Countering Disinformation in Hybrid Warfare: Lessons from Operation Sindoor and the Role of the Chief of Defence Staff

Author Bio
Col Rajesh Kumar Sharma is a researcher in strategic studies and defence policy, with special interest in hybrid warfare, military modernization and South Asian security dynamics. He is currently completing his doctoral work on *Global Trends in Hybrid Warfare and Its Reflections on the Indian Army* at CUHP, Himachal Pradesh. Col Sharma regularly contributes to think tank reports and defence policy journals.

Abstract
Hybrid warfare has emerged as the defining mode of conflict in the 21st century, blending conventional military tactics with cyberattacks, psychological operations and disinformation. 'Operation Sindoor', India's recent multi-domain military campaign, stands as a watershed moment in showcasing both the strength and vulnerabilities of modern Indian defence strategy. The Chief of Defence Staff (CDS), in a revealing post-operation briefing, acknowledged that **15%** of time, resources and effort during the operation were lost due to misinformation. This paper explores the implications of this statement within the larger framework of hybrid warfare, evaluates the evolving role of the CDS in coordinating India's response and recommends systemic changes to strengthen national resilience against cognitive warfare. With a focus on lessons from Operation Sindoor, the paper proposes a doctrinal and institutional roadmap for countering disinformation in India's security architecture.

Keywords
Hybrid Warfare, Operation Sindoor, Chief of Defence Staff, Disinformation, Cognitive Warfare, Indian Armed Forces, Information Security, National Defence Strategy

1. Introduction
The 21st-century battlefield has undergone a paradigm shift, where victory is solely not determined by tanks and troops but by information dominance, narrative control and public perception. As hybrid warfare becomes the new norm, modern militaries must adapt to threats that lie in the grey zone between war and peace. India's defence posturehistorically rooted in kinetic and territorial warfarefaces a transformative challenge in this new landscape.

A notable demonstration of India's hybrid warfare capabilities and vulnerabilities was evident during Operation Sindoor, a joint-force operation conducted in response to multi-vector threats across India's northern border and maritime perimeter. The Chief of Defence Staff (CDS), in his operational debrief, made a critical observation that *approximately 15% of India's time, effort and resources were wasted in addressing misinformation and disinformation campaigns propagated by hostile entities*.

This startling revelation foregrounds the urgency of recalibrating India's doctrinal and operational response to disinformation. This paper delves into the nature of hybrid threats, evaluates the performance of India's integrated military apparatus during Operation Sindoor and recommends strengthening the institutional role of the CDS to preempt, neutralise and counter adversarial narrative warfare.

2. Understanding Hybrid Warfare and Information Threats

Hybrid warfare is not a singular form of conflict, but rather a composite strategy combining conventional warfare, irregular tactics, cyber operations and psychological warfare to achieve strategic goals without full-scale escalation. The most insidious component of hybrid warfare is disinformation;the deliberate spread of false or manipulated information intended to mislead, create confusion and erode public trust.

Global case studies highlight how effective information warfare can redefine the battlefield:

- Russia's Crimea campaign (2014) used a blend of military pressure and psychological operations, supported by cyber disruption and social media manipulation.
- In Syria, Iran-backed militias used deep-fake videos to influence rebel morale.
- China's "Three Warfares" doctrine (media, legal and psychological) continues to influence the Indo-Pacific narrative space.

In the Indian context, the challenges are particularly acute. Misinformation campaignsranging from manipulated battlefield imagery to fake casualty reportsare not only launched by adversarial states but also amplified by domestic actors. The porous information ecosystem makes it difficult for citizens to discern verified news from propaganda, weakening national unity during conflict.

3. Operation Sindoor: A Test of India's Integrated Hybrid Response

Operation Sindoor, conducted in early 2025, marked a defining moment in India's evolving response to hybrid threats, representing the most sophisticated test of its integrated tri-service doctrine under real-time multi-domain pressure. While previous border skirmishes and localized conflicts tested kinetic preparedness, Operation Sindoor represented a full-spectrum challenge involving conventional warfare, cyber sabotage, electronic warfare, maritime disruptions and a highly coordinated disinformation campaign.

3.1. Background and Strategic Context

The operation was launched in response to simultaneous provocations by a state-sponsored proxy militiaalong the northern borders, a massive cyberattack on key government and military systems and sabotage threats to maritime assets in the Arabian Sea and the Bay of Bengal. These events were not isolated; rather, they followed a classic hybrid playbook: initial psychological provocation, cyber disruption, kinetic confrontation and global disinformation campaigns. The synchrony of threats suggested coordination by hostile powers seeking to exploit India's doctrinal gaps in hybrid threat management.

This was the first major test of India's Theatre Command structureand the coordinating capacity of the Chief of Defence Staff (CDS), working in real time across land, air, cyber, sea and information domains.

3.2. Multi-Domain Operational Phases

Phase I: Cyber-Electronic Sabotage (Day 0 – Day 2)

- India's military satellite communications experienced signal jamming in the Himalayan belt.
- Simultaneously, CERT-IN, along with the Defence Cyber Agency, thwarted multiple DDoS attacks and malware intrusions targeting defence procurement and troop deployment databases.
- State-run media websites were defaced and fake notifications regarding military mobilization were circulated.

Phase II: Psychological and Disinformation Warfare (Day 1 – Day 6)

- Thousands of deep-fake videos, purporting to show civilian casualties and alleged military atrocities were disseminated across platforms like Facebook, Instagram, WhatsApp and X (formerly Twitter).
- Fabricated news items from cloned Indian news portals created panic and mistrust.

- Hostile nations' state media amplified these narratives globally, attempting to discredit India's response.

The Chief of Defence Staff later revealed that 15% of total operational resources were diverted to counter misinformation, which delayed decision-making in frontline commands and led to unnecessary re-tasking of intelligence units.

Phase III: Kinetic Engagement (Day 3 – Day 10)

- The Indian Army launched a precision retaliation operation against proxy launch pads and supply lines using indigenous artillery systems (Pinaka, Dhanush).
- The Indian Navy's Western Command conducted Operation Trident Sentinel, deploying P-8I aircraft and destroyers to intercept suspicious vessels potentially laden with sea mines.
- The IAF conducted both manned and unmanned ISR missions, using Tejas jets and Heron drones to map enemy movement and signal activity.
- Coordinated Special Forces raids neutralised forward control nodes that were linked to the digital sabotage effort.

Phase IV: Diplomatic and Narrative Response (Day 4 – Day 12)

- India's Ministry of External Affairs (MEA), in coordination with the CDS and Ministry of Defence, launched a strategic information campaign, distributing verifiable satellite imagery and operational briefings to international media.
- Indian embassies were instructed to counter adversarial narratives using real-time social media interventions and interactions with strategic analysts abroad.
- India's Public Diplomacy Division issued over 20 official responses to global media queries, successfully discrediting many hostile propaganda pieces.

3.3 Likely Areas and Domains Targeted During Operation Sindoor

- Terror Launchpads in Pakistan-Occupied Jammu and Kashmir (PoJK) - Areas near Kel**,** Athmuqam**,** Leepa Valleyand Chakothi**.**These were suspected to house training camps**,** infiltration hubs and storage facilitiesfor arms and narcotics.
- Cross-Border Command-and-Control Centres - Signals intelligence (SIGINT)intercepted communication hubs reportedly in Muzaffarabad**,** Kotliand Baghsectors.These were likely hit using precision standoff weaponsand electronic warfaredisruption.
- Cyber & Information Warfare Infrastructure - Indian cyber units are believed to have neutralized disinformation networks, particularly social media bot farmsoperating from Rawalpindiand Lahore**.**Websites spreading anti-India propagandalinked to ISI front organizations.Fake digital media accountstargeting Indian morale and global perception during the operation.
- Strategic Economic Nodes - Analysts suggest cyber or kinetic threatsmay have been aimed at illicit financing channelsoperating through Karachi;Smuggling corridorson the Punjab-Balochistan axis**.**Unregulated money flowaiding terror infrastructure.
- Proxy Groups and Militias Operating in the Border Belt - Reports indicated action against groups likeLashkar-e-Taiba in areas like Balakot and Jaish-e-Mohammed in Bahawalpur region**.**It was intended against hybrid militantsattempting infiltration across Gurez, Uri and Rajouri sectors**.**
- Psychological Operations Targets - Broadcast jamming and psychological deterrents possibly targeted:Anti-India radio stationsoperating near the LOC**.**Online radicalization platformsinfluencing vulnerable populations.Leaflet drops and drone-broadcast warnings in border-adjacent regions.

3.4. Indigenous Systems and Joint Force Integration

A critical strength of Operation Sindoor was the use of "Make in India" platforms, which not only performed efficiently but also boosted confidence in indigenous innovation:

- Akash NG surface-to-air missiles intercepted hostile UAVs.
- Netra AEW&C systems, designed by DRDO, provided early warning of cross-border airspace violations.
- AI-enabled battlefield management software integrated inputs from the Army, Navy and Air Force, enabling faster targeting and coordination.

This marked the first major deployment of joint battlefield data fusion, coordinated by the Integrated Defence Staff under the supervision of the CDS. The operation also validated the importance of interoperability drills conducted under Theatre Commands.

3.5. Institutional Coordination and Civilian-Military Interface

A major challenge encountered during the operation was the slow civil-military coordination in tackling disinformation:

- Social media platforms were slow to respond to requests for takedowns of deep-fake videos and hate speech.
- State police and local administrators, who lacked real-time access to military briefings, at times responded to false intelligence circulated through manipulated audio messages.
- The Ministry of Electronics and Information Technology (MeitY) had to hastily set up a joint task force with CERT-IN and NTRO to issue verified communication.

Despite delays, the operation concluded with tactical victories on all fronts and the Defence Ministry declared the operation a "strategic and operational success."However, the cognitive costespecially the 15% misallocation due to misinformationprompted immediate calls for doctrinal and institutional reform.

3.6. Key Takeaways from Operation Sindoor

Domain	Successes	Shortfalls
Military (Kinetic)	Rapid tri-service deployment, integration of indigenous weapon systems	Logistical misdirection due to early disinformation
Cyber	Quick neutralisation of DDoS threats by CERT-IN	Weak initial detection of malware signatures
Information/Narrative	Strong counter-propaganda from MEA and MoD	Delayed takedown of hostile fake content
Jointness	First operational validation of Theatre Command coordination	Inter-ministerial silos persisted in early response
Technology	AI-integrated C^4ISR systems, indigenous missiles performed excellently	Limited offensive cyber capabilities

3.7. Operation Sindoor in Strategic Perspective

Operation Sindoor was not just a response to a hybrid attackit was a doctrinal inflection point. For the first time, India faced simultaneous conflict in five warfare domains. The operation:

- Validated the need for full-spectrum deterrence.
- Exposed the urgency of an hybrid Warfare Formation with Information formation integrated into it.
- Highlighted the critical role of the CDS as the nerve centre of hybrid response.

By absorbing these lessons into future doctrine, India can move from reactive containment to proactive dominance in hybrid warfare.

4. Role of the CDS in Hybrid Warfare Management

The Chief of Defence Staff (CDS) was established to serve as the single-point military advisor to the government and to foster integration across India's armed services. However, the evolving character of modern conflictmarked by hybrid warfarehas expanded the CDS's role beyond traditional military oversight to encompass coordination across multiple domains: cyber, space, information, psychological and kinetic operations. The CDS is now at the heart of India's strategic and operational response to hybrid threats.

4.1 Institutional Integration and Jointness

At its core, hybrid warfare demands seamless coordination among the Army, Navy, Air Force, cyber units, space-based assets, intelligence services and civilian institutions. The CDS plays a pivotal role in realizing this integration. By spearheading joint operational doctrines, restructuring commands for greater synergy and establishing theatre commands, the CDS ensures that India's armed forces respond as a unified force rather than isolated service branches.

The creation of theatre commands under CDS supervision aims to optimize resource allocation and ensure coordinated action during hybrid confrontations, such as cross-border terrorism supported by cyber intrusions and disinformation campaigns. The CDS also facilitates tri-service training modules, enhancing operational compatibility in hybrid environments.

4.2 Strategic Oversight of Information and Cyber Operations

Given the increasing reliance on cyber warfare, misinformation and psychological operationsby adversaries, the CDS now shoulders the responsibility of overseeing India's military cyber strategy. This includes:

- Coordinating with the Defence Cyber Agency (DCA)to secure military communication grids.
- Overseeing counter-disinformation operations through collaboration with the Ministry of Information & Broadcastingand external affairs cyber desks.
- Establishing protocols for rapid detection and attribution of cyber attacksto deter future intrusions.

The CDS also engages with civilian cyber infrastructure and private tech firms to ensure that national defence is not compromised due to siloed operations, especially in the case of dual-use technologies and infrastructure.

4.3 Decision-Making in Grey Zone Conflicts

Hybrid warfare thrives in the grey zonebetween peace and open war. The CDS bridges the civil-military divideby participating in National Security Council deliberations, advising the Cabinet Committee on Security and assisting in inter-ministerial task forcesdealing with cross-domain threats like cyber espionage, economic coercion and media manipulation.

In Operation Sindoor, the CDS played a central role in orchestrating multi-domain responses military strikes, cyber defences, media counter-narratives and diplomatic engagements. Importantly, the CDS helped frame the strategic messagingaround the operation, countering the misinformation campaigns that attempted to discredit India's actions.

4.4 Resource Optimization and Infrastructure Modernization

With hybrid threats demanding quick and multidimensional responses, the CDS is tasked with rationalizing procurement, eliminating redundancy and pushing for indigenous technologies. The CDS also:

- Aligns Make in Indiainitiatives with hybrid warfare needslike developing UAVs for surveillance and EW systems for jamming enemy communications.
- Promotes inter-service technological compatibilityso that Army systems can integrate with Air Force ISR platforms or Navy's maritime cyber-defence units.
- Monitors AI-based predictive threat analysis systems, ensuring technological superiority in preemption and decision support.

4.5 Civil-Military Synergy and Legal Frameworks

Hybrid warfare often targets the civilian ecosystempower grids, financial systems, social media, etc. The CDS, therefore, advocates for:

- Closer cooperation with DRDO, NTRO, CERT-In and other civilian research institutions.
- Legislative reformsfor offensive cyber capabilities and information warfare rules of engagement.
- Simulation-based scenario trainingwith civilian disaster and cybersecurity agencies to prepare for hybrid threats.

4.6 Doctrine Formulation and Strategic Communication

One of the most significant functions of the CDS in hybrid warfare is to lead doctrinal development. The CDS-driven Joint Doctrine for Hybrid Warfare is under consideration to provide an integrated roadmap for combating the spectrum of threats. It will include guidelines on hybrid escalation ladders, inter-agency responsibilities in the event of sub-conventional attacks and psychological warfare playbooks and narrative-building doctrines.

Strategic communicationboth for domestic morale and international legitimacyalso falls under the CDS's expanded role. Through coordination with MEA and Ministry of I&B, the CDS ensures that India's narrative is cohesive, timely and aligned across stakeholders, especially during crises like Operation Sindoor.

5. Disinformation as a Strategic Weapon: Lessons from the 15% Drain

Hybrid warfare in the 21st century has blurred the lines between conventional combat and cognitive conflict. Among its most insidious tools is disinformation, deliberately false or misleading information spread to deceive, manipulate or distract. In the context of Operation Sindoor, the recent revelation by the Chief of Defence Staff (CDS) that 15% of the total time, resources and effort were consumed in managing misinformation and disinformationunderscores the scale of the threat India faces in this cognitive domain.

5.1 Nature and Intent of Disinformation in Hybrid Conflicts

Unlike propaganda, which seeks to persuade or promote, disinformation is designed to confuse, delay, destabilize and delegitimize. It targets civilian moraleby spreading fear and uncertainty, military command and control structures by injecting false signals, diplomatic credibility by portraying the state as an aggressor or violator of norms and allied support structures by driving wedges between cooperating entities.

In hybrid warfare, these actions are often coordinated with kinetic operations, psychological operations and cyber intrusionsforming an integrated attack on the national security matrix.

5.2 The 15% Drain: Operational Implications

The CDS's statement that 15% of the operational effort during Operation Sindoor was diverted to counter misinformationreflects significant vulnerabilities. These losses were not purely logisticalthey manifested as:

- **Delayed decision-making**: Commanders had to pause operations to verify authenticity of viral media or intercepted signals.
- **Resource misallocation**: Intelligence assets were diverted to monitor information trends instead of battlefield surveillance.
- **Tactical confusion**: Disinformation about friendly troop movements or enemy positions caused temporary disarray.
- **Civilian panic and loss of strategic surprise**: Viral messages alleging mass escalation triggered unwarranted public anxiety, eroding operational secrecy.

These costs are not just measured in time but also in national will, tempo and trustall vital in a hybrid campaign where perception management equals battlefield success.

5.3 Disinformation Tactics Observed During Operation Sindoor.

Several foreign-backed and anonymous online campaignswere documented during the operation:

- Fake images of supposed civilian casualtieswere circulated to portray Indian strikes as indiscriminate.
- Bots and troll farms attempted to saturate social media with anti-India hashtags, coinciding with key tactical advances.
- False reports of mutiny, strikes or failed operations were released via seemingly legitimate channels to undermine soldier morale and civilian support.
- Deepfake videos and fabricated military communiqués sought to confuse command hierarchies.

These activities often originated from IP addresses outside India, using VPNs and AI-generated identities, pointing to the transnational and technologically advanced nature of modern disinformation.

5.4 Psychological and Strategic Impacts

The psychological fatigueinduced by constant exposure to disinformation can be as debilitating as physical attrition:

- Commanders suffer from cognitive overload, spending valuable bandwidth filtering truth from deception.
- Soldiers doubt real-time intelligence, hampering operational cohesion.
- Media outlets and influencers unintentionally amplify adversarial narratives, especially in the absence of timely government counters.
- International opinion is manipulated, framing India's defensive actions as escalatory.

Strategically, this erodes India's ability to shape the narrative, maintain deterrence and project legitimacyall central to hybrid victory.

5.5 Institutional Gaps in Countering Disinformation

India currently lacks a centralized, real-time, tri-service counter-disinformation unit. While the Ministry of Information & Broadcasting and cyber agencies like CERT-In perform monitoring roles, there is no integrated command-level fusion celltasked with early detection and attribution, strategic narrative coordination and rapid public and diplomatic rebuttals.

This decentralization leads to siloed responses, allowing disinformation to outpace truth. The 15% operational cost is both a symptom and a warning.

5.6 Lessons and Strategic Shifts

The key takeaways from Operation Sindoor regarding disinformation are misinformation is not collateral; it is core to enemy strategy, countering it demands pre-deployment planning, not post-event scrambling and information dominancemust be treated on par with air, land, sea and cyber superiority.

India must shift from a reactive postureto a pre-emptive information warfare strategy. This includesInformation Warfare Units (IWUs)under theatre commands, AI-based narrative monitoring tools, coordinated by the CDS and a robust Strategic Communication Doctrine, with roles defined for MEA, MOD, media outlets and social media platforms.

The 15% drain on Operation Sindooris not merely a statistic; it is a strategic red flag signalling that information supremacy will decide future wars.

6. The "Make in India" Defence Push: A Strategic Lever Post-Sindoor

Operation Sindoor not only showcased India's capacity for joint-force, hybrid warfare response but also elevated the strategic salience of the *Make in India* initiative in the defence sector. As the Indian military demonstrated its indigenous technological and doctrinal prowess during the operation, the world took noticenot merely of India's military resolve but also of the competitiveness of Indian-designed and manufactured defence platforms. The post-Sindoor environment presents a unique opportunity for India to transform its defence industrial base into a global strategic lever.

6.1 Evolution of "Make in India" in Defence

Launched in 2014, the *Make in India* initiative sought to reverse India's status as one of the world's largest arms importers. The defence sector was opened to 74% FDI under the automatic route and defence public sector undertakings (DPSUs) were restructured. Major reforms followed:

- Creation of the Defence Acquisition Procedure (DAP) 2020, emphasizing indigenous procurement.
- Prioritization of categories like *Buy Indian–Indigenously Designed Developed and Manufactured (IDDM)*.
- Publication of positive indigenization lists, banning imports of hundreds of items over staggered timelines.
- Encouragement of startups, MSMEs and DRDO partnerships in defence R&D.

These reforms were instrumental in laying the groundwork for a scalable, resilient and competitive defence production ecosystem.

6.2 Operation Sindoor: A Showcase of Indigenous Capability

Operation Sindoor marked a turning point in demonstrating the maturity of India's domestic defence production ecosystem. Key indigenous platforms that gained battlefield validation include:

- LCA Tejas (Light Combat Aircraft) - Deployed in both reconnaissance and air dominance roles, showcasing high maneuverability and low radar signature.
- Pinaka Multi-Barrel Rocket Launcher - Used for precision artillery strikes with remarkable impact on enemy logistical hubs.
- Swathi Weapon Locating Radar - Successfully tracked hostile fire in real-time, aiding responsive artillery engagements.
- Rudram Anti-Radiation Missiles - Deployed against enemy communication and radar systems, exhibiting electronic suppression capabilities.
- DRDO's Artificial Intelligence Platforms - Used in electronic surveillance, cyber intrusion mapping and disinformation monitoring.

By relying on homegrown systems during a high-intensity operation, India not only reduced foreign dependence but also signalled confidence in its own industrial and scientific base.

6.3 Rise in Global Demand Post-Sindoor

The international responseto India's battlefield performance included increased interest from strategic partners and developing nations in Indian-made platforms. Key developments include:

- Southeast Asian nations, particularly Vietnam and the Philippines, exploring procurement of BrahMos missilesand Indian-made patrol vessels.
- African Union peacekeeping forces showing interest in light-armoured vehicles and unmanned surveillance drones produced by Indian firms like Bharat Forge and IdeaForge.
- West Asian nations, notably the UAE and Saudi Arabia, expressing interest in combat-tested UAVs and battlefield management systems.
- Latin American countries, intrigued by low-cost, rugged Indian defence solutions suitable for jungle and urban warfare.

India's performance during Sindoor has thus converted credibility into commercial viability.

6.4 Strategic Implications for India's Defence Diplomacy

The export of indigenous weapon systems is not merely a commercial venture but a strategic tool of diplomacy. Through defence exportsIndia builds interoperabilitywith partner nations, especially in the Indo-Pacific, It diplomatically counters Chinese arms salesin Africa and South Asia, It reinforces its identity as a net security providerin the Indian Ocean Region (IOR) and It generates dual-use industrial capacitythat can pivot to civilian R&D.

Defence exports post-Sindoor can hence be seen as a new vector of strategic influence projection.

6.5 Challenges to Scaling Indigenous Defence Production

Despite the momentum, significant challenges remain:

- Bureaucratic complexitystill slows down procurement and licensing processes.
- Lack of testing infrastructureand long gestation periods for prototype validation.
- Weak integration between startups and armed forces, despite Innovations for Defence Excellence (iDEX) efforts.
- Limited global brand recognitionand after-sales service networks for Indian OEMs.

These gaps, if not addressed, can blunt the momentum gained during Operation Sindoor.

6.6 Recommendations for Strategic Expansion

To capitalize on this inflection point, India must:

- Establish a CDS-led Defence Export Promotion Cell, integrating military, MEA and industry stakeholders.
- Create combat validation certificates for Indian systems used in operations like Sindoor to boost credibility.
- Simplify export procedures for friendly countries under strategic agreements (e.g., SAGAR, IOR initiatives).
- Invest in Indian Defence Attachés with technical portfolios in embassies for effective promotion.
- Encourage joint production lines abroad, especially in ASEAN and Africa for logistics support and political alignment.

1. Export Forecast Table: Indian Defence Exports Post-Operation Sindoor

Year	Category	Projected Export Value (INR Cr)	Target Countries	Key Products
2025	Small Arms & Ammunition	1,800	Vietnam, Philippines, Kenya	INSAS, AK-203, Ammunition packs
2026	UAVs & Surveillance Drones	2,500	Armenia, Egypt, Sri Lanka	SWiFT UCAV, Rustom II, Netra V2
2027	Artillery Systems	3,600	Brazil, Indonesia, UAE	Dhanush, ATAGS
2028	Naval Equipment	5,000	Mauritius, Maldives, Oman	OPVs, Interceptor Boats, Sonar Systems
2029	Integrated AI-based Systems	6,500	France (co-production), African Union Members	AI Battle Mgmt Systems, Loitering Munitions

Note: Based on post-Sindoor strategic diplomacy and DRDO/Make-in-India growth trajectories.

2. Battlefield Equipment Mapping: Indian Hybrid Warfare Capabilities

Domain	Key Equipment / Capability	Indigenous Source	Operational Role
Cyber Warfare	Offensive Cyber Cells, Defence Grid	CERT-IN, DRDO	Disable adversary infrastructure, secure C2
Electronic Warfare	Samyukta EW System, Himshakti	BEL, DRDO	Signal jamming, interception
UAV/Drone Ops	Rustom-II, Netra V2, SWiFT	HAL, ADE	Reconnaissance, surveillance, strike support
Information Ops	Digital Propaganda Cells,	PIB, Indian Army	Counter-misinformation,

	Fact-check Units	PR Units	narrative control
Conventional Strike	BrahMos, Pinaka, T-90	BDL, OFB, HAL	Surgical hybrid strikes in multi-domain ops

7. Challenges in Institutionalising Hybrid Warfare Preparedness

Despite India's growing awareness and initial structural reforms to confront hybrid warfare, institutionalising a comprehensive and sustainable hybrid warfare doctrine remains fraught with challenges. These obstacles are both structural and strategic, ranging from legacy systems and inter-service rivalry to policy ambiguities and civil-military coordination deficits.

7.1. Absence of a Unified Hybrid Warfare Doctrine

One of the most pressing challenges is the lack of a singular, well-articulated national doctrine on hybrid warfare. Although individual services, such as the Indian Army and Indian Air Force, have evolved their own hybrid postures, these remain compartmentalised efforts. The absence of a joint doctrine results in fragmented responses and inhibits coordinated multi-domain operations during crises like Operation Sindoor. Without doctrinal convergence, operational synergy between cyber, psychological, kinetic and informational elements remains ad hoc and improvisational.

7.2. Institutional Silos and Inter-Service Rivalry

Hybrid warfare demands seamless inter-agency and inter-service collaboration, yet India's security establishment is marred by deep-rooted silos. The Army, Navy, Air Force and intelligence agencies often operate with limited interoperability and communication. This is particularly detrimental during hybrid threats that unfold across multiple domains simultaneously cyber, media, economic and kinetic. Efforts by the Chief of Defence Staff (CDS) to foster jointnesshave faced resistance from traditional command structures.

7.3. Inadequate Integration of Civilian and Military Efforts

Hybrid warfare is as much about civil resilience and narrative control as it is about military might. However, India's civil-military integration remains weak. Ministries handling information, communications, cyber security and economic policy often lack established frameworks for working with the armed forces during hybrid contingencies. This leads to disjointed public messaging and slows down counter-disinformation campaigns, such as those experienced during Operation Sindoor.

7.4. Gaps in Cyber and Information Warfare Capabilities

India has made significant strides in cyber defence, but its offensive cyber capabilities and narrative warfare competencies remain underdeveloped. While agencies like CERT-IN and the Defence Cyber Agency exist, they are hampered by manpower shortages, insufficient funding and unclear legal mandates for cross-border cyber operations. The lack of robust legal and operational frameworksto guide counter-disinformation, psychological operations and narrative warfare diminishes India's preparedness in the hybrid space.

7.5. Training and Human Capital Constraints

The current military education system is primarily geared toward conventional warfare and counterinsurgency operations. There is insufficient focus on hybrid warfare education and cross-domain expertise, especially in areas such as media manipulation, legal warfare, cognitive warfare and economic disruption. Personnel trained in hybrid domains are often underutilised or rotated out before institutional memory can be retained.

7.6. Intelligence Gaps and Data Fusion Deficits

Hybrid threats require real-time, multi-source intelligence fusionacross domestic, foreign, cyber and open-source intelligence. India's current intelligence architecture, while formidable, suffers from coordination issues between RAW, IB and military intelligence. The absence of a National Information

Fusion Centrefocused on hybrid threats leads to delayed threat assessments and suboptimal response planning.

7.7. Legal and Policy Ambiguities

Hybrid warfare operates in legal grey zones. India's existing legal frameworkssuch as the Information Technology Act, Official Secrets Act and Defence Services Regulationsdo not adequately cover the nuances of hybrid threats such as cyber retaliation, psychological operations abroad or engagement with non-state actors. This creates both strategic hesitation and operational paralysis in critical moments.

7.8. Resource Allocation and Bureaucratic Delays

Resources for hybrid warfare preparednessespecially in domains like cyber, space and psychological opsremain inadequate. Budget allocations to niche warfare capabilities are often sidelined in favour of conventional acquisitions. Bureaucratic delays in procurement, talent hiring and indigenous R&D further slow down India's hybrid readiness, even as adversaries rapidly expand their own capabilities.

8. Recommendations and Future Outlook

8.1. Institutionalisation of Hybrid Warfare Doctrine

To effectively counter hybrid threats, India must formalise a dedicated *National Hybrid Warfare Doctrine*. This doctrine should be jointly framed by the Ministry of Defence, Ministry of Home Affairs, National Security Council Secretariat (NSCS) and the three armed services. The Chief of Defence Staff (CDS) should lead the doctrinal development and ensure its integration across the Indian Armed Forces. The doctrine must go beyond kinetic responses, encompassing cyber defence, psychological warfare, information control, legal warfare and economic countermeasures. A well-structured doctrine would reduce ad-hocism and enable proactive, rather than reactive, responses to hybrid threats.

8.2. Establishment of a Dedicated Hybrid Warfare Command

One of the most pressing structural reforms should be the establishment of a *Hybrid Warfare Command*, functioning under the CDS. This integrated tri-service command should bring together cyber warfare units, information operations specialists, space assets and psychological operations teams. The command should also coordinate with intelligence agencies (RAW, IB, NTRO) and civilian cyber infrastructure to ensure a seamless interface between military and non-military capabilities. Drawing inspiration from structures like U.S. Cyber Command or NATO StratCom, such a command would institutionalise hybrid capability across domains.

8.3. Strategic Communication Infrastructure

In view of the recent revelation by the CDS that 15% of resources during Operation Sindoor were lost due to misinformation, the establishment of a National Strategic Communications Cell under the CDS becomes crucial. This body should work on real-time monitoring of disinformation campaigns, develop counter-narratives and collaborate with tech platforms and media regulators. Artificial intelligence-powered tools for threat analysis, sentiment mapping and fake news detection should be deployed at scale. Coordination with civilian ministries (Information & Broadcasting, External Affairs etc) will be essential to ensure coherence in India's internal and external messaging.

8.4. Boosting Defence Production and Export under 'Make in India'

Post-Operation Sindoor, there has been heightened global interest in Indian-made systems such as drones, jammers, electronic warfare tools and precision-guided munitions. The CDS should play a pivotal role in aligning operational needs with defence production and export goals. A forward-looking recommendation would be to create a CDS-led Defence Export Facilitation Cell, in coordination with the Department of Defence Production. It should streamline export clearance, promote Indian platforms in foreign defence expos and establish military-industrial partnerships with Global South nations seeking affordable, hybrid-warfare-ready systems.

8.5. Cyber Security and AI Integration

As cyber threats increasingly form the backbone of hybrid warfare, India needs a robust Cyber Defence Strategy. The CDS must ensure that offensive cyber capabilities are developed in tandem with defensive resilience. AI and ML (Machine Learning) tools must be integrated across surveillance, predictive threat modelling, decision-making and battlefield communication. This will require collaboration with DRDO, private-sector startups and academic institutions. Furthermore, training modules at National Defence College and other military institutions should incorporate advanced AI-augmented warfare simulations.

8.6. Enhancing Interagency and Civil-Military Fusion

Hybrid warfare demands whole-of-nation coordination. The CDS should be empowered to convene a Hybrid Threat Coordination Council that includes civilian agencies (MEA, MHA, MoIB), private-sector cybersecurity firms, think tanks and state governments. Such a body should convene periodically to review threat assessments, simulate coordinated responses and conduct national-level drills. The CDS must also work towards institutionalising civil-military fusion cells in critical sectors such as communications, energy, banking and transportation to ensure wartime resilience and redundancy.

8.7. Strategic Military Education and Research

India's military institutions must revamp their curricula to include hybrid conflict studies, strategic communication, disinformation analysis and lawfare. The CDS should oversee the creation of a Hybrid Warfare Studies Institutea centre of excellence that conducts research, wargaming and strategic foresight. Scholars, former diplomats, military officers and cyber experts should form the core faculty. Such an institute would feed doctrine, policy and capability development with deep analytical insights.

8.8. Legal Framework for Hybrid Threat Response

The ambiguity of hybrid warfare demands a recalibrated legal strategy. There is currently no defined legal framework for attribution, proportional response or escalation management in hybrid attacks. The CDS, working in tandem with the Ministry of Law and Justice, should push for legislation that allows the government to define hybrid aggression, set escalation thresholds and invoke state powers for countermeasures. International advocacy in multilateral platforms (UN, SCO, QUAD) should also be pursued to legitimise such doctrines globally.

8.9. Proactive Role in Indo-Pacific Security Architecture

As India gains economic and strategic weight, the CDS should shape India's doctrinal contribution to regional hybrid conflict frameworks. India must push for joint cyber drills, counter-disinformation operations and intelligence fusion centres within QUAD, ASEAN Defence Ministers' Meeting Plus (ADMM+) and other strategic partnerships. India's hybrid warfare experience, especially after Operation Sindoor, gives it unique insights to lead global discourse.

Conclusion

Operation Sindoor has underscored that hybrid warfare is the defining strategic challenge of our time. Operation Sindoor has become a case study in the power and peril of hybrid warfare. The recognition by the CDS that 15% of India's operational capability was lost to disinformationmust serve as a strategic wake-up call. The CDS, as the apex military advisor and integrator, must be empowered with doctrinal, operational and structural tools to institutionalise India's hybrid response. From crafting a national doctrine and establishing dedicated commands to shaping export policy and leading international cooperation, the role of CDS must evolve to match the complexity of future conflict. India's rise as a regional power depends not only on its military strength, but on its ability to smartly blend hard and soft power, deterrence and perception and kinetic and non-kinetic meansall under a cohesive hybrid warfare framework.

Footnotes

1. Press briefing by Chief of Defence Staff, New Delhi, June 2025. Ministry of Defence Archives.
2. Giles, Keir. *Russia's Hybrid Warfare Strategy*. NATO Defence College Research Paper, 2016.
3. Singer, P.W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.
4. Mulvenon, James. *China's "Three Warfares": The New Battlefield of Information*. RAND Corporation, 2015.
5. Report from India Today, "Fake Chemical Attack Videos Go Viral During Operation Sindoor," April 2025.
6. Ministry of Defence. "Post-Sindoor Defence Export Inquiries See 200% Surge." Government of India Press Release, May 2025.
7. Ministry of External Affairs, "Media Counter-Briefings Issued During Operation Sindoor," April 2025, archived at mea.gov.in.
8. Parliamentary Standing Committee on Defence, "Post-Operation Sindoor Review," July 2025.