at undermining or influencing the policies, security, or stability of the US, its allies, and partner nations, around the world.

In early January 2024, the US Department of State introduced an important new instrument for addressing this problem which is called as*: "The Framework to Counter Foreign State Information Manipulation***."** This framework replaced the existing agency GEC with new policies. The main objective of this new framework is to foster a shared understanding of the threat posed by foreign information manipulation and to define a coordinated set of action areas through which the US, together with its allies and partners, can formulate joint responses and strengthen the resilience of free and open societies.[25]



Furthermore, this framework is also instrumentalised as a tool for diplomatic engagement to address the challenges of FIMI with the purpose of deepening cooperation with like-minded partners. The framework is structured in five key action areas: (1) National Strategies and Policies, (2) Governance Structures and Institutions, (3) Human and Technical capacity, (4) Civil society, independent media, and Academia and (5) Multilateral engagement.[26] The US explicitly identifies the Russian Federation and the People's Republic of China (PRC) as the principal foreign actors engaged in FIMI against the US and its allies.[27]

Hence, the US treats FIMI as a transnational threat and a threat to its National Security, extending to its allies and partners. It underpinned that authoritarian states manipulate information to corrode the foundations of free and democratic society by influencing the public discourses, distorting crucial national and global debates and weakening the democratic institutions.[28]

North Atlantic Treaty Organisation (NATO)

The NATO conceptualizes FIMI within a broader framework of information threats, defined as intentional, harmful, manipulative, and coordinated activities, including information manipulation and interference by foreign actors and disinformation spread through traditional and social media, designed to create confusion, deepen divisions, destabilise societies and ultimately weaken the Alliance. NATO strictly states that it does not prescribe what people can or cannot say and protects freedom of expression when it is a question of information threat. Its response framework includes short, medium, and long-term measures as well as proactive measures. This response is built around four core functions: (1) understanding the information environment, (2) preventing and reducing the effectiveness of information threats, (3) containing and mitigating incidents, and (4) recovering stronger by learning lessons from information threats.[29] The NATO recognises Russia and China as the primary threat actors.

NATO has significantly reinforced its alert systems, expanded real-time information-sharing mechanisms, and intensified coordinated responses, particularly through strategic communications and further strengthening cooperation with partner nations to ensure a unified, resilient, and proactive stance against information threats.[30] Its Strategic Communications Centre of Excellence (StratCom COE) serves as a key hub for analysing FIMI operations and providing strategic guidance to member states. Complementing NATO's efforts, the G7 has formally recognised FIMI as a shared and escalating threat to democratic societies and the integrity of global information ecosystems. Since the establishment of the G7 Rapid Response Mechanism (RRM) in 2018, member states have prioritised a coordinated and collective approach to countering state-sponsored disinformation and influence campaigns. Successive G7 communiqués and summit declarations have consistently underscored the importance of information sharing, coordinated attribution, and joint countermeasures to strengthen democratic resilience against malign information operations.[31]

India

In the case of India, it does not maintain a standalone governmental definition of FIMI or Disinformation, but in practice, New Delhi has been addressing this challenge through election-integrity measures, platform obligations, fact-checking, and referencing “FIMI” in Quad statements.

The Election Commission of India (ECI), through its 2024 guidelines on the *“Responsible and Ethical Use of Social Media Platforms,"* identified manipulated, AI-generated, and deepfake content as major threats to electoral integrity. The ECI warned that such material can distort voter perception, deepen societal divisions, and erode trust in the democratic process. Emphasizing its constitutional duty to ensure free and fair elections, the Commission invoked legal provisions under the Model Code of Conduct, the Information Technology Act (2000), The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the Indian Penal Code and framework of the twin acts namely the Representation of People Act, 1950 and 1951 to regulate fake information/disinformation/misinformation and digital manipulation. This guideline situates election-related disinformation[32]within India’s broader framework of information security. This aligns conceptually with global efforts to counter-FIMI, however there is no such explicit reference.

On the other hand, the Government of India has designated the Press Information Bureau (PIB), Fact Check Unit (FCU) under the Ministry of Information and Broadcasting, as the official mechanism to counter misinformation. It was established in November 2019, with the objective to deter fake news, provide a public reporting channel, and verify information related to government policies and initiatives. Acting as suo motu or on public complaints, it monitors, detects, and counters disinformation campaign about the Government of India, thereby promoting transparency and information integrity.[33]

From a strategic standpoint, India's approach to FIMI aligns with the broader spectrum of hybrid and non-kinetic threats combining cyber, psychological, and narrative dimensions. In the Quad Joint Statement (2024), the Government of India, alongside the US, Japan, and Australia, reaffirmed a collective commitment to protecting the integrity of the information environment. The statement underscores a shared recognition that FIMI, including disinformation which poses a growing threat to democratic discourse, public trust, and international stability. It explicitly identifies FIMI as a tactic aimed at sowing discord and manipulating domestic and international affairs, thus framing it as a strategic challenge rather than a mere communication issue.[34]

In conclusion, the absence of clear and official definitions of *disinformation*, *misinformation*, and FIMI underscores a critical policy gap in India's information governance landscape. While the Government of India has introduced mechanisms such as the Press Information Bureau's Fact Check Unit (FCU) and issued regulatory measures under the Information Technology Rules (2021), these initiatives primarily address content moderation and fact verification rather than establishing a unified conceptual framework. Without explicit definitions, it becomes challenging to distinguish between malicious foreign interference, domestic political misinformation, and unintentional information errors, thereby limiting the effectiveness of both preventive and punitive responses.

Examining Pakistan's FIMI architecture

Reflecting on the present context, Pakistan's FIMI ecosystem consists of a layered network of Official State actors, State-backed or Aligned media, Foreign Media, Think Tanks, Social media platforms, and X influencers. The dynamics of *Operation Sindoor,* which extended the conflict beyond the traditional battlefield into the cognitive and informational spheres, exposed the operational depth of Pakistan's FIMI ecosystem. This episode of conflict demonstrated how state institutions, state-linked media, and aligned digital networks were activated in tandem to propagate disinformation, misinformation, and projected influence across both domestic and international audiences. In doing so, *Operation Sindoor* provided a critical case study of how hybrid conflict is increasingly fought not only through conventional military means but also through strategically orchestrated information warfare, further supplemented by transnational actors and networks.

By drawing upon the conceptual framework established in the European Union's European External Action Service (EEAS) FIMI Reports, this study identifies that Pakistan's FIMI architecture can be categorised into four interrelated blocs. *Firstly,* the Official state apparatus, which encompasses the Inter-Services Intelligence (ISI), which is central to the FIMI ecosystem, Inter-Services Public Relations (ISPR) and the Ministry of Foreign Affairs (MFA). *Secondly,* State-linked media outlets and think tanks such as Radio Pakistan, The Dawn, and think tanks such as Pakistan Strategic Forum (PSF), and the Institute of Strategic Studies Islamabad (ISSI). Thirdly, State-backed and aligned social media networks, that can be further divided into a) state-run propaganda accounts and b) covert social media accounts and lastly, Foreign Media and Social media Influencers who actively amplify pro-Pakistan narratives. Together, these channels, both overt and covert, form the backbone of Pakistan's FIMI playbook. This structural categorisation has been developed through analytical extrapolation from the EEAS FIMI framework, which is visually represented in the chart below.

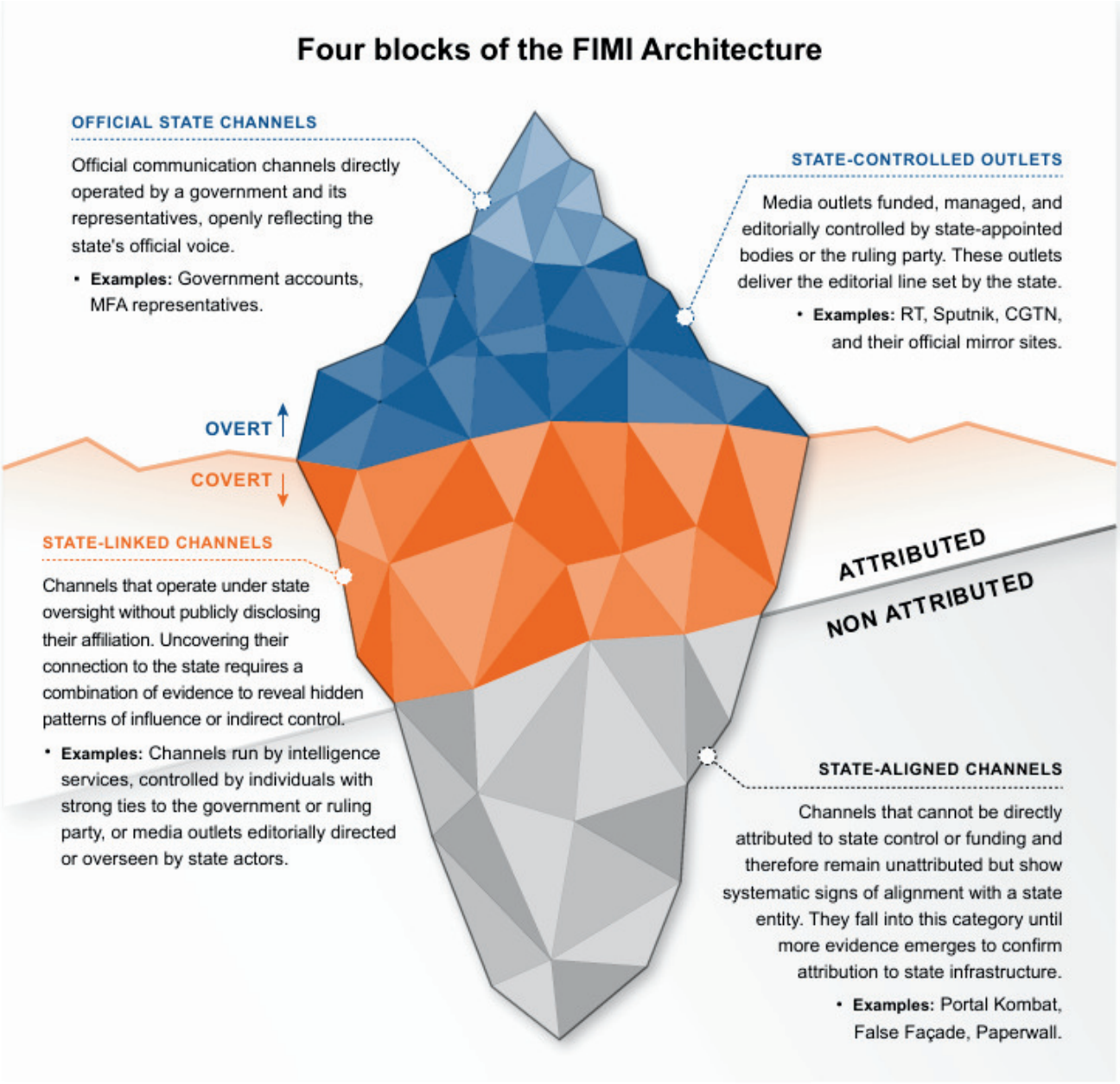


Figure 3: FIMI Iceberg - The four blocks that compose the FIMI Architecture

Figure 1
Source: EEAS FIMI 3rd Report

What differentiates this phase of India and Pakistan conflict from earlier episodes is Pakistan's ability to externalise its disinformation campaigns, drawing active amplification from foreign media and X influencers. Their involvement not only broadened the reach of Islamabad's narratives but also embedded them within global information ecosystems, illustrating how FIMI can weaponise transnational networks to shape perceptions far beyond the immediate conflict zone. In doing so, the case of *Operation Sindoor* underscores how FIMI transcends national boundaries, weaponising transnational networks to shape perceptions, manufacture legitimacy, and influence debates far beyond the immediate conflict zone.

Dominant Narratives of Operation Sindoor Driven by Islamabad Disinformation Campaign

Various competing narratives originated from Pakistan during *Operation Sindoor,* however, this report captures the ones that dominated the landscape.

1. *Operation Sindoor* is a false flag operation of India which is orchestrated to defame Pakistan.[35]
2. *Operation Sindoor* is an unprovoked act of aggression and a blatant violation of Pakistan's sovereignty and territorial integrity.[36]
3. India's missile strikes damaged Pakistan's civilian infrastructure, religious sites and killed civilians, including women and children.[37]
4. *Operation Sindoor* have exposed the BJP's and PM Narendra Modi's hateful politics against Muslims, to both the Indian people as well as to the international community. [38]
5. Pakistan has defeated India, both in conventional warfare and on diplomatic and narrative fronts. [39]
6. India is sponsoring terrorism against Pakistan through Afghanistan and Balochistan.[40]
7. Pakistan is a victim of Indian state-sponsored terrorism, who has sacrificed armed forces, law enforcement agencies, and civilians for both national and global peace and suffered millions of dollars of economic loss.[41]
8. India is actively engaged in transnational aggression within and outside Pakistan, and also killing Sikh minorities in Canada and targeting their activist in the US and Australia.[42]
9. Indian Army is in a state of panic and killing its own Sikh soldiers, and the incident has left the Sikh unit enraged.[43]
10. India is attempting to weaponise water by diverting Indus River tributaries, threatening Pakistan's agricultural future and escalating conflict.[44]
11. Pakistan have destroyed 8 Indian jets, including 4 Rafale jets, with Chinese-made PL-15E long-range missiles, launched from J-10C fighters.[45]
12. Pakistan have crushed the S-400 air defence system with JF-17 Thunder jets[46] and damaged the Bathinda and Sirsa Airfields. [47]
13. India has lost international support and suffered a major diplomatic setback.[48]
14. Operation Bunyān un Marsoos marks a decisive success on all fronts against India. [49]
15. India has surrendered to Pakistan, with the Indian Army raising a white flag at the Chora Complex along the Line of Control, acknowledging its defeat. [50]
16. Pakistan dictated the US-brokered peace after securing a calculated victory against India.[51]

Decoding Operational Goals of Pakistan's FIMI Disinformation Campaign during Operation Sindoor

Immediately after the Pahalgam attack and following Operation *Sindoor*, India was targeted by a concerted FIMI disinformation campaign orchestrated by Pakistan. As evident, Pakistan's response to India's *Operation Sindoor* was not limited to diplomatic denials and military posturing but led to the further escalation into a calculated disinformation campaign designed to undermine India's strategic and diplomatic standing. From ISI to state-backed and aligned media to diplomatic channels, each arm played a coordinated role in constructing and amplifying false narratives. Meanwhile, Pakistani social media networks and pro-Pakistani media and X foreign influencers amplified and circulated doctored visuals, including video game footage and old conflict clips, falsely claiming Pakistani strikes on Indian military bases.

The following table decodes Pakistan's systematic FIMI disinformation campaign, outlining its presumed strategic goals, operational objectives, and illustrative examples.

Strategic goals	Objectives of FIMI	Examples
To delegitimise India's response to Pahalgam terror attack, framing both Pahalgam terror attack and "*Operation Sindoor*" as "False flag Operation" and shift narratives in Pakistan's favour.	-To promote claims through media interviews, think tank publications, and coordinated messaging on social media. -To undermine international support for India and sow doubt about the legitimacy of its security operations. -To reinforce narratives that portray Pakistan as a victim of external manipulation rather than a source of regional instability	-Raoof Hasan, a former special assistant to ex-Prime Minister Imran Khan, told *Al Arabiya English* that the Pahalgam attack was a 'false flag operation' and part of what he described as a decades-long pattern of 'regional adventurism' designed to destabilise Pakistan.[52] - Pakistan's think tank, the *Institute of Strategic Studies Islamabad (ISSI),* published an issue brief framing *Operation Sindoor* as a false flag operation. The brief argued that the Modi government instrumentalised the attack to advance its domestic political agenda as well as its broader strategic objectives vis-à-vis Pakistan.[53]
To malign India's international image and portray it as an aggressive and repressive state.	- To target India's global posture, with an intention on shaping perceptions among human rights organisations, Western governments, and diaspora communities.	-Falsely propagated that Bunyan-un-Marsoos and Ma'raka-e-Haq[54] achieved a massive success of Pakistan's operations like and claim that these operations are God-sent moment to asserted that Pakistan's international standing.[55]

	- To selectively highlight human rights issues in FIMI disinformation campaigns in order to evoke strong emotional responses and construct a narrative of moral equivalency or even moral superiority in favour of Pakistan. -To manipulate diplomatic developments such as visa suspensions or persona non grata declarations to portray the bilateral relationship as hostile primarily due to Indian aggression rather than mutual deterioration.	
Undermine India's military credibility and malign its reputation by questioning their professionalism, capacity and ethical conduct of Indian Armed forces.	-To spread fabricated and false claims of military defeat. -To sow doubts about India's military preparedness and internal cohesion -To circulate fabricated reports claiming Indian strikes harmed civilians implying violations of international humanitarian norms. -To erode public trust in the government and armed forces and weaken the morale of the armed forces	-One of the most prominent false claims widely circulated during the disinformation campaign was the alleged capture of pilot Shivangi Singh. -Pakistan's social media accounts also shared a fabricated documents on Indian Army war preparedness[56] and the narrative of surrender and white flag is widely circulated. [57]

Tarnish Rafale's combat reputation in both Indian and global sphere; and portray China's J-10C as superior aircraft.	-To prevent Rafale from gaining a psychological edge by presenting Chinese J-10C as an alternative (amplified by China) [58] and present Pakistan air defence as highly capable and superior. - To undermine Indian public confidence by publishing opinion pieces and media narratives that questioned the aircraft's operational effectiveness, portraying it as vulnerable, wasteful and strategically ineffective.	- Recirculation of old and unverified crash photos as alleged Rafale wreckage, mislabelled videos of unrelated fighter crashes, and amplified social media hashtags on X and Facebook to portray the Rafale as vulnerable. -Pakistan has asserted Rafale being shot down by the Chinese-made PL-15E long-range missiles, launched from J-10C fighters.[59] - Pakistan, through its state-backed and aligned media, propagated narratives that denigrated the Rafale by presenting selective comparative analyses aimed at highlighting perceived weaknesses of the aircraft.[60] - The official X account of the Government of Pakistan also shared a footage from the video game ARMA 3, falsely portraying it as footage of an Indian jet being shot down.

To leverage the Indus Waters Treaty (IWT) suspension to shape international perception of India as treaty violator and gain diplomatic support.	-To project India as a regional aggressor and violator of international norms. - To internationalise the Indus Waters Treaty dispute by shifting it from bilateral mechanisms to multilateral forums where Pakistan can exert greater diplomatic leverage.	- Pakistan's narratives portrayed India's suspension of the Indus Waters Treaty as illegal and an attempt to 'weaponise' water resources, framing it as a dramatic tactics and further provoking international attention against India.[61]
Revive and internationalise of Kashmir question	-To portray Kashmir as an unresolved question of self-determination and human rights - To mobilise global diplomatic pressure on India and reframe the conflict from a bilateral matter to one requiring multilateral intervention -To leverage membership of Organisation of Islamic cooperation (OIC) to defame and incite hostility attitude against India	-Amidst heightened tensions, Pakistan's National Security Committee (NSC), hastily framed Kashmir as an unresolved UN dispute, portraying unrest as an "organic backlash" to India's state oppression and sought to depict India as a systematic violator of human rights to draw international attention. [62] -There are numerous instances where Pakistan exhaustingly uses OIC[63] to tarnish India's image by playing the religion card and drawing misleading parallels between Kashmir and Gaza. -Repeatedly internationalising the Kashmir dispute at the UNSC with the intent to cast India as an aggressor.[64]

Figure 2
Source: Author

Dissecting Tactics, Techniques and Procedures (TTPs) of Islamabad

TTPs provide a structured understanding of adversarial behaviour of the actors, outlining the strategic intent (*why*), the methodological approach (*how*), and the specific operational execution (*how exactly*) of disinformation activities.[65] Therefore, Tactics denotes the strategic goals and objectives that threat actors or malign state seek to achieve, Techniques are the methods how they used it to achieve those objectives, and Procedures details the specific, often unique and implementation of techniques across multiple tactics or attack phases, thereby reflecting the threat actor's intent.[66]

Tactics

According to the EEAS, [67] the tactics are conceptualised through the use of the "5D model": dismiss, distort, distract, dismay, and divide, each representing a different way in which malign actors seek to influence and disrupt democratic societies. Building on this understanding, which frames disinformation campaign tactics around these five objectives, this study applies the 5D model to evaluate Operation Sindoor. The evidence suggests that Pakistan employed all five dimensions of the framework in its information operations related to the campaign.

5D's	Illustrative Explanations
Dismiss	Pakistan's Deputy Prime Minister Ishaq Dar moved a resolution in the country's Parliament, dismissing any links between Pakistan and the attack. The resolution stated that it rejected all "*frivolous and baseless attempts*" to connect Pakistan to the incident, condemning what it called an "*orchestrated and mala fide campaign*" by the Indian government. This move exemplifies Islamabad's attempt to dismiss responsibility, downplay its role, and deflect international scrutiny.[68] This has been followed by the systematic narrative construction, amplification of false flag operation allegations, dissemination of narratives in the domestic and international media,[69] and on various social media platforms.

Distort	Following the Pahalgam attack, Pakistani PML-N Senator Irfan Siddiqui framed the Pahalgam incident as propaganda against Pakistan, calling it a "false flag operation" timed with diplomatic visits.[70] He asserted that India has habit of staging such incidents around high-profile diplomatic visits is not new. On the other hand,[71] PHJK Chairman Uzair Ahmed Ghazali and Federal Minister for Information Attullah Tarar distorted the narrative by framing the incident as a political ploy by the Modi regime and orchestrated by the Indian state, further drawing a comparison with the Pulwama attack.[72] This coordinated narrative construction exemplified the Distort tactic, as it shifted focus away from the attack itself and redirected global attention toward India's credibility and political conduct.
Distract	Islamabad's Barrister Sultan Mahmood Chaudhry sought to distract from Pakistan's culpability by reframing the discourse around broader political issues such as reviving the Kashmir dispute, criticizing India's abrogation of Articles 370,35A, and Indus Water Treaty, invoking narratives of Indian aggression and Hindutva ideology, and further attempting to pin India as a "global terrorist" by linking it to alleged acts of terrorism in Canada and Pakistan.[73] This was all executed under the broader *Distract* mode of Pakistan's FIMI strategy, which aimed at provoking international scrutiny against New Delhi about human rights and transnational terrorism, and ultimately shifting the narrative away from Pakistan's role in the Pahalgam incident.
Dismay	Pakistan employed the "Dismay" tactic by amplifying escalatory rhetoric designed to instil a fear of large-scale conflict. Defence Minister Khawaja Muhammad Asif[74] warned that the Kashmir dispute could lead to an "all-out war" with India, while Minister Hanif Abbasi[75] declared that "130 nukes are kept for you" in a direct threat to New Delhi.

	Similarly, Army Chief Asim Munir threatened to bomb any dam India might construct on the Indus River. These statements were intended to generate alarm, reinforce the image of imminent danger, and pressure the international community into viewing Pakistan as a vulnerable actor forced into confrontation. On the other hand, Pakistan amplified fears of cyber insecurity by spreading narratives around the so-called "Dance of the Hillary"[76] virus, allegedly targeting Indian users. By framing it as a Pakistani cyber offensive, the campaign sought to create panic, erode public confidence in India's digital resilience, and project Islamabad as possessing asymmetric capabilities beyond conventional domains. In addition to this, Pakistan also attempted to launch a cyberattack targeting defence infrastructure with a misleading email containing a PDF titled "OP Sindoor Lessons For Action".[77] These cyber-panic narratives complemented the *Dismay* objective, reinforcing an atmosphere of fear and vulnerability.
Divide	As observed, Pakistan deployed divide tactics to spread disinformation, with the deliberate objective of diverting the attention of both regional and global audiences. Rather than allowing focus to remain on the Pahalgam incident itself, Pakistan rushed to redirect and divide international attention by amplifying alternative grievances, reviving past accusations, and framing India as both oppressive at home and destabilising abroad. For instance, Federal Minister for Information Attaullah Tarar used the Pahalgam attack to divide public opinion and appeal to the international community by amplifying existing tensions. He asserted that Sikh minorities are targeted in the United States, Canada, and Australia, portraying that India is engaged in state-sponsored and transnational aggression. This narrative sought to defame India, frame it as a common enemy, and ultimately divert or divide attention from the actual incident.[78] He further blatantly emphasised that Pakistan is sacrificing its armed forces, law enforcement agencies, and civilians in the pursuit of national and global peace.[79]

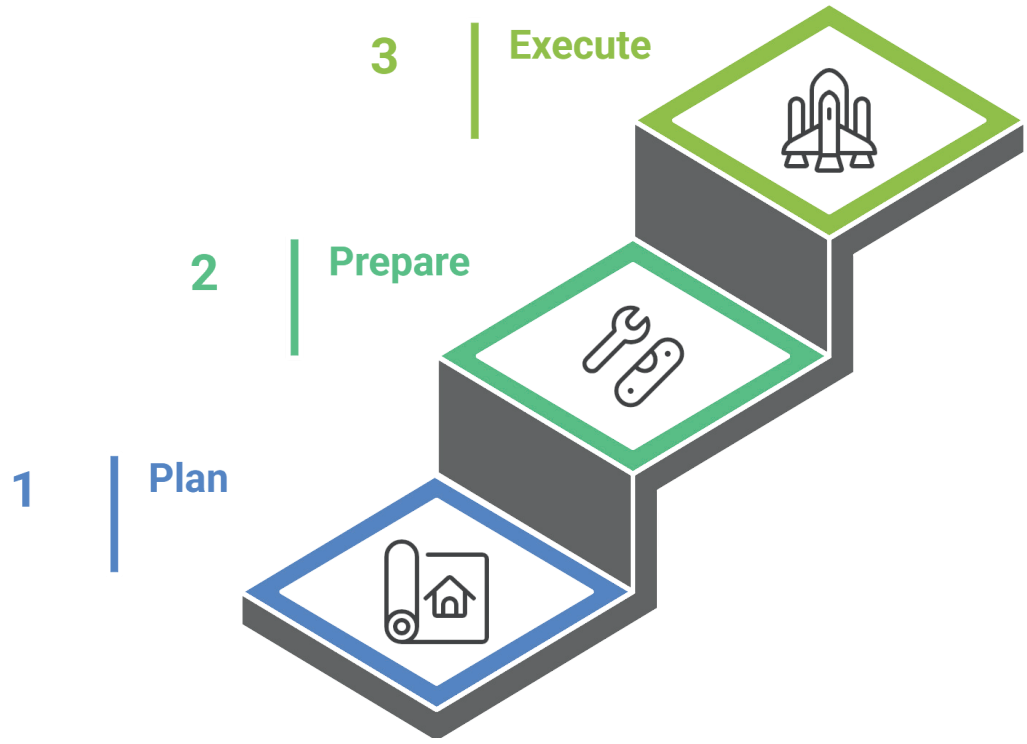
	On the other hand, Pakistan's FIMI disinformation campaign sought to divide Indians by claiming that Prime Minister Modi's "hateful politics" had been exposed, with both domestic and international audiences who are rejecting the BJP's alleged anti-Muslim campaign following the Pahalgam attack. Narratives accused the Modi government of fuelling Hindu-Muslim riots and stripping Muslims of their rights.[80] Pakistan also attempted to sow division within the Indian Army by circulating a fabricated story that Sikh soldiers had been killed by the army and that a senior Sikh Officer had been arrested.[81] This highlights how Pakistan employed the tactic of division to further its objectives.

Figure 3
Source: Author

Taken together, these operations illustrate that Pakistan did not employ the 5Ds in isolation but as interdependent tactics, where each fed into the other to amplify fear, confusion, and mistrust. The result was a sophisticated campaign that blurred accountability, weakened democratic resilience, and ensured the crisis narrative remained contested across domestic, regional, and global levels.

Techniques

Techniques refer to the stages of disinformation influence operations conducted by malign state actors, typically carried out in three phases: Plan, Prepare, and Execute.[82] The table below, adapted



Plan	Prepare	Execute
-Degrade adversary -Discredit credible sources -Facilitate state propaganda -Geographic segmentation	-Developed image-based content -Developed video-based content - Formal diplomatic channels -Reframe Context -Leverage existing narratives -Respond to breaking news, events or active crisis -Prepare assets impersonating legitimate entities -Appropriate content - Distort facts - Aggregate information into evidence collages -Develop new narratives -Deceptively edit images (cheapfakes) -Obtain private documents -Leverage existing inauthentic news sites -Reuse existing content -Co-opt trusted sources -Use hashtags -Create inauthentic documents -Create inauthentic websites -Amplify existing conspiracy theory narratives -Develop AI-generated videos (deepfakes) - Develop memes -Create hashtags and search artifacts -Deceptively labelled or translated	-Post across platform -Flooding the information space -Call to action to attend -Post across groups -Continue to amplify -Dox -Encourage attendance at events -Cross-posting -Inauthentic sites amplify news and narratives

Figure 4
Source: 1st EEAS FIMI Report

The *first phase,* "Plan", reflects the strategic goals and objectives guiding FIMI actors. Pakistan's disinformation campaign demonstrated meticulous planning in orchestrating FIMI influence operations against India following the Pahalgam terror attack and *Operation Sindoor* (refer to the table (Fig. 2) of strategic goals). For instance, Pakistan swiftly mobilised to frame the incident as a "false flag operation", seeking to deflect blame and discredit India's counter-terror narrative. This immediate narrative manipulation underscored a premeditated effort to shape both domestic and international perceptions even before verified information emerged.

The second and third phases, **"**Prepare" and "Execute", refer to the diverse techniques employed by Pakistan to undermine India's credibility and public perception. These two stages involve from producing image and video-based content to crafting new narratives to shape opinion and disseminating across the various official and social media platforms. During *Operation Sindoor*, for example, numerous recycled and AI-generated visuals surfaced online.[83] A notable example was Pakistan's claim of shooting down a Rafale jet near Bahawalpur, an assertion later debunked, as the visuals were traced to the crash of an Indian MiG-29 fighter jet in Barmer, Rajasthan, in September 2024.[84] In addition, both cheapfakes and deepfake videos were deployed to mislead audiences and gain virality on social media platforms. One such instance was a video purporting to show External Affairs Minister Dr S. Jaishankar apologising, allegedly admitting that India had falsely blamed Pakistan for the Pahalgam terror attack. Concurrently, memes framed Operation Sindoor as a failure for India, using satire and nationalistic humour to mock Indian actions and boost Pakistani pride.[85] These examples highlight the coordinated use of technical deception and narrative manipulation to influence both domestic and international opinion.

In continuation, one of the most prominent techniques mirrored in Pakistan's preparedness and position to use its diplomatic channels to launch a disinformation campaign against India. For instance, MFA Pakistan leveraged its diplomatic channels when, on 8 May, it issued a statement rejecting India's claims of cross-border strikes in Pathankot, Jaisalmer, and Srinagar. The MFA instead accused India of running a "reckless propaganda campaign",[86] when in reality Pakistan has launched an attack on several locations in the Northern states.[87]

In terms of reframing the context and leveraging existing narratives, Pakistan drew heavily on long-standing narratives rooted, for example, in the Kashmir conflict and also the Balakot crisis of 2019. Since the Balakot airstrikes, Pakistan has consistently framed India as a "regional aggressor" that manufactures "false flag" incidents to advance its political agenda or justify military action in Kashmir. This framing re-emerged during Operation Sindoor, with Pakistani officials and ISPR-linked media swiftly branding the Pahalgam terror attack as another false

By invoking the Kashmir victimhood narrative, Pakistan tapped into decades of emotive discourse portraying itself as the defender of Kashmiri Muslims against Indian "occupation." Social media campaigns and digital troll farms revived hashtags #FreeKashmir, #StopIndianAggression, and #EndIndianOccupation, as well as crafted new ones like #SindoorFail and #KashmirUnderAttack, linking the strikes under *Operation Sindoor* to alleged repression in Kashmir.[88] Pakistan executed this plan by creating thousands of fake social media accounts impersonating Indian citizens and officials to spread coordinated disinformation. Investigations by the *CyberPeace Foundation* and *DisInfoLab India* (2025) revealed that India banned over 3,200 such accounts, including 480 high-reach ISI-linked operatives, used to amplify anti-India narratives, circulate fake visuals, and manipulate online discourse.[89]

On the other hand, new narratives emerged, such as pinning India as a 'terrorist state", accusing of sponsoring transnational terrorism against the Kashmiri people, Pakistan, and its citizens in Canada.[90] Simultaneously, Pakistan positioned itself as "the frontline state in the war against terrorism," recasting Indian precision strikes as unprovoked aggression against a responsible actor combating extremism. Further, Pakistan demonstrated a pre-planned and reactive posture, swiftly exploiting breaking news from India to advance its agenda. E.g., Immediately after Prime Minister Modi's post-ceasefire public address, several Pakistani political leaders responded by branding him a *"fascist"* and a *"defeated gambler,"* signalling the existence of an organised narrative response mechanism rather than spontaneous political commentary.[91]

KASHMIR PROPAGANDA

There is also ample online evidence showing how Pakistan recycled old content to fabricate events during Operation Sindoor. For instance, several Pakistan-based accounts widely circulated an image claiming that a Rafale fighter jet had been shot down by Pakistani forces. However, a reverse image search revealed that the photo had no connection to Operation Sindoor. In reality, it depicted a MiG-21 crash[92] from a training exercise in Punjab in May 2021, which was later confirmed by India's PIB Fact Check Unit. This incident highlights Pakistan's routine use of recycled visuals and misattributed media to lend false credibility to its disinformation campaigns. It clearly underscores the level of premeditation and preparedness behind these operations.

In the case of co-opting trusted sources, Pakistan co-opted trusted sources during Operation Sindoor by channelling its narratives through sympathetic journalists, state-aligned media outlets, diaspora influencers, and affiliated think tanks. Media platforms and Islamabad-based policy institutes amplified ISPR-driven talking points, giving disinformation an appearance of analytical legitimacy and independent validation. For example, the Pakistan Strategic Forum, a defence-oriented digital platform with known links to state narratives, amplified false claims about the downing of Indian Rafale jets, helping spread the disinformation across social media networks.[93]

Pakistan's level of preparedness was evident when Islamabad circulated a forged document purportedly detailing the Indian Army's operational readiness. The fabricated file, shared widely across various social media platforms, was designed to undermine troop morale and erode public confidence in India's military capabilities.[94] It is notable to highlight that, soon after the April 22, 2025, attack, the Pakistan-linked APT[95] group Transparent Tribe (APT36) launched credential-phishing and malware campaigns using fake domains impersonating the Jammu & Kashmir Police and Indian Air Force. A malicious PDF titled as an official "Report Update Regarding Pahalgam Terror Attack.pdf" document created on April 24, 2025, by the alias *"Kalu Badshah"* exemplified how the group rapidly exploited the crisis to target Indian government and defence personnel.[96]

Since 2022, this Pakistan-linked APT36(Transparent Tribe) has significantly evolved its tactics, techniques, and procedures (TTPs), adopting new distribution methods and tools to enhance its reach and persistence. The group registered multiple spoofed domains mimicking the official *Kavach* authentication app portal and leveraged Google Ads' paid search feature to promote these malicious sites to the top of search results for Indian users, thereby increasing the likelihood of credential theft and malware delivery.[97] As informed by India's Ministry of Information and Broadcasting, the government blocked over 1,400 URLs on digital media during Operation Sindoor.[98] These incidents illustrate how cyber

operations and disinformation campaigns functioned in tandem, as both fronts moved together to undermine India's security and credibility. With technical intrusions reinforcing narrative warfare, these two domains, cyber-espionage and information manipulation, are deeply intertwined, enabling Pakistan to both steal sensitive data and shape public perception simultaneously.

In the context of amplifying existing conspiracy theory narratives, again, the narrative of a "false flag operation" has emerged as a classic conspiracy theory propagated by Pakistan to undermine India's credibility in the international arena. Every message comes with intention and provocation to grab the attention of the international community and hold India responsible for orchestrating these attacks to delegitimise Pakistan and manufacture a pretext for retaliation. It is observed that, from the Pulwama attack and Balakot strikes (2019)[99]to the Pahalgam attack and Operation Sindoor (2025), this blasphemous and baseless false flag conspiracy theory and its narrative have been consistently and aggressively propagated by Pakistan.

Soon after the Pahalgam attack, Pakistan amplified existing narratives framing these crises not as isolated incidents but as part of a recurring pattern of false flag operations allegedly orchestrated by India for its own political objectives and military actions. Drawing on past attacks, Mumbai (2008), Pathankot (2016), Uri (2016), and Pulwama (2019), Pakistan's narratives implicated that India slants these false flag operations are designed to deceptively attribute responsibility to Pakistan.[100] This trend shows how Pakistan uses these narratives to attack India and discredit its counter-terrorism efforts, portraying genuine security operations as staged or politically motivated. By consistently framing terrorist incidents as "false flag" operations, Pakistan seeks to shift blame, confuse international perception, and weaken India's credibility in global forums, while simultaneously deflecting attention from militant groups operating from its own territory.

Procedures

By analysing the intersection of tactics and techniques, it is possible to identify the underlying procedures employed in Pakistan's disinformation operations. These procedures can be conceptually illustrated through TTP (Tactics, Techniques, and Procedures) frequency heat charts, similar to those presented in the European Union's EEAS study. However, as this research is qualitative in nature, it does not generate quantitative data**.** Instead, the EEAS heat flow chart is referenced here to conceptually demonstrate how various techniques, such as image-based content manipulation, deepfake production, or coordinated account network, are employed to achieve specific strategic objectives. The chart thus serves as an explanatory framework, enabling a clearer understanding of procedural patterns within disinformation campaigns. An example of this framework, along with the EEAS explanation of procedures, is provided below for contextual reference.

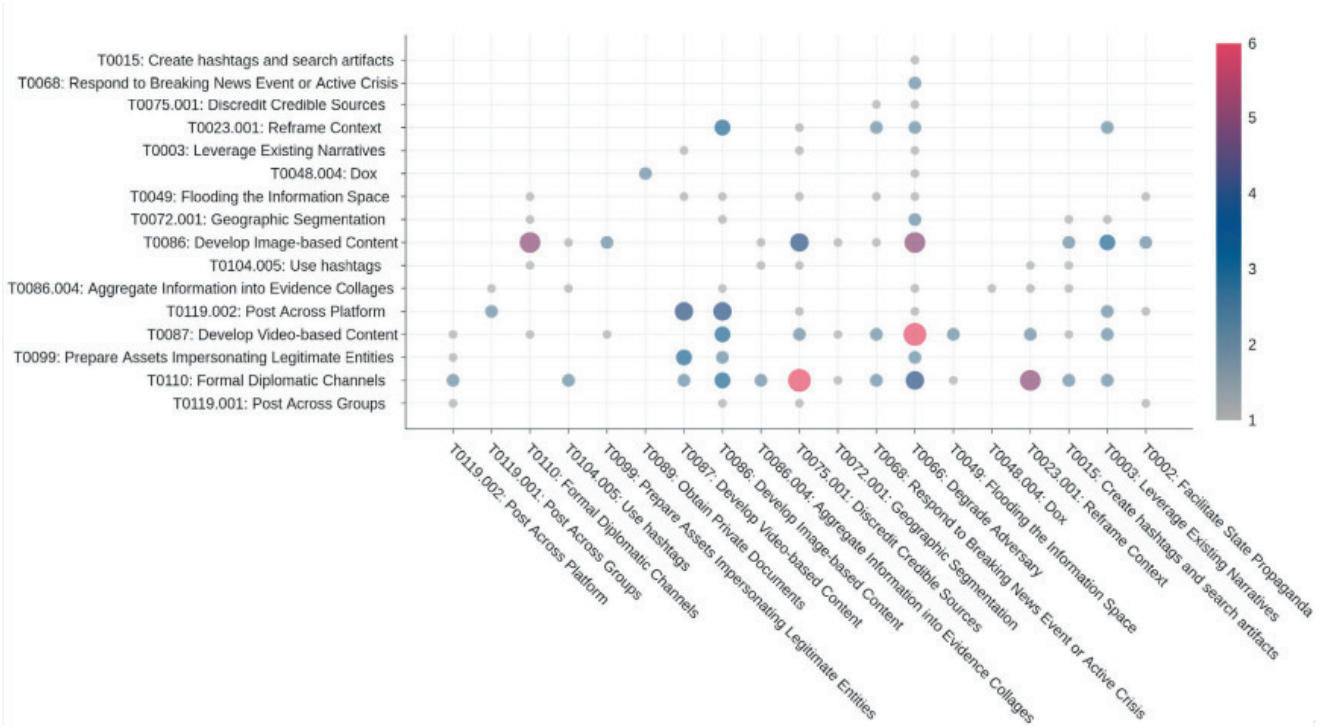


Figure 5
Source: 1st EEAS FIMI Report

Role of Foreign Media

This study highlights a major development in Pakistan's state-driven disinformation campaign against India following *Operation Sindoor*. Pakistan not only instrumentalised its state-controlled media and diplomatic channels but also strategically exploited foreign media outlets and influential X personalities to amplify both disinformation and misinformation, to disseminate narratives, cultivate confusion, deliberately targeting international audiences to delegitimise India's actions during *Operation Sindoor*, but also public opinion in India.

This study examines the role of state-run foreign media (China, Turkey and Azerbaijan) and X foreign influencers who propagated Pakistan's anti-India narratives during *Operation Sindoor*. Two critical observations are made: *Firstly,* the foreign media and X accounts rapidly amplified Pakistan's narrative, often borrowing the talking points directly from Islamabad's state-run media and official military briefings. *Secondly,* there was a deliberate and sustained effort to portray Pakistan as holding the upper hand during the conflict, particularly through glorified coverage of "Operation Bunyan-un-Marsoos" while consistently framing India as the aggressor.

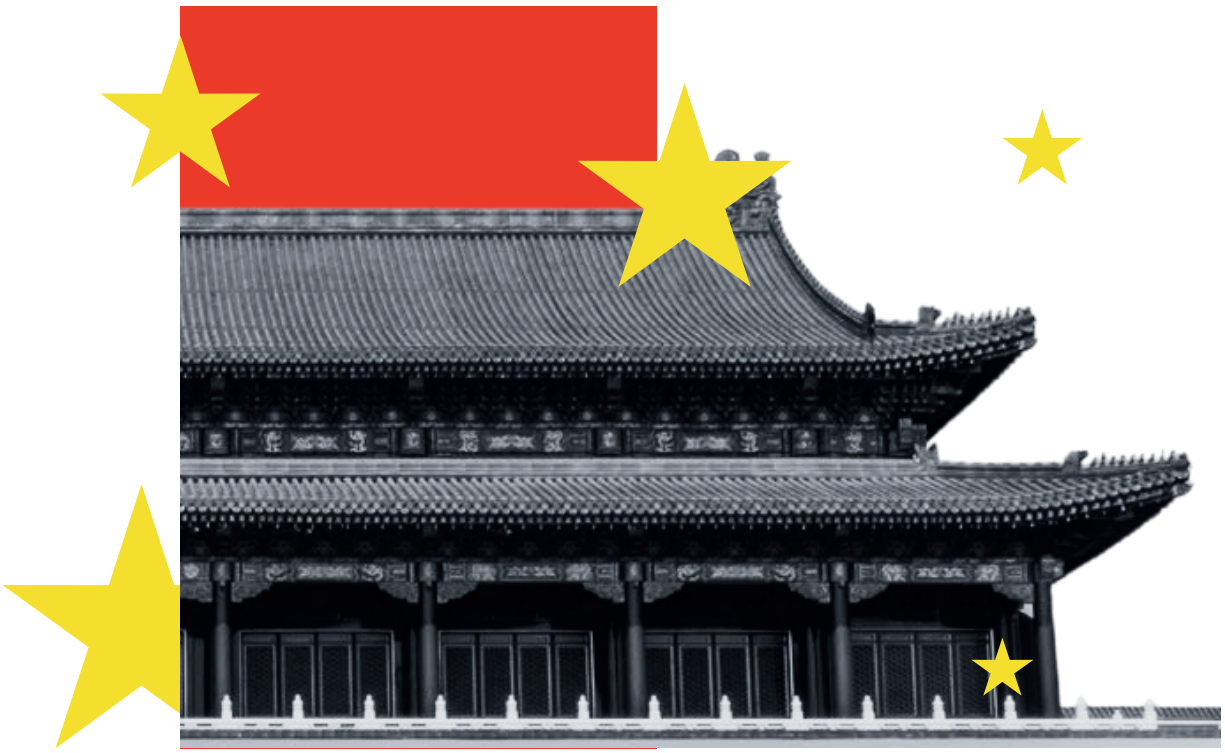
Role of Foreign Media

China

China's state-run media Xinhua News Agency effectively became a mouthpiece for Pakistan's narrative during *Operation Sindoor*. It reported that India had targeted civilian settlements in six areas within Pakistan and amplified claims made by the Pakistan Air Force (PAF) that it had shot down five Indian fighter jets, including three Rafales, one MiG-29, one Sukhoi, as well as a combat drone.[101] The same news has been amplified by the Global Times, echoing Pakistan's narratives.[102] The Global Times further posted a fabricated video claiming the downing of a third Indian jet, which gained traction on X with over 3.8 million views and thousands of engagements.[103] Following this, the Embassy of India in Beijing issued a scathing response. It accused the outlet of actively spreading disinformation as part of a broader propaganda effort around Operation Sindoor, and demanded that Global Times should "verify facts and cross-examine sources".[104] This post has also garnered over 3.4 million views with thousands of engagements.

Understanding this media connection reflects how these activities are closely intertwined with the strategic and multifaceted China-Pakistan bilateral relationship. China and Pakistan have repeatedly reaffirmed their status as "iron-clad friends"[105] & "all-weather strategic cooperative partners,"[106] with cooperation

extending across high-level political, defence, economic, media and cultural domains. Ironically, in July 2025, Pakistan and China agreed to strengthen ties between their state broadcasters, launch joint broadcasting projects, institutional collaboration, and a unified narrative to combat fake news and disinformation.[107] Thus, this is how Pakistan is actively participating and benefiting from a coordinated media architecture that aligns with China's strategic messaging in the present and will be in the future.



Turkey

Likewise, Turkey's state-run media TRT World and Anadolu Ajansi (AA) exhibited the same behaviour. In recent years, Turkish media outlets particularly TRT World have become increasingly instrumental in amplifying pro-Pakistan narratives, especially in the context of Pakistan's conflict with India. This alignment is evident in the outlet's repeated and uncritical dissemination of claims originating from Pakistani state media, often in the absence of independently verifiable evidence. India's cyber-intelligence has flagged TRT as an extension of Turkish foreign policy under President Erdoğan, working in coordination with Pakistan's ISPR. Moreover, TRT has frequently promoted Chinese and Pakistani positions on sensitive issues such as Ladakh, Arunachal Pradesh, and India's border disputes as well as portrayed India as anti-Muslim, highlighting contentious domestic issues like the Citizenship Amendment Act (CAA), the National Register of Citizens (NRC), and the Hijab controversy.[108]

In its recent coverage of the India-Pakistan conflict, TRT World deliberately referred to "*Operation Sindoor"* as the "so-called"[109] operation, openly challenging the legitimacy of India's official narrative, while simultaneously glorifying Pakistan's response, "Operation Bunyan-un-Marsoos".[110] This language clearly signals diplomatic alignment with Pakistan's stance by undermining India's motives and distorting the framing of the conflict. Following this, TRT further propagated Pakistan's narrative of shooting down five Indian warplanes and drones, both on their website[111] and X.[112]

Another Turkish media outlet, Anadolu Ajansi (AA), disseminated Pakistan's military fabricated sources and Pakistan Television Corporation (PTV) report on the destruction of a missile storage site in India's Beas region and the S-400 system in Adampur.[113] This exemplifies biased reporting and the uncritical dissemination of one-sided narratives, as the article unreservedly echoed Pakistan's claims while ignoring India's perspective.

Given mounting evidence, a pressing question emerges: Are Turkey and Pakistan working in collusion to malign India's image? The answer appears positive. Reports suggest that Turkey and Pakistan have established a coordinated propaganda network as early as 2014. Evidence indicates that prominent Turkish state media outlets have shifted their recruitment strategy, moving away from Western journalists to hiring Pakistani and Indian Kashmiri journalists in significant numbers. Sources reveal that recruitment at TRT World has accelerated to such an extent that nearly one-fourth of its top and mid-level positions are reportedly occupied by journalists from the Indian subcontinent. Further investigations point to close coordination between Türkiye's National Intelligence Organisation (MIT) and Pakistan's Inter-Services Intelligence (ISI) in developing an expanded propaganda and influence network, with TRT World and the Anadolu Agency (AA) serving as its main operational centres. Moreover, the plan reportedly involved collaboration with Pakistan's Inter-Services Public Relations (ISPR) through a joint initiative, designating TRT World as the nodal agency to execute this confidential program.[114]With such a strong nexus and systematic collaboration, it becomes evident that Pakistan and Turkey have been actively cooperating to shape anti-India narratives and influence global public opinion against New Delhi.

In addition to the convergence of their intelligence operations, it is essential to examine how Turkey and Pakistan have sustained a strategic and multi-dimensional partnership over the years, encompassing defence, trade, culture, and diplomacy. The two countries have actively collaborated on military projects, maintained consistent alignment on key regional issues such as Kashmir, and fostered strong people-to-people connections. Consequently, this close political and intelligence relationship helps explain the alignment of Turkish state media with Pakistan's narratives.

Azerbaijan

On the other hand, Azerbaijan openly aligned with Pakistan's position following the Pahalgam attack, issuing statements that condemned India and accused it of undermining regional stability[115] and blatant aggression. Demonstrating unwavering and strong solidarity[117] with Pakistan, the Azerbaijani Ministry of Foreign Affairs and several MP's repeatedly endorsed Islamabad's stance and echoed its concerns on regional security. Reinforcing this position, Azerbaijan's state-run news agency, AZERTAC, provided extensive coverage of the India-Pakistan confrontation[118] and amplified narratives critical of India. The article echoed Pakistan's narrative by alleging the destruction of 26 Indian military targets in "Indian Illegally Occupied Jammu and Kashmir" and "Mainland India." It amplified false claims about the BrahMos storage facility and S-400 system at Adampur being hit by the Pakistan Air Force, citing the ISPR's press conference to reinforce this narrative. Under the banner of "Operation Bunyan-un-Marsoos," it further glorified unverified claims of Pakistani armed drones flying over major Indian cities, including the Capital, New Delhi.[119]

Furthermore, these state-run media also disseminated Pakistan's military propaganda, falsely claiming that the Pakistan Armed Forces had destroyed the Brigade Headquarters at "K G Top" and a supply depot in Uri, and that a cyberattack had caused 70% of India's electricity grid to be dysfunctional.[120] These assertions have no basis in verified reports and represent a deliberate attempt to amplify false narratives targeting India's defense and critical infrastructure.

Since its establishment, Azerbaijan and Pakistan have maintained a close, strategic partnership rooted in mutual support on regional issues. Since establishing diplomatic relations in 1992, they have cooperated in defense, trade, and culture, including joint military training, economic collaboration, and educational exchanges. Both countries consistently endorse each other's positions internationally, which underpins Azerbaijan's amplification of Pakistan's narratives during *Operation Sindoor*.[121]

Therefore, these dynamics explain how Pakistan has utilised its bilateral relationships and allied media networks to shape international perception, amplify strategic narratives, and delegitimise India's actions. The convergence of diplomatic backing, state-aligned media, and social media amplification demonstrates a sophisticated model of digital and geopolitical influence, where allied states collaborate to project power, control narratives, and advance shared strategic interests without direct engagement in the conflict.

Role of X Influencers

Due to technological constraints arising from the banning of several X foreign influencers who were disseminating pro-Pakistan narratives, this report presents a limited dataset and analysis. Nevertheless, it aims to provide an insightful examination of the role these foreign influencers played in shaping information flows and public perception during the Pahalgam attack and *Operation Sindoor*.

In today's digital era, with the rapid proliferation of social media platforms, a new agency emerged to whom we can refer as a "political influencer" or "influence actors" which has profoundly and dramatically reshaped public opinion, decision-making processes and the broader dynamics of political discourse. While some of these actors operate genuinely and independently, others engage in impersonation. The most concerning aspect is that most of these actors are strategically planted by FIMI actors to serve as instruments of targeted influence and information disruption.

These influencers gain followers through a combination of emotional engagement, narrative manipulation, and algorithmic exploitation. By leveraging trending socio-political issues, sensational content, and coordinated amplification networks, they build perceived credibility and community trust. Over time, this enables them to subtly influence public opinion, distort factual discourse, and, in some cases, shape policy sentiment in alignment with the objectives of foreign or hostile information operations.

Immediately after the Pahalgam attack and the subsequent *Operation Sindoor*, these dynamics were prominently observable across multiple digital platforms, particularly on X, where coordinated narratives, influencer amplification, and disinformation campaigns were most active. A coordinated network of political influencers, including both verified and inauthentic accounts, sought to amplify divisive narratives and undermine official communication channels. As observed, pro-Pakistan digital assets circulated pro-Pakistan narratives aimed at discrediting *Operation Sindoor* and eroding public trust in institutional responses. The timing, consistency, and linguistic alignment of their posts indicate a structured influence campaign designed to exploit the information void in the immediate aftermath of the attack and to shape global perception against India's counter-terror measures.

To cite a few examples, one account, operating under the username @thinking_panda, a Chinese account, posted content promoting a pro-Pakistan narrative. The post claimed that China supports the Pakistani government rather than terrorist organisations, asserting that Beijing opposes terrorism but not the Indian government. It further argued that there is no evidence of the Pakistani government carrying out attacks on Indian tourists and suggested that China opposes any military action by the Modi administration against Pakistan for political gain, while remaining obligated to support its Pakistani allies.[122]

The same account propagated another narrative emphasising Pakistan's supposed technological and tactical superiority over India. The post claimed that China's exported J-10CE fighter jets, priced at approximately $70 million each, had outperformed India's Rafale aircraft, which were allegedly valued at $285 million a piece. It further asserted that India had recently placed a $7.5 billion order for 26 additional Rafales on April 28, implying wasteful expenditure and poor strategic judgment. The post concluded that, despite possessing only 20 J-10CEs, Pakistan had already achieved air superiority dominance. This content sought to reinforce perceptions of Pakistan's military advantage through Chinese technology while simultaneously portraying India's defence procurement as economically imprudent and operationally ineffective. Such narratives align with broader FIMI objectives aimed at undermining India's defence credibility and bolstering China's image as a superior defence partner in the region.

Furthermore, this account also posted content directed towards Indonesian users. The message sought to discredit Indonesia's defense procurement from France while simultaneously reinforcing the false claim of Pakistan's air superiority using Chinese J-10C aircraft. By employing humour and an informal tone, the account attempted to humanise propaganda, making it more shareable and persuasive among non-Indian audiences. This reflects a strategic shift within FIMI-linked influence network,s expanding target outreach to neutral or third-party states to boost the perceived legitimacy of Chinese defense technology and erode confidence in Western defense partnerships.[123]

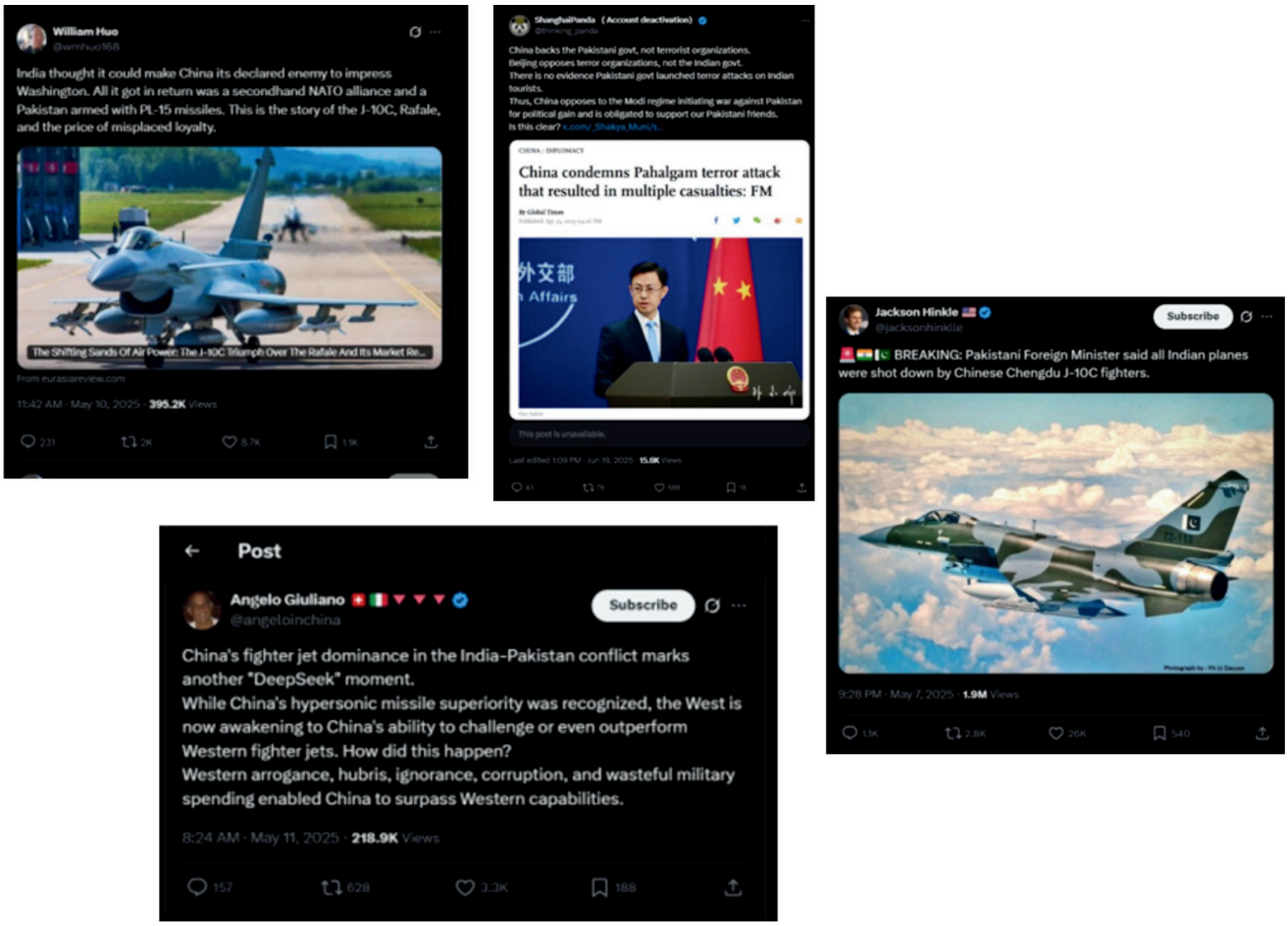


Figure 6
Source: X

Another Chinese account @wmhuo168, circulated a narrative aimed at discrediting India's strategic alignment with the United States. The post asserted that India had sought to make China its declared enemy to impress Washington, but in doing so had gained only a "secondhand NATO alliance" while enabling Pakistan to acquire PL-15 missile systems. Framed as the story of the J-10C, Rafale, and the price of misplaced loyalty, the message sought to undermine India's defence partnerships, questioning the credibility of Western support, and elevating China's position as a more capable and self-reliant power in the region.[124] The post exemplifies how coordinated disinformation content was tailored to exploit geopolitical rivalries and weaken confidence in India's foreign policy decisions. The same account further commented on Indian jets as scrambled, while portraying Pakistan as acting decisively, highlighting China's strategic influence. The post suggested that although India responded militarily, the true victor was China, which "dominated the battlefield" through covert means without engaging directly. This narrative emphasizes China's strategic superiority and promotes the perception of Beijing as a behind-the-scenes power broker, subtly undermining India's response while bolstering China-Pakistan alignment.[125]

Another China-linked account @angeloinchina, promoted a narrative portraying the conflict as proof of China's military and technological superiority. The post claimed that "China's fighter jet dominance in the India-Pakistan conflict marks another 'DeepSeek' moment," arguing that the West was only now realising China's ability to "challenge or even outperform Western fighter jets." It attributed this shift to "Western arrogance and wasteful military spending," aiming to glorify China's defence capabilities while discrediting Western systems and India's strategic alignment with them.[126]

One of the most prominent foreign influencers involved in narrative amplification during the Pahalgam attack and Operation Sindoor was @jacksonhinklle, an American-based digital political influencer or commentator known for promoting pro-China, pro-Russia, and pro-Pakistan narratives. This account amplified the narrative, echoing claims made by the Pakistani Foreign Minister that all Indian aircraft had been shot down by Chinese-manufactured Chengdu J-10C fighter jets.[127] This post reinforced pro-Pakistan and pro-China messaging by portraying Chinese defence technology as decisively superior and instrumental in the conflict. By leveraging a well-known influencer persona, the account lent perceived legitimacy to the disinformation, thereby extending its reach and impact across both domestic and international audiences. This reflects a deliberate tactic within broader FIMI-linked influence operations utilising high-visibility digital figures to amplify state-aligned propaganda under the guise of independent commentary.

Analysing these accounts reveals a coordinated pattern of digital influence operations during the Pahalgam attack and Operation Sindoor. These actors amplified pro-Pakistan and pro-China narratives, exaggerated Pakistan's military effectiveness, highlighted Chinese technological superiority, and undermined India's defence credibility. By combining emotive messaging, selective framing, and high-visibility influencers, they extended the impact to both domestic and international audiences. In addition to this, these accounts also extended the narratives to third-party audiences like Indonesia to broaden influence.

PRO PAK
PRO CHINA

Pakistan's FIMI actors and its role during Operation Sindoor

Pakistan's FIMI ecosystem is a multi-layered apparatus that combines state institutions, intelligence agencies, diplomatic channels, media organisations, and transnational media and X influencer networks to advance its strategic objectives, particularly against India. Below is the brief explanation of the Pakistan FIMI actors.

1. Inter-Services Intelligence (ISI)

Pakistan's ISI occupies a central position in disinformation warfare against India, operating closely with the Inter-Services Public Relations (ISPR). Together, they have built an extensive propaganda ecosystem designed to manipulate the perception of the international community and undermine India's image.

1. Narrative shaping and strategic messaging

Through coordinated campaigns with the ISPR, the ISI pushes narratives portraying Pakistan as a victim of Indian aggression. Indian intelligence reports[128] highlighted the uniform timing, tone, and amplification of such content often released during key conflict moments as clear evidence of a state-sponsored operation. The disinformation is spread across major platforms, including X (formerly Twitter), Facebook, Instagram, and YouTube, frequently amplified by Pakistani media outlets and social media influencers.

2. Digital & Social Media Operations

The ISI reportedly manages networks of fake social media accounts to propagate anti-India narratives. Indian cyber agencies[129] have exposed thousands of such accounts linked to Pakistan's military and intelligence apparatus, posting synchronised disinformation within minutes to create viral momentum. Over 4,300 accounts have been suspended during investigations. According to some sources, in the past, the ISI has created 5,000[130] fake Twitter and Facebook accounts, many of which use stolen images of global and Baloch leaders to cultivate hatred against India. This orchestrated digital offensive demonstrates a centrally directed, state-backed information warfare campaign against India. Therefore, the ISI's roadmap and ISPR's role extend far beyond propaganda; it represents a calculated and enduring threat to India's National Security and internal stability.

3. Strategic Infiltration and expansion into India's digital democratic space
Reports suggest that the ISI has developed a network of dormant assets inside India, which are positioned to inject tailored narratives or leak information during moments of crisis. This marks a shift from episodic propaganda to continuous, embedded influence operations. By infiltrating India's information space, the ISI ensures its disinformation appears organic and difficult to trace. These actors amplify anti-India content, exploit social divisions, and reinforce ISPR-driven narratives to weaken public trust and undermine India's credibility at home and abroad.[131] It is imperative to draw attention that Pakistan's ISI has been actively recruiting Indian social media influencers or honey-trapping professionals to advance Islamabad's objectives. Notable cases include social media influencer Jyoti Malhotra and mechanical engineer Ravindra Verma, who were allegedly manipulated to further Pakistan's strategic interests.[132] Therefore, the ISI's roadmap and ISPR's role extend far beyond propaganda; they represent a calculated and enduring threat to India's National Security and internal stability.

2. The Inter-Services Public Relations (ISPR)

The Inter-Services Public Relations (ISPR), the media wing of the Pakistan Army, has moved beyond its traditional role into becoming an important actor of Pakistan's state-sponsored disinformation apparatus, working closely with the ISI and foreign allies. During *Operation Sindoor*, the ISPR systematically exploited social media platforms to conduct psychological operations, deploying a range of tactics to disseminate misinformation and manipulated narratives, including fabricated claims of downed Indian jets, doctored images, recycled war footage, counterfeit public advisories, and wrongly pinning India for staging a false flag operation. One of the more outrageous claims is that Indian forces fired missiles at Amritsar, a major Indian city of profound religious significance to Sikhs. This allegation was made by Lieutenant General Ahmed Sharif Chaudhry, Director General of Pakistan's ISPR. The main aim was to spread fear, divide and demoralise Indian citizens, and undermine India's international credibility, which reflects on the classical tactics of Pakistan's state-led disinformation strategy.

As observed, one of the main objectives of ISPR is to project Pakistan's and China's military superiority to its domestic and international audience while also simultaneously downplaying military operational capabilities and weakening India's public confidence in defence institutions. These ISPR-driven activities are further amplified by Chinese-linked social media networks and Turkish state outlets such as TRT World and Anadolu Agency (AA), who mimicked Pakistan's narrative and pushed its propaganda, significantly extending its reach and perceived legitimacy of Pakistan's disinformation campaigns. This strategy allows Pakistan's ISPR to hit two targets at one time, to undermine India while cultivating international partnerships with actors sympathetic to, or strategically aligned with, Pakistan.

3. Ministry of Foreign Affairs (MFA)

The Ministry of Foreign Affairs (MFA) of Pakistan equally played an active and central role in Islamabad's FIMI disinformation strategy by not just issuing denials but producing detailed alternate narratives (Statements, Press briefings) to influence the global opinion. Through diplomatic channels and public statements, the MFA provides legitimacy to the state-run propaganda, framing Pakistan's claims as evidence-based and countering India's messaging in international arenas. For India, this means countering Pakistan's disinformation not only at the strategic or military level but also diplomatically by challenging these narratives in international institutions, releasing counter-evidence, and engaging in public diplomacy.

For instance, on 8th May, the MFA issued a statement rejecting Indian claims about Pakistan's cross-border strikes in Pathankot, Jaisalmer and Srinagar and accused India of running a reckless propaganda campaign. The statement frames India as a regional aggressor and while simultaneously rallying international sympathy for Pakistan.[138] Similarly, on 9th May, Pakistan submitted the same statement to the United Nations Security Council with a request to circulate the message under the item entitled "The India-Pakistan Question".[139] Again, on 23rd May, MFA issued a press briefing seeking to deflect and dismiss India's concern on terrorism, by resorting to its habitual tactic of referring to Jammu and Kashmir as *"Indian Illegally Occupied Jammu and Kashmir (IIOJK)"*, a calculated move intended to provoke international outrage and sustain the anti-India narrative in global discourse.[140]

These repeated measures and statements illustrated how Pakistan's MFA uses its diplomatic voice to shape and control global narratives, often aligning with ISPR/ISI messaging.

4. State-backed and aligned Media outlets

Pakistan's state-controlled and aligned media have emerged as a central actor in Pakistan's disinformation architecture, functioning as deliberate amplifiers of state narratives crafted by the ISPR. Through coordinated reporting, selective framing, and the dissemination of misleading or fabricated content, these outlets inject strategic messaging into both domestic and international information spaces. Their coverage consistently reinforces Islamabad's preferred geopolitical narratives, portraying Pakistan as a responsible regional actor and India as an aggressor while concealing or distorting facts that challenge official positions.

This media ecosystem, comprising television networks, state-run newspapers, and government-linked digital platforms, operates in tandem with social media influence networks and diplomatic messaging from the Ministry of Foreign Affairs. Together, they create a self-reinforcing echo chamber that legitimises Pakistan's strategic posture, manipulates public perception, and undermines India's image in global discourse. By blurring the boundaries between journalism and psychological operations, these outlets have effectively transformed Pakistan's information sphere into an instrument of hybrid warfare.

Evidently, prominent outlets such as PTV, Radio Pakistan, The Express Tribune, Samaa TV, and English-language dailies such as The Nation and Dawn frequently structure their coverage to mirror Islamabad's strategic messaging, amplifying state-approved narratives on national security, legitimising Pakistan's foreign policy posture, and reinforcing anti-India sentiment within domestic and international audiences.

For instance, immediately after Operation Sindoor, Pakistan's state-controlled media launched a coordinated campaign labelling it as a false-flag operation, accusing India of staging the attacks and waging a proxy war to destabilise Pakistan. The messaging was designed to shift blame entirely onto India, confuse both domestic and international audiences, and shield Islamabad from accountability.[141] On the other hand, The Dawn portrayed Pakistan as the world's frontline state against terrorism, emphasising the heavy human and economic toll it has endured. At the same time, it accused India of deliberately creating instability along Pakistan's eastern borders to distract from Pakistan's counter-terrorism operations. These narratives clearly shifted the blame onto India, deflecting attention from Pakistan's own role in regional tensions while presenting Islamabad as the responsible, victimised actor.[142] These examples illustrate how Pakistan systematically weaponises its media, military, and diplomatic machinery to spread disinformation, deflect accountability, manipulate public perception, and undermine India's credibility both domestically and internationally.

5. Think Tanks

Think tanks in Pakistan, including the Institute of Strategic Studies Islamabad (ISSI), Pakistan Strategic Forum (PSF), and Centre for International Strategic Studies (CISS), operate as intellectual and semi-official extensions of the state's FIMI apparatus. These institutions produce research, policy briefs, and media content that consistently align either subtly or overtly with Pakistan's strategic objectives, effectively providing scholarly legitimacy and analytical cover to the state's information, influence, and disinformation campaigns.

For instance, on 29th May, ISSI issued a policy brief which framed the Pahalgam attack as a false-flag operation orchestrated by India to divert attention from domestic unrest and upcoming elections. The brief emphasised the timing of the attack, coinciding with high-profile foreign visits and domestic protests as a strategic opportunity for New Delhi to consolidate nationalist sentiment.[143]

On the other hand, CISS aggressively portrayed the Pakistan Air Force (PAF) as far superior to the Indian Air Force (IAF), while questioning India's strategic and operational capabilities. It claimed that the PAF had delivered a befitting response to India by shooting down five Indian aircraft, including three French-made Rafales, one MiG-29, one Su-30 fighter, and a Heron surveillance drone following Operation Bunyanum Marsoos. It is a clear attempt to inflate Pakistan's military image and mislead both domestic and international audiences. By selectively citing historical encounters, it claimed that the PAF has repeatedly outperformed the IAF, framing Pakistan's airpower as both dominant and deterrent-ready, while reinforcing anti-India sentiment and projecting military credibility for Islamabad's audience.[144] In addition to that, the same misinformation of downing the Rafale jets has been amplified by the PSF in X.[145]

This shows Pakistan systematically weaponises its think tanks to provide intellectual cover for propaganda, amplify anti-India narratives, and legitimise Islamabad's strategic objectives in both regional and global arenas.

6. Foreign Media and X influencers

Another significant component of Pakistan's FIMI ecosystem is the involvement of foreign media outlets and international influencers who amplify Pakistan's strategic narratives. This dynamic became particularly visible during Operation Sindoor, when several foreign-based social media personalities and alternative media platforms echoed the same narratives that originated from Pakistani state-linked or pro-establishment sources. As discussed above, the Chinese Media state outlets such as Global times, and Xinhua Times.

7. Fake social media accounts and digital troll farms

During Operation Sindoor, Pakistan's FIMI deployed massive troll farms, cyber volunteers, and paid influencers to run coordinated campaigns against India, amplifying hashtags, memes, deepfakes, and old and recycled videos timed to the strikes and related diplomatic events to maximise impact on social media. In addition, the use of generative AI and bot networks has significantly amplified both the scale and speed of the disinformation campaigns across the social media platforms (Facebook, X, Instagram).

The main idea was to flood the online global information ecosystem and suppress the truth. Many fake accounts were spotted praising Pakistan, which amplified the misinformation contents in the X. For instance, when a post on downing Rafale jets near Bahawalpur gained virality, it was amplified by both the genuine accounts as well as the bot accounts. The image was later debunked by the PIB FCU, which confirmed the MiG-21 crash in Moga, Punjab, in 2021.[146] Significantly, Indian journalist and fact-checker Mohammed Zubair also drew a list of accounts originating from Pakistan and which were mimicking as Indian armed personnel in the X.[147] According to reports by the CyberPeace Foundation and DisInfoLab India, Pakistan created a vast network comprising 1,825 YouTube channels, 3,200 X accounts, and 192 government-linked handles to inundate Indian cyberspace with anti-national content.[148]

These activities highlight a deliberate, coordinated strategy by the ISI to deploy thousands of accounts and digital assets, combining AI, bots, and human operatives, to wage a multi-layered disinformation war against India during Operation Sindoor.

India's Response

India has adopted a pro-active and multi-pronged strategy to counter a disinformation campaign from Pakistan. This approach is grounded in a structured framework encompassing three core dimensions: Institutional-Technical and Diplomatic.

Institutional and Technical Dimension:

The Government of India acted swiftly with the realisation of FIMI Disinformation and Misinformation operations emanating from Pakistan, and instrumentalised the available statutory and institutional tools. The Press Information Bureau (PIB) Report[149]dated 30th July 2025, emphasised strongly on countering disinformation and misinformation originating from foreign countries and the actions the Government of India has taken.

To counter disinformation and misinformation, India took a concrete step: *Firstly,* the Government of India provided authentic information periodically in the public domain through official communication channels to keep the media and citizens updated and informed about the developments, as well as provided the relevant details of operations of the defence force with audio-video visual and satellite imagery. While Pakistan's official channels, including defence and diplomatic platforms, were found disseminating misleading and false information, India chose to uphold transparency and truth in its communications, factual rebuttals, and robust digital vigilance. *Secondly,* India established a centralised Control Room for an Inter-ministerial coordination which comprised representatives from the Indian Army, Navy, and Air Force, along with officers from various Government media units, and Press Information Bureau (PIB). The Control Room functioned 24x7, facilitating information dissemination to all media stakeholders as well as monitoring and identifying fake news and misinformation.

According to this report, the Fact Checking Unit (FCU) of the Press Information Bureau (PIB) worked around the clock to counter Pakistan's propaganda. The unit actively monitored, detected, and identified disinformation and misinformation campaigns in real time, targeting India and the Indian Armed Forces. The identified instances of disinformation and fake news were promptly shared with the relevant intermediaries, including major social media platforms, digital news aggregators, and law enforcement agencies, for appropriate remedial measures. These actions included the removal of misleading content, suspension of accounts responsible for dissemination, and initiation of legal proceedings where applicable.

The report revealed that the Ministry blocked over 1,400 URLs on digital media platforms during Operation Sindoor. These URLs contained false and misleading information, anti-India narratives, inciteful content against the Indian Armed Forces, and communally sensitive material primarily originating from Pakistan-based social media accounts. For instance, the Press Information Bureau (PIB) made an early intervention when a fabricated social media post falsely claiming that the Pakistani Army had destroyed an Indian military post began gaining significant traction on platform X (formerly Twitter).[150] In addition to this, as mentioned above, India has banned 4300 social media accounts. Another prominent example, a widely circulated video of a drone attack in Jalandhar, Punjab, was proven false and misleading. The PIB Fact Checking Unit quickly debunked the footage, confirming it actually showed a farm fire unrelated to any military operations.[151] This prompt response by PIB exemplifies how disinformation and misinformation campaigns are strategically countered through timely fact-checking and official communication, thereby preventing the spread of false narratives and maintaining public trust.

The primary legal basis for the above action was Section 69A of the Information Technology Act, 2000, which the government effectively instrumentalised to deal with the cross-border misinformation and disinformation campaigns. Under this provision, the Government issued orders to block websites, social media accounts, and specific posts in the interest of India's sovereignty and integrity, national defence, state security, and public order. On the other hand, the Ministry of Information and Broadcasting also circulated a circular to all National Media channels to refrain from broadcasting live coverage of defence operations and the movement of security forces, in the interest of national security.

Diplomatic Dimension:

The subsequent measure undertaken by the Government of India demonstrated a commendable degree of pragmatism. Post-Pahalgam attack and Operation Sindoor strategically advanced its diplomatic outreach by dispatching seven-party delegations,[152] comprising 51 political leaders from various parties and eight former diplomats, to 33 countries with multifaceted objectives. The unified objective of this initiative was to send a strong message to the global community that India has a zero-tolerance policy against terrorism,[153] underscored Pakistan's involvement in cross-border terrorism, intensified international pressure on Islamabad, and simultaneously garnered broader support for India's position on the global stage.[154]This effort also played a crucial role in countering Pakistan's narrative in international forums and information or narratives originating from foreign lands.

The All-Party delegation, consisting of several MPs divided into seven groups from various political parties, not only reflects India's national consensus and firm stance against terrorism but also powerfully projects a unified image of a pluralistic India, particularly significant at a time when the Modi government faces international criticism over alleged democratic backsliding and rising majoritarianism. Therefore, the message conveyed by this delegation is multifaceted in its purpose, aimed not only at foreign governments but also for legislators, international media, and the wider public, particularly in countries where New Delhi believes the expected solidarity and support have been lacking.[155]

Considering Pakistan's role in strategically maligning India's image through official diplomatic channels and disinformation campaigns, most notably its politicised misuse of its non-permanent member of the UN Security Council (2025-2026), during which it succeeded in amending the original UNSC statement to omit. The Resistance Front's (TRF)[156] role in the Pahalgam attack with the backing of other powers, and its continued attempts to manipulate the Organisation of Islamic Cooperation (OIC) into issuing critical and biased statements against India, the All-Party delegation's visit was both necessary and timely to counter this narrative and expose Pakistan.

The seven-party delegation has demonstrated notable diplomatic success in achieving its objectives. A notable example was Colombia's retraction of its earlier statement, which had expressed condolences for the loss of lives in Pakistan following the Indian strikes during Operation Sindoor. This reversal came after a meeting between the All-party delegation led by Congress MP Shashi Tharoor and Colombia's Vice Minister of Foreign Affairs, Rosa Yolanda Villavicencio. Furthermore, Colombia reaffirmed its official position and reiterated its support for India.[157] On the other hand, India's All-Party delegation led by Lok Sabha MP Ravi Shankar Prasad to Denmark faced little disruption when Pakistani protesters tried to interrupt the delegation; however, it remained unaffected. In addition to that, the Pakistan embassy tried to hijack the relationship and established the notion that Denmark is Islamabad's sympathiser, as well as attempted to push Pakistan's narrative in the local media.[157] However, India's delegation received strong support from Denmark on India's position,[159] while Freddy Svane, the former Danish Ambassador to India, also welcomed India's diplomatic offensive to expose Pakistan globally.[160]

To sum up, India's response to Pakistan's disinformation campaign has been swift and strategic. Through legal tools, real-time fact-checking, and coordinated communication, India countered false narratives at home. Globally, the All-Party delegation successfully exposed Pakistan's propaganda and secured international support, reaffirming India's credibility and its firm stance against terrorism.

Policy Recommendations

To effectively counter FIMI operations and campaigns, India must shift from a fragmented, reactive posture to a proactive, institutionalised, integrated and multi-domain national strategy. This section provides a set of recommendations aimed at developing a conceptual framework, robust FIMI resilience architecture that aligns strategic communications, legal reform, public awareness, and international cooperation.

1. Develop a tailored FIMI concept and comprehensive framework for India:

Firstly, India must establish an official definition of disinformation and misinformation, and conceptualise FIMI within this framework. This is essential for developing a comprehensive understanding of the issue and formulating effective counter-FIMI measures. This should go beyond generic cyber or disinformation policies and be rooted in India's unique geopolitical and socio-cultural context. It must be emphasised that FIMI is not only a threat to India's National Security and Foreign Policy but also endangers India's cultural and religious diversity. Like the US, India's approach to FIMI must also extend to India's existing and potential partners, framing FIMI as a shared transnational threat. This will ensure that it becomes an integral part of India's broader foreign and security policy calculus, fostering joint preparedness and coordinated responses with like-minded partners.

Secondly, given the scale, persistence, and strategic alignment of Pakistani FIMI operations with other countries, India should officially treat Pakistan as the primary FIMI threat actor. This strategic clarity is vital to channel diplomatic, intelligence, and technological resources proportionately. While prioritising Pakistan as the foremost source of FIMI threat actors, India must also remain vigilant in identifying other emerging state and non-state actors that could exploit similar tactics in the future.

2. Establish a National Strategic Communications Centre

India should establish a National Strategic Communications Centre to systematically counter foreign disinformation and propaganda. This dedicated mechanism will enable India to identify, map, strategise, expose, and counter FIMI efforts that are aimed at undermining or influencing the policies, security, or stability of India, and its partners. One of the best models India can draw inspiration from is Taiwan, which has developed a national-level response and a decentralised framework to counter FIMI.

3. Diversify the functions of the PIB's Fact Checking Unit (FCU)

To improve operational efficiency, the PIB's Fact Check Unit should be diversified into domain-based teams, each specialising in distinct sectors of disinformation and misinformation. As mentioned above, Taiwan's counter FIMI mechanism follows the specific-domain based target to tackle FIMI disinformation. Nevertheless, India can also draw lessons and best practices from other international models, such as the EU's EUvsDisinfo flagship project, the U.K.'s Counter Disinformation Unit and Rapid Response Unit, and Ukraine's Centre for Countering Disinformation. By adapting the best practices from these initiatives, India can develop approaches tailored to its unique geopolitical context and socio-cultural landscape.

4. Advance Research-Led Institutional Capacity to Counter FIMI

As discussed above in prioritising research it is pertinent to strengthen expert-driven research, technological innovation, and program development within key national institutions such as the National Critical Information Infrastructure Protection Centre (NCIIPC), the Indian Cyber Crime Coordination Centre (I4C), and emerging Cognitive Warfare and Information Security research hubs, to enhance India's institutional capacity and operational effectiveness in countering FIMI.

5. Integrate FIMI Disinformation mechanism into National Education and Media Literacy

India should integrate FIMI awareness into national education policies and media literacy to build long term societal resilience. This means teaching students how to critically assess online content, verify sources, detect manipulative narratives, and understand the algorithms that shape their information environment. Best practices can be drawn from Finland, Lithuania and Estonia who have already integrated digital literacy on disinformation and propaganda in their education system. On the other hand, a nationwide media literacy campaign must run in multiple regional languages targeting broader segments of society, helping citizens identify fake news, deepfakes, and coordinated influence narratives. This will allow India to develop "Cognitive deterrence" not only against FIMI disinformation campaigns but also to the other online led campaigns.

6. Enact a dedicated FIMI legislation

India should develop a robust legal response to combat FIMI. This requires modernising existing laws and enacting targeted legislation to explicitly cover orchestrated foreign disinformation campaigns, AI-generated deepfakes, and covert influence operations that threaten national security or democratic processes. It can draw lessons from Taiwan's Anti-Infiltration Act and the EU's Digital Services Act.

7. International Cooperation

Given the transnational nature of the FIMI threat, India must seek to establish international cooperation with like-minded democratic countries to share intelligence on disinformation networks, develop common standards for digital transparency, and coordinate public exposure of hostile influence campaigns. India should also deepen its engagement with the existing multilateral frameworks, such as with the EU, QUAD, ASEAN and other regional and international organisations to align strategies, build collective resilience, and shape international norms against foreign information manipulation. By doing so, India can not only strengthen its own information security but also contribute to safeguarding the broader democratic digital ecosystem.

Conclusion

To conclude, this study illustrates how Pakistan's information warfare against India evolved from traditional propaganda into a calculated, technology-driven campaign of manipulation. What distinguishes the Pahalgam and *Operation Sindoor* episode from earlier conflicts is the sophistication and speed of Pakistan's digital warfare. Its multi-layered ecosystem, comprising the Inter-Services Intelligence (ISI), Inter-Services Public Relations (ISPR), Ministry of Foreign Affairs (MFA), state-controlled and aligned media, and affiliated think tanks, worked in synchronised coordination with foreign media networks and transnational influencers. Together, these actors forged an ecosystem capable of producing and disseminating falsehoods at a scale that transcends borders and penetrates both domestic and global information spaces.

Pakistan's FIMI disinformation campaign pursued clear and coordinated objectives: to delegitimise India's counterterrorism operations, attack India's political and military leadership, fabricate international sympathy for itself, and fracture India's domestic unity. Through orchestrated amplification of doctored visuals, falsified reports, and conspiracy-laden "false flag" narratives, Islamabad sought to invert reality, casting India as the aggressor and Pakistan as the aggrieved victim. Within hours of *Operation Sindoor*, Pakistani official channels and media outlets, reinforced by Chinese, Turkish, and Azerbaijani media, saturated global digital networks with claims of Indian military failure, civilian casualties, and violations of international law. This seamless collaboration between state organs and proxy amplifiers demonstrates how Pakistan has transformed disinformation into a strategic instrument of statecraft, an inexpensive yet potent weapon of asymmetric warfare.

The FIMI framework applied in this study confirms that Pakistan weaponised all five dimensions of the EU's 5D model-Dismiss, Distort, Distract, Dismay, and Divide-through a sophisticated web of Tactics, Techniques, and Procedures (TTPs). It dismissed the Pahalgam terror attack and *Operation Sindoor* by branding them as *false-flag operations* orchestrated by India to malign Pakistan. It manipulated information through disinformation, misinformation, cheapfakes, deepfakes, forged documents, and AI-generated visuals, seeking to divert international attention by resurrecting divisive narratives surrounding Kashmir, human rights, and the alleged repression of minorities. Concurrently, it dismayed global audiences with nuclear threats, cyber panic, and fabricated military claims, while seeking to divide Indian society along communal and political lines.

Pakistan's strategy represented the "weaponisation of misinformation" into a full-spectrum disinformation warfare doctrine. By converting scattered falsehoods into a coordinated, state-driven propaganda ecosystem, Islamabad maximised reach, credibility, and psychological effect. The deliberate portrayal of *Operation Sindoor* as a false-flag attack became the central axis of this campaign, allowing Pakistan to invert accountability, project victimhood, and recast India's counter-terrorism operation as an act of aggression.

An important revelation of this report is the externalization of Pakistan's FIMI architecture through the involvement of foreign media and X influencers. Outlets such as *Global Times* (China), *TRT World* and *Anadolu Ajansi* (Turkey), and *AZERTAC* (Azerbaijan) reproduced Pakistan's propaganda almost verbatim, reflecting an emerging nexus of like-minded states pursuing geopolitical objectives through coordinated narrative warfare. Similarly, the participation of foreign X influencers helped extend the reach and credibility of Pakistani disinformation, embedding it within international digital discourse. This convergence of state-driven and non-state amplification represents the globalisation of disinformation campaigns where narrative influence becomes a shared instrument among strategic partners seeking to challenge India's diplomatic standing and regional influence.

This research also identifies a critical gap in India's policy framework: the absence of an explicit official definition and institutional mechanism addressing FIMI as a National security threat. While India has established fact-checking mechanisms like the PIB Fact Check Unit and adopted digital ethics codes, these measures remain fragmented and reactive. The challenge posed by transnational disinformation requires a holistic, multi-domain response and whole-of-society approach that integrates national security, diplomacy, and civil society. Therefore, India must move beyond "tactical containment" and establish a comprehensive, long-term strategy on cognitive defense, and deterrence and informational sovereignty to counter-FIMI.

Ultimately, Pakistan's disinformation offensive during and after *Operation Sindoor* serves as a critical case study in 21st-century cognitive warfare. It demonstrates that future conflicts will be fought as much in the minds of populations as in physical domains. For India, the challenge lies not merely in countering falsehoods but in defending the integrity of its information ecosystem and free and open digital space. The cognitive battlefield is here, and victory will belong not to those who shout the loudest, but to those who can sustain truth, trust, and strategic clarity in an age of weaponised narratives.

References

1. The print, (2025), “Pahalgam terror attack: Not any Intelligence Bureau team, Hindu tourists were the target” [Online: Web] Accessed 16 August 2025. URL: https://theprint.in/india/pahalgam-terror-attack-not-any-intelligence-bureau-team hindu-tourists-were-the-target/2600267/
2. Business standard (2025), “In a first, UNSC report names TRF as group behind Pahalgam terror attack”, [Online: Web] Accessed 16 Dec 2025. URL: https://www.business-standard.com/india-news/in-a-first-unsc-report-names-trf-asgroup-behind-pahalgam-terror-attack-125073001636_1.html
3. Press Trust of India (PTI). (2025), “Key timeline: Operation Sindoor and related developments”, The Print, [Online: Web] Accessed 16 Dec 2025. URL: https://theprint.in/india/key-timeline-operation-sindoor-and-relateddevelopments/2623720/
4. Press Trust of India (PTI). (2025), “Key timeline: Operation Sindoor and related developments”, The Print, [Online: Web] Accessed 16 Dec 2025. URL: https://theprint.in/india/key-timeline-operation-sindoor-and-relateddevelopments/2623720/
5. Press Trust of India (PTI). (2025), “Key timeline: Operation Sindoor and related developments”, The Print, [Online: Web] Accessed 16 Dec 2025. URL: https://theprint.in/india/key-timeline-operation-sindoor-and-relateddevelopments/2623720/
6. Bhat, R. (2013), “Fighting wards through radio broadcasts”, Journal of Mass Communication & Journalism, 3 (147), [Online: Web] Accessed 16 Dec 2025.
7. Watkins, L.A. (2025), “Pakistan’s media discipline after Pahalgam: Tactical or Transformational?”, International Policy Digest, [Online: Web] Accessed 16 Dec 2025. URL: https://intpolicydigest.org/pakistan-s-media-discipline-after-pahalgam-tactical-ortransformational/
8. DISA (2025), “Pakistan’s weaponization of disinformation against India”, [Online: Web] Accessed 16 Dec 2025. URL: Pakistan's Weaponization of Disinformation Against India | DISA
9. European External Action Service (2025), Information integrity and countering foreign information manipulation & interference (FIMI), European Union External Action Service Publication. Brussels. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
10. Bryjka, F. (2024), “EU Adopts to Countering Foreign Information Manipulation and Interference”. PISM. URL: PISM
11. European External Action Service (2022), “2021 StratCom Activity Report - Strategic Communication Task Forces and Information Analysis Division”. Brussels.
12. Disinformation (n.d.), “EU Foreign Information Manipulation and Interference (FIMI)”, [Online: Web] Accessed 19 August. 2025, URL: Foreign Information Manipulation and Interference (FIMI)
13. European External Action Service (2023), 1st EEAS Report on Foreign Information Manipulation and Interference Threats. Brussels. URL: 1st EEAS Report on Foreign Information Manipulation and Interference Threats

14. European External Action Service (2024), 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. Brussels. URL: 2nd EEAS Report on Foreign Information Manipulation and Interference Threats |EEAS
15. Disinformation (n.d.), "EU Foreign Information Manipulation and Interference (FIMI)", [Online: Web] Accessed 19 August. 2025. URL: Foreign Information Manipulation and Interference (FIMI)
16. European External Action Service (2019), Factsheet: Rapid Alert System (RAS). Brussels. URL: Factsheet: Rapid Alert System | EEAS
17. European External Action Service (2024), EEAS Stratcom's responses to Foreign Information Manipulation and Interference (FIMI) in 2023. Brussels. URL: EEAS Stratcom's responses to foreign information manipulation and interference(FIMI) in 2023 | EEAS
18. Disinformation (n.d.), "EU Foreign Information Manipulation and Interference (FIMI)", [Online: Web] Accessed 19 August 2025. URL: Foreign Information Manipulation and Interference (FIMI)
19. Rachael Burton (2018), "Disinformation in Taiwan and Cognitive Warfare", [Online: Web] Accessed 20 August 2025. URL: Disinformation in Taiwan and Cognitive Warfare | Global Taiwan Institute
20. Doublethink Lab (2024),"2024 Taiwan Elections: Foreign Influence Observation-Preliminiary Statement" [Online: Web] Accessed 20 August 2025. URL: 2024 Taiwan Elections: Foreign Influence Observation — Preliminary Statement | by Doublethink Lab | Doublethink Lab | Medium
21. Max tsung-chi Yu, Karl Ho (2022), "COVID and Cognitive Warfare in Taiwan", Accessed 20 August 2025. URL: COVID and Cognitive Warfare in Taiwan - PMC
22. Yu, C. (2024), "Taiwan Counters FIMI - Governmental and Parliamentary Responses", Taiwan Information Environment Research Center (IORG), [Online: Web] Accessed 20 August 2025. URL: https://iorg.tw/_en/a/taiwan-counters-fimi-gov-parl#h2-3
23. Yu, C. (2024), "Taiwan Counters FIMI - Governmental and Parliamentary Responses", Taiwan Information Environment Research Center (IORG), [Online: Web] Accessed 21 August 2025. URL: https://iorg.tw/_en/a/taiwan-counters-fimi-gov-parl#h2-3
24. Department of Homeland Security (2018), Foreign Interference Taxonym, United States of America. URL: Foreign%20Interference%20Taxonomy%20[July%202018].pdf
25. Disinformation (n.d.), "EU Foreign Information Manipulation and Interference (FIMI)", [Online: Web] Accessed 19 August. 2025, URL: Foreign Information Manipulation and Interference (FIMI)
26. U.S Department of State (2024), The Framework to Counter Foreign State Information Manipulation, United States of America. URL: The Framework to Counter Foreign State Information Manipulation - United States Department of State
27. United States Department of State (2024), The Department of State Announces Initiatives to Counter Foreign State Information Manipulation, American Journal of International Law, Vol. 118, No. 3, pp. 533–539, United States of America. URL: The Department of State Announces Initiatives to Counter Foreign State Information Manipulation | American Journal of International Law | Cambridge Core
28. U.S. Department of State (2024), The Framework to Counter Foreign State Information Manipulation, United States of America. URL: The Framework to Counter Foreign State Information Manipulation - United States Department of State

29. North Atlantic Treaty Organization (NATO) (2025), NATO's approach to counter information threats, Updated 03 February 2025. Brussels. URL: NATO - Topic: NATO's approach to counter information threats
30. North Atlantic Treaty Organization (NATO) (2024), NATO's approach to counter information threats: Public summary, 18 October 2024. Brussels. URL: NATO - Official text: NATO's approach to counter information threats - Public summary, 18-Oct.-2024
31. Disinformation.ch (n.d.), "EU Foreign Information Manipulation and Interference (FIMI)", [Online: Web] Accessed 24 August 2025. URL: https://www.disinformation.ch/EU_Foreign_Information_Manipulation_and_Interference_%28FIMI%29.html
32. Election commission of India (2024), Responsible and ethical use of social media platforms and strict avoidance of any wrongful use of political parties and their representatives during MCC period in General Elections and by elections, 6 May 2024, New Delhi. URL: https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf
33. Ministry of Information & Broadcasting, Government of India (2024), Government notifies PIB's Fact Check Unit under IT Rules 2021, Press Information Bureau, 20 March 2024, New Delhi. URL: Press Release: Press Information Bureau
34. Ministry of External Affairs, Government of India (2024), Quad Foreign Ministers' Meeting Joint Statement, 29 July 2024, New Delhi. URL: https://www.mea.gov.in/bilateral-documents.htm?dtl%2F38044%2FQuad+Foreign+Ministers+Meeting+Joint+Statement
35. Dunya News (2025), "Rushed FIR over Pahalgam incident exposes India's false flag operation: Tarar", [Online: Web] Accessed 24 August 2025. URL: Rushed FIR over Pahalgam incident exposes India's false flag operation: Tarar
36. operationsindoor.site |
37. The Nation (2025), "Pakistan releases dossier exposing Pahalgam false flag, Indian aggression", [Online: Web] Accessed 24 August 2025. URL: Pakistan releases dossier exposing Pahalgam False Flag, Indian aggression
38. Associated Press of Pakistan (2025), "Indian people, international community reject Modi's false flag operation in Pahalgam attack", [Online: Web] Accessed 24 August 2025. URL: Indian people, int'l community reject Modi's false flag operation in Pahalgam attack
39. Sabah News (2025), "Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy", [Online: Web] Accessed 25 August 2025. URL: Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy
40. Aaj News (2025), "India involved in sponsoring terrorism against Pakistan, says FO spokesperson; emphasises Pakistan has long been a victim of terrorism", [Online: Web] Updated 13 March 2025. Accessed 27 August 2025. URL:] India involved in sponsoring terrorism against Pakistan, says FO spokesperson -Pakistan - Aaj English TV
41. The Nation (2025), "RAW agents behind attack on London HC: Tarar", [Online: Web] Accessed 27 August 2025. URL: RAW agents behind attack on London HC: Tarar
42. Sabah News (2025), "Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy", [Online: Web] Accessed 2 September 2025. URL: Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy

43. Dialogue Pakistan (2025), “Indian army kills five of its Sikh soldiers as two units exchange fire in IIOJK”, [Online: Web] Accessed 2 September 2025. URL: Indian army kills five of its Sikh soldiers as two units exchange fire in IIOJK
44. Radio Pakistan (2025), “Analysts hail Deputy PM Ishaq Dar for urging India to shun anti-Pakistan policies”, [Online: Web] Accessed 2 September 2025. URL: https://www.radio.gov.pk/30-06-2025/analysts-hail-deputy-pm-ishaq-dar-forurging-india-to-shun-anti-pakistan-policies
45. Samaa TV (2025), “Pakistan downed 8 Indian jets in May, including 4 Rafales”, [Online: Web] Accessed 2 September 2025. URL: Pakistan downed 8 Indian jets in May, including 4 Rafales
46. The News (2025), “VIDEO: Pakistan crushes India’s S-400 system in Adampur”, [Online: Web] Accessed 2 September 2025. URL: VIDEO: Pakistan crushes India’s S-400 system in Adampur
47. Urdu Point (2025), “Pakistan destroys S-400 defence system, airfields”, [Online: Web] Published 10 May 2025. Accessed 2 September 2025. URL: Pakistan Destroys S-400 Defence System, Airfields - UrduPoint
48. DAWN (2025), “India’s post-Pahalgam gambit fails to win global support”, [Online: Web] Accessed 5 September 2025. URL: India’s post-Pahalgam gambit fails to win global support - World - DAWN.COM
49. World News Pakistan (2025), “Pakistan responds decisively to Indian aggression in Operation Bunyan Al-Marsoos: DG ISPR”, [Online: Web] Accessed 5 September 2025. URL: Pakistan responds decisively to Indian aggression in operation Bunyan Al Marsoos:DG ISPR | World News Pakistan
50. Dunya News (2025), “Jubilations erupt across Pakistan as India surrenders”, [Online: Web] Accessed 5 September 2025. URL: Jubilations erupt across Pakistan as India surrenders
51. Dawn (2025), “Pakistan dictates the pause, Baqir Sajjad Syed”, Online: Web] Accessed 5 September 2025. URL: Pakistan dictates the pause - Newspaper - DAWN.COM
52. Al Arabiya English (2025), “Ex-Pakistani PM assistant: Kashmir attack was false flag”, [Online: Youtube] Accessed 7 September 2025. URL: Ex-Pakistani PM assistant: Kashmir attack was false flag
53. Institute of Strategic Studies Islamabad, Issue Brief, DOMICIDE, ARRESTS, AND HATE WAVE: KASHMIRIS PAY THE PRICE OF INDIAN FALSE FLAG OPERATION, May 9, 2025. URL: IB_Mahwish_May_9_2025.pdf
54. Pak Mirror (2025), “Bunyan Al Marsoos: Pakistan’s strategic military operation strengthening National Security, Ali Raza”, [Online: Web] Accessed 5 September 2025. URL: Bunyan Al Marsoos: Pakistan’s Strategic Military Operation Strengthening National Security
55. Pakistan Observer (2025), “India’s misadventure proved suicidal for its international standing: Gen Zubair”, [Online: Web] Accessed 7 September 2025. URL: India’s misadventure proved suicidal for its international standing: Gen Zubair Pakistan Observer
56. The Stateman (2025), “PIB warns against fake Army document leaks: 16 Pakistani Youtube channels banned”, [Online: Web] Accessed 7 September 2025. URL: PIB warns against fake Army document leaks; 16 Pakistani YouTube channels banned - The Statesman

57. Dunya NEWS (2025), “Jubilations erupt across Pakistan as India Surrenders”, [Online: Web] Accessed 7 September 2025. URL: Jubilations erupt across Pakistan as India surrenders
58. AP NEWS (2025), “French Intelligence: China used embassies to undermine sales of France’s flagship Rafale fighter jet”, [Online: Web] Accessed 7 September 2025. URL: France fights to defend the reputation of its flagship fighter jet | AP News
59. The Express Tribune (2025), “How Indigenous technology helped PAF down Rafale”, [Online: Web] Accessed 7 September 2025. URL: How indigenous technology helped PAF down Rafale
60. Geo NEWS (2025), “Rafale vs J-10C: Battle of 4.5-gen fighters” [Online: Web] Accessed 7 September 2025. URL: Rafale vs J-10C: Battle of 4.5-gen fighters
61. DAWN (2025), “Pahalgam attack: India suspends Indus Waters Treaty with immediate effect, close Attari border crossing”, [Online: Web] Accessed 7 September 2025. URL: Pahalgam attack: India suspends Indus Waters Treaty with immediate effect, closes Attari border crossing - Pakistan - DAWN.COM
62. DAWN (2025), “India’s worn-out narrative: Full text of statement on NSC’s decisions”, [Online: Web] Accessed 7 September 2025. URL: ‘India’s worn-out narrative’: Full text of statement on NSC’s decisions - Pakistan -DAWN.COM
63. Statement by the Deputy Prime Minister/Foreign Minister at the Annual CoordinationMeeting of Foreign Ministers of OIC Member States
64. Meeting of the UN Security Council on the India-Pakistan Question
65. MITRE, Resources, Frequently Asked Questions, [Online: Web] Accessed 10 September 2025. URL: https://attack.mitre.org/resources/faq/
66. Hénin, N. (2023, April). FIMI: Towards a European redefinition of foreign interference. EU DisinfoLab.
67. EEAS or European External Action Service is essentially the diplomatic service and foreign affairs arm of the European Union (EU)
68. The Hindu (2025), “Pakistan Senate passes resolution rejecting India’s ‘attempt’ to link Pahalgam terror attack with Islamabad”, [Online: Web] Accessed 10 September 2025. URL: Pakistan Senate passes resolution rejecting India's 'attempt' to link Pahalgam terror attack with Islamabad - The Hindu
69. To name a few: Pakistan political leaders/personalities or diplomats such as Raoof Hasan (Al Arabiya English), Mohammad Faisal (Sky News), Attaulah Tarar (Sky News), carried the Islamabad’s message to the world through media.
70. The same narrative “habit of stagging incidents”, has been parroted by other politicians in Pakistan.
71. Fourth Pillar Post (2025), “India’s Pahalgam Narrative a Propaganda Drama”, [Online: Web] Accessed 10 September 2025. URL: India's Pahalgam Narrative a Propaganda Drama: Irfan Siddiqui
72. DAWN (2025),” Anti-India rally in Muzaffarabad condemns Pahalgam incident, calls for UN probe”, [Online: Web] Accessed 10 September 2025. URL: Anti-India rally in Muzaffarabad condemns Pahalgam incident, calls for UN probe Pakistan - DAWN.COM

73. Voice of Masses (2025), “Azad Jammu and Kashmir President Barrister Sultan Mahmood Chaudhry has stated that India is projecting itself as a peace-loving nation globally while concealing the atrocities committed against Kashmiris in occupied Kashmir”, [Online: Web] Accessed 10 September 2025. URL: Azad Jammu and Kashmir President Barrister Sultan Mahmood Chaudhry has stated that India is projecting itself as a peace-loving nation globally while concealing theatrocities committed against Kashmiris in occupied Kashmir – https://www.dailyindependent.com.pk
74. Sky NEWS (2025),” Pakistan warns Kashmir row could lead to ‘all-out war’ with India”, [Online: Youtube] Accessed 10 September 2025. URL: Pakistan warns Kashmir row could lead to 'all-out war' with India | The World with Yalda Hakim - YouTube
75. News9Tweets (2025), “The good and the bad: Outlines of tomorrow,” [Online: Twitter] Accessed 13 September 2025. URL: https://x.com/News9Tweets/status/1916482958069764244?s=20
76. DISA (2025), “Debunking “Dance of the Hillary”: An Analysis of a Viral Pakistani Malware Hoax”, [Online: Web] Accessed 13 September 2025. URL: Debunking "Dance of the Hillary": An Analysis of a Viral Pakistani Malware Hoax | DISA
77. India Today (2025), “Spying: Pakistani hackers target India's defence sector with Op Sindoor bait”, [Online: Web] Accessed 13 September 2025.URL: Spying: Pakistani hackers target India’s defence sector with Op Sindoor bait - India Today
78. Sabah News (2025), “Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy”, [Online: Web] Accessed 16 September 2025. URL: Attaullah Tarar says India has institutionalized terrorism as a tool of foreign policy
79. The Nation (2025), “RAW agents behind attack on London HC: Tarar”, [Online: Web] Accessed 16 September 2025. URL: RAW agents behind attack on London HC: Tarar
80. Associated Press of Pakistan (2025), “Indian people, international community reject Modi’s false flag operation in Pahalgam attack”, [Online: Web] Accessed 16 September 2025. URL: Indian people, int’l community reject Modi’s false flag operation in Pahalgam attack
81. https://disa.org/pakistans-disinformation-campaign-following-the-pahalgam-terrorattack-targets-sikh-soldiers-with-khalistani-support/
82. Hénin, N. (2023, April). FIMI: Towards a European redefinition of foreign interference. EU DisinfoLab.
83. Press Trust of India (2025), “PTI Fact Check: It's CHEAPFAKE! AI-generated video of EAM Jaishankar shared with false, fabricated, baseless claims; details inside”, [Online: Web] Accessed 24 September 2025. URL: https://www.ptinews.com/fact-detail/It-s-CHEAPFAKE!-AI-generated-video-of-EAM-Jaishankar-shared-with-false--fabricated--baseless-claims%3B-details-inside/2545264
84. PIB Fact Check (2025), “An old image showing a crashed aircraft is being re-circulated by pro-Pakistan handles in various forms in the current context of 'Operation Sindoor”, [Online: Twitter] Accessed 24 September 2025. URL: https://x.com/PIBFactCheck/status/1919973596665135471
85. The Asian Mirror (2025), “‘Sindoor Ban Gaya Tandoor’: Pakistanis flood social media with memes after Indian airstrikes”, [Online: Web] Accessed 24 September 2025. URL: https://theasianmirror.com/latest/61020/sindoor-ban-gaya-tandoor-pakistanis-floodsocial-media-with-memes-after-indian-airstrikes/
86. Statement on Baseless Indian Allegations

87. NEWS18 (2025), “Pakistan Attacks J&K, Punjab, Rajasthan: Locations, Response, And More”, [Online: Web] Accessed 24 September 2025. URL: Pakistan Attacks J&K, Punjab, Rajasthan: Locations, Response, And More | Explained | Explainers News - News18
88. Abhishek R. (2025),”How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?”, [Online: LinkedIn] Accessed 24 September 2025. URL: How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?
89. Abhishek R. (2025),”How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?”, [Online: LinkedIn] Accessed 24 September 2025. URL: How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?
90. Radio Pakistan (2025), “India sponsoring terrorism in Pakistan and beyond: DG ISPR”, [Online: Web] Accessed 24 September 2025. URL: India sponsoring terrorism in Pakistan and beyond: DG ISPR
91. Geo NEWS (2025), “Political leaders respond to Modi's speech after ceasefire”, [Online: Web] Accessed 24 September 2025. URL: Political leaders respond to Modi's speech after ceasefire
92. The Hindu (2025), “Fact Check: False claims surrounding Operation Sindoor flood social media”, [Online: Web] Accessed 24 September 2025. URL: https://www.thehindu.com/news/national/fact-check-false-claims-surrounding-operation-sindoor-flood-social-media/article69552318.ece
93. https://x.com/ForumStrategic/status/1921527231710433453
94. PIB Fact Check (2025), “Pro-Pakistan social media accounts are falsely claiming that confidential documents related to the preparedness of the #IndianArmy have been leaked”, [Online: Twitter] Accessed 24 September 2025. URL: PIB Fact Check on X: "Pro-Pakistan social media accounts are falsely claiming that confidential documents related to the preparedness of the #IndianArmy have been leaked #PIBFactCheck ❌ These documents are #FAKE ✅ Please avoid sharing unverified information and rely only on official sources from https://t.co/qRGdn8vUgr" / X
95. Pakistan Strategic Forum (2025), “From the battlefield to the operations in the air, CAS Air Chief Marshal Zaheer Ahmad Baber Sidhu of the Pakistan Air Force.”, [Online: Facebook] Accessed 24 September 2025. URL: Facebook
96. Seqrite (2025), “Advisory: Pahalgam Attack themed decoys used by APT36 to target the Indian Government”, [Online: Web] Accessed 25 September 2025. URL: Advisory: Pahalgam Attack themed decoys used by APT36 to target the Indian Government | Seqrite
97. Zscaler (2022), “APT-36 Uses New TTPs and New Tools to Target Indian Governmental Organizations”, [Online: Web] Accessed 25 September 2025. URL: Indian Governmental Organizations Targeted by APT-36
98. Ministry of Information & Broadcasting (2025), “Government Debunks Pakistani Propaganda Against India and Armed Forces via Official Fact-Check Unit”, [Online: Web] Accessed 25 September 2025. URL: Press Release:Press Information Bureau
99. DAWN (2020), “Pakistan rubbishes India's 'charge sheet' in Pulwama attack case as 'motivated propaganda'”, [Online: Web] Accessed 25 September 2025. URL: Pakistan rubbishes India's 'charge sheet' in Pulwama attack case as 'motivated propaganda' - World - DAWN.COM

100. Global Defense Insight (2025), “A Recurring Pattern of India’s False Flag Operation”, [Online: Web] Accessed 25 September 2025. URL: https://defensetalks.com/a-recurring-pattern-of-indias-false-flag-operation/
101. Xinhua (2025), “26 civilians killed, 46 injured in Indian attack on Pakistan: official”, [Online: Web] Accessed 25 September 2025. URL: https://english.news.cn/20250507/cd4eb93abfcf4fc0a9f01fd70b55bec0/c.html
102. Global Times (2025), “India confirms air strikes on Pakistan-controlled Kashmir”, [Online: Web] Accessed 25 September 2025. URL: India confirms air strikes on Pakistan-controlled Kashmir - Global Times
103. Global Times (2025), “The Pakistan Air Force (PAF) has shot down another Indian fighter jet in response to overnight airstrikes carried out by India at multiple locations in Pakistan, sources from the Pakistani military said on Wednesday”, [Online: Twitter] Accessed 25 September 2025. URL: https://x.com/globaltimesnews/status/1919891598894366992
104. India in China (2025), “Dear @globaltimesnews, we would recommend you verify your facts and cross-examine your sources before pushing out this kind of dis-information.”, [Online: Twitter] Accessed 25 September 2025. URL: India in China on X: "(1/n) Dear @globaltimesnews , we would recommend you verify your facts and cross-examine your sources before pushing out this kind of dis-information." / X
105. https://gb.china-embassy.gov.cn/eng/zgyw/202502/t20250206_11550159.html
106. Ministry of Foreign Affairs People’s Republic of China (2018), “Joint Statement between the People's Republic of China and the Islamic Republic of Pakistan on Strengthening China-Pakistan All-Weather Strategic Cooperative Partnership and Building Closer China-Pakistan Community of Shared Future in the New Era” China DIFF FORMAT
107. DAWN (2025), “Pakistan, China agree on joint media cooperation against fake news”, [Online: Web] Accessed 25 September 2025. URL: https://www.dawn.com/news/1923261/pakistan-china-agree-on-joint-media-cooperation-against-fake-news
108. FirstPost (2025), “7 factors that forced India to crack down on Turkey's TRT”, [Online: Web] Accessed 28 September 2025. URL: https://www.firstpost.com/world/india-bans-blocks-trt-world-media-boycott-turkey-tensions-with-pakistan-operation-sindoor-13888418.html
109. TRT World (2025), “Pakistan warns India of 'devastation' after New Delhi's 'jingoistic statements”, [Online: Web] Accessed 16 October 2025. URL: Pakistan warns India of 'devastation' after New Delhi's 'jingoistic statements' - TRT World
110. TRT World (2025), “Pakistan launches 'Bunyan-un-Marsoos' military operation against India”, [Online: Web] Accessed 25 September 2025. URL: Pakistan launches 'Bunyan-un-Marsoos' military operation against India - TRT World
111. TRT World (2025), “Pakistan downs five Indian warplanes and drones — Defence Minister”, [Online: Web] Accessed 25 September 2025. URL: Pakistan downs five Indian warplanes and drones — Defence Minister - TRT World
112. TRT World (2025), “Pakistan has shot down five Indian warplanes and taken some Indian soldiers’ prisoner, Defence Minister Khawaja Asif and Pakistani military spokesperson say”, [Online: Twitter] Accessed 25 September 2025. URL: https://x.com/trtworld/status/1919903625687535971

113. Anadolu Ajansı (2025), “Islamabad launches retaliatory attacks against Indian military installations: Pakistan Army”, [Online: Web] Accessed 26 September 2025. URL: Islamabad launches retaliatory attacks against Indian military installations: Pakistan Army
114. Turkey-Pakistan: Secret Army of Mercenary Journalists, A Strategic Report 2021. Research Institute for European and American Studies (RIEAS) on 26 February 2021. URL: https://rieas.gr/images/editorial/medasiajournalist21.pdf
115. Azertac (2025), “The United Nations Security Council held closed consultations under the agenda item ‘The India-Pakistan Question’”, [Online: Web] Accessed 26 September 2025. URL: The United Nations Security Council held closed consultations under the agenda item “The India-Pakistan Question” - AZERTAC
116. Azertac (2025), “Pakistan launches “Operation Bunyan-un-Marsoos” to respond to blatant aggression; targets key Indian military installations”, [Online: Web] Accessed 26 September 2025. URL: Pakistan launches “Operation Bunyan-un-Marsoos” to respond to blatant aggression; targets key Indian military installations - AZERTAC
117. Ministry of Foreign Affairs Azerbaijan, No:184/25, Statement on escalation of tension between India and Pakistan. Republic of Azerbaijan. URL: https://mfa.gov.az/en/news/no18425
118. Azertac (2025), “Azerbaijan’s Foreign Ministry condemns military attacks against Pakistan”, [Online: Web] Accessed 26 September 2025. URL: Azerbaijan’s Foreign Ministry condemns military attacks against Pakistan - AZƏRTAC - Zəif görənlər üçün
119. Azertac (2025), “26 Indian military targets hit during “Operation Bunyan-un-Marsoos”: Pakistan” [Online: Web] Accessed 26 September 2025. URL: 26 Indian military targets hit during “Operation Bunyan-un-Marsoos”: Pakistan - AZERTAC
120. Azertac (2025), “Pakistan launches “Operation Bunyan-un-Marsoos” to respond to blatant aggression; targets key Indian military installations”, [Online: Web] Accessed 26 September 2025. URL: Pakistan launches “Operation Bunyan-un-Marsoos” to respond to blatant aggression; targets key Indian military installations - AZERTAC
121. The Diplomatic Insight (2025), “Azerbaijan-Pakistan Ties: A Bond of Strength and Trust”, [Online: Web] Accessed 26 September 2025. URL: Azerbaijan-Pakistan Ties: A Bond of Strength and Trust - TDI
122. Shanghai Panda (2025), “China backs the Pakistani govt, not terrorist organizations.” [Online: Twitter] Accessed 28 September 2025. URL: ShanghaiPanda （Account deactivation） on X: "China backs the Pakistani govt, not terrorist organizations. Beijing opposes terror organizations, not the Indian govt. There is no evidence Pakistani govt launched terror attacks on Indian tourists. Thus, China opposes to the Modi regime initiating war against Pakistan for https://t.co/t8HAVSYLbC" / X
123. Shanghai Panda (2025), “Dear Indonesian friends, you spent $8.1b to buy 42 Rafale fighter jets - this money could’ve bought 203 J-10Cs that defeated Rafales in Air battle between Pakistan & India days ago.”, [Online: Twitter] Accessed 28 September 2025. URL: ShanghaiPanda （Account deactivation） on X: "Dear Indonesian friends, you spent $8.1b to buy 42 Rafale fighter jets - this money could’ve bought 203 J-10Cs that defeated Rafales in Air battle between Pakistan & India days ago. I feel your deal is not a good deal.😅 https://t.co/HC2fi6Y72c" / X

124. William Huo (2025), “India thought it could make China its declared enemy to impress Washington. All it got in return was a second hand NATO alliance and a Pakistan armed with PL-15 missiles. This is the story of the J-10C, Rafale, and the price of misplaced loyalty.”, [Online: Twitter] Accessed 28 September 2025. URL: https://x.com/wmhuo168/status/1921085939687801114?s=20
125. William Huo (2025), “India scrambled jets. Pakistan struck back. But the real winner flew quietly above them all made in China. Here's how Beijing's invisible eye dominated the battlefield without firing a shot.”, [Online: Twitter] Accessed 28 September 2025. URL: https://x.com/wmhuo168/status/1924973627977462109?s=20
126. Angelo Giuliano (2025), “China's fighter jet dominance in the India-Pakistan conflict marks another "DeepSeek" moment.”, [Online: Twitter] Accessed 28 September 2025. URL: https://x.com/angeloinchina/status/1921398504381141208?s=20
127. Jackson Hinkle (2025), “BREAKING: Pakistani Foreign Minister said all Indian planes were shot down by Chinese Chengdu J-10C fighters.”, [Online: Twitter] Accessed 28 September 2025. URL: https://x.com/jacksonhinklle/status/1920146198154838338?s=20
128. DISA (2025),”Pakistan’s Alleged Disinformation Campaign Against India During Operation Sindoor”, [Online: Web] Accessed 28 September 2025. URL: Pakistan's Alleged Disinformation Campaign Against India During Operation Sindoor | DISA
129. DISA (2025),” Pakistan’s Alleged Disinformation Campaign Against India During Operation Sindoor”, [Online: Web] Accessed 28 September 2025. URL: Pakistan's Alleged Disinformation Campaign Against India During Operation Sindoor | DISA
130. India Today (2025), “Pakistan's ISI uses social media to spread defamatory lies about India”, [Online: Web] Accessed 28 September 2025. URL: Pakistan's ISI uses social media to spread defamatory lies about India - India Today
131. DISA (2025),” Exclusive: ISPR’s Disinformation Campaign Against India”, [Online: Web] Accessed 28 September 2025. URL: Exclusive: ISPR's Disinformation Campaign Against India | DISA
132. NDTV (2025), “The Spy Next Door: How Ordinary Indians Became Pakistani ISI Assets”, [Online: Web] Accessed 28 September 2025. URL: The Spy Next Door: How Ordinary Indians Became Pakistani ISI Assets
133. DISA (2025),” Exclusive: ISPR’s Disinformation Campaign Against India”, [Online: Web] Accessed 28 September 2025. URL: Exclusive: ISPR's Disinformation Campaign Against India | DISA
134. Samaa TV (2025), “India fired six ballistic missiles on own territory: ISPR”, [Online: Web] Accessed 30 September 2025. URL: India fired six ballistic missiles on own territory: ISPR
135. Radio Pakistan (2025), “Armed Forces fulfilled promise with nation against India's blatant aggression: DG ISPR”, [Online: Web] Accessed 30 September 2025. URL: Armed Forces fulfilled promise with nation against India's blatant aggression: DG ISPR
136. Geo News (2025), “PAF downed five Indian aircraft in largest aerial battle of modern times”, [Online: Web] Accessed 30 September 2025. URL: PAF downed five Indian aircraft in largest aerial battle of modern times
137. DISA (2025),” Exclusive: ISPR’s Disinformation Campaign Against India”, [Online: Web] Accessed 30 September 2025. URL: Exclusive: ISPR's Disinformation Campaign Against India | DISA

138. Statement on Baseless Indian Allegations
139. United Nation Security council, Letter dated 8 May 2025 from the Permanent Representative of Pakistan to the United Nations addressed to the President of the Security Council. 9 may 2025. Switzerland. URL: https://digitallibrary.un.org/record/4082024/files/S_2025_299-EN.pdf
140. Permanent mission of Pakistan to the United Nations, "Transcript of the Media Briefing by the Spokesperson on Friday, 23rd May 2025". Switzerland. URL: https://pakungeneva.pk/transcript-of-the-media-briefing-by-the-spokesperson-onfriday-23rd-may-2025/
141. The Nation (2025), "False Flag Operation", [Online: Web] Accessed 1 October 2025. URL: False Flag Operation
142. DAWN (2025), "'India's worn-out narrative': Full text of statement on NSC's decisions", [Online: Web] Accessed 1 October 2025. URL: 'India's worn-out narrative': Full text of statement on NSC's decisions - Pakistan - DAWN.COM
143. Institue of Strategic Studies Islamabad (2025), "Pahalgam Incident: Another False Flag Operation?", [Online: Web] Accessed 1 October 2025. URL: https://issi.org.pk/wp-content/uploads/2025/04/IB_Mahwish_April_29_2025-2.pdf
144. Centre for International Strategic Studies (2025), "Pakistan's Response to 'Operation Sindoor'", [Online: Web] Accessed 1 October 2025. URL: Pakistan's Response to 'Operation Sindoor' - CISS Pakistan - Center For International Strategic Studies
145. https://x.com/ForumStrategic/status/1921527231710433453
146. India Today (2025), "Pakistan's propaganda machine in overdrive after Operation Sindoor", [Online: Web] Accessed 1 October 2025. URL: https://www.indiatoday.in/world/story/pakistans-propaganda-machine-in-overdrive-after-operation-sindoor-2721388-2025-05-08
147. Mohammed Zubair (2025), "Beware! These are Pakistani propaganda accounts pretending to be Indian Army Personals.", [Online: Twitter] Accessed 3 October 2025. URL: https://x.com/zoo_bear/status/1919930898159698383?s=20
148. Abhishek R. (2025)," How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?", [Online: LinkedIn] Accessed 3 October 2025. URL: How India Debunked Pakistani Social Media Propaganda Post Operation Sindoor?
149. Ministry of Information & Broadcasting (2025), "Government Debunks Pakistani Propaganda Against India and Armed Forces via Official Fact-Check Unit", [Online: Web] Accessed 3 October 2025. URL: Press Release:Press Information Bureau
150. Mint (2025), "Govt fact-checking unit swings into action in the wake of Operation Sindoor to highlight false claims", [Online: Web] Accessed 3 October 2025. URL: Govt fact-checking unit swings into action in the wake of Operation Sindoor to highlight false claims | Mint
151. DISA (2025), "India Neutralizes Pakistani Disinformation Campaign", [Online: Web] Accessed 8 October 2025. URL: India Neutralizes Pakistani Disinformation Campaign | DISA
152. Ministry of External Affairs, "Visit of All Party Delegations (OPERATION SINDOOR)", URL: https://www.mea.gov.in/visit-of-all-party-delegations-operation-sindoor.htm

153. Akashvani News (2025), “Govt to send all party delegation to 32 Nations to highlight India’s Anti-Terror resolve in backdrop of Operation Sindoor”, [Online: Web] Accessed 9 October 2025. URL: Govt to send all party delegation to 32 Nations to highlight India’s Anti | DD News On Air
154. The Print (2025), “7 delegations & 1 message: How India chose 33 countries for ambitious diplomatic push post-Op Sindoor”, [Online: Web] Accessed 12 October 2025. URL: https://theprint.in/diplomacy/7-delegations-1-message-how-india-chose-33-countries-for-ambitious-diplomatic-push-post-op-sindoor/2630617/
155. The Hindu (2025), “Influencing interlocutors: On Operation Sindoor, India’s delegations”, [Online: Web] Accessed 12 October 2025. URL: Influencing interlocutors: On Operation Sindoor, India’s delegations - The Hindu
156. The Economic Times (2025), “Pakistan got UNSC to drop mention of LeT offshoot TRF”, [Online: Web] Accessed 12 October 2025. URL: Pakistan got UNSC to drop mention of LeT offshoot TRF - The Economic Times
157. Akashvani News (2025), “Colombia withdraws statement condoling deaths in Pakistan after Indian strikes during Operation Sindoor”, [Online: Web] Accessed 13 October 2025. URL: Colombia withdraws statement condoling deaths in Pakistan after Indian strikes during Operation Sindoor | DD News On Air
158. India Today (2025), “As Op Sindoor gains global traction, Pak resorts to desperate tactics in Denmark”, [Online: Web] Accessed 15 October 2025. URL: As Operation Sindoor gains global traction, Pakistan resorts to desperate tactics in Denmark - India Today
159. ANI (2025), “"Delegation that PM Modi has sent is having an impact," All-Party Delegation member says”, [Online: Web] Accessed 15 October 2025. URL: "Delegation that PM Modi has sent is having an impact," All-Party Delegation member says
160. Akashvani News (2025), “India’s Tough Stand on Terror Draws Global Praise; Denmark Backs Modi’s Response”, [Online: Web] Accessed 15 October 2025. URL: https://www.newsonair.gov.in/indias-tough-stand-on-terror-draws-global-praise-denmark-backs-modis-response/

Thank You Note

This report represents not just an analytical exercise but a collective commitment. A commitment to truth, integrity, and India's information sovereignty. The team at Future Shift Labs (FSL) extends its deepest gratitude to everyone who made this publication possible.

We express our sincere appreciation to Sunanda R. Marak, whose intellectual depth and unwavering rigour have shaped this study into a comprehensive and thought-provoking contribution to the field of digital geopolitics. Her ability to bridge theory with actionable insight reflects the highest standards of scholarship and national relevance.

We also extend our heartfelt thanks to Mr Nitin Narang, Founder of FSL, and Mr Sagar Vishnoi, Director of FSL, for their strategic vision and guidance throughout this project. Their belief in fostering interdisciplinary research at the intersection of technology, policy, and national security continues to inspire our work every day.

Special acknowledgement is due to our research associates, data analysts, and editorial team, who meticulously verified sources, mapped digital trails, and designed this report with precision and care. Their behind-the-scenes effort forms the backbone of every credible insight contained within these pages.

Finally, we thank our partners in academia, media, and policy institutions who continue to engage with us in building a resilient, transparent, and globally aware information ecosystem.

This report is dedicated to all digital defenders, researchers, and policymakers striving to protect the cognitive frontiers of India, where ideas, narratives, and technologies intersect. May it serve as both a resource and a reminder that in the age of hybrid warfare, information integrity is the first line of national defence.

Future Shift Labs

Future Shift Labs Foundation,
Address: 13th Floor, Skymark One, H-10/A Tower E, Sector - 98, Noida, Uttar Pradesh - 201301

www.futureshiftlabs.com