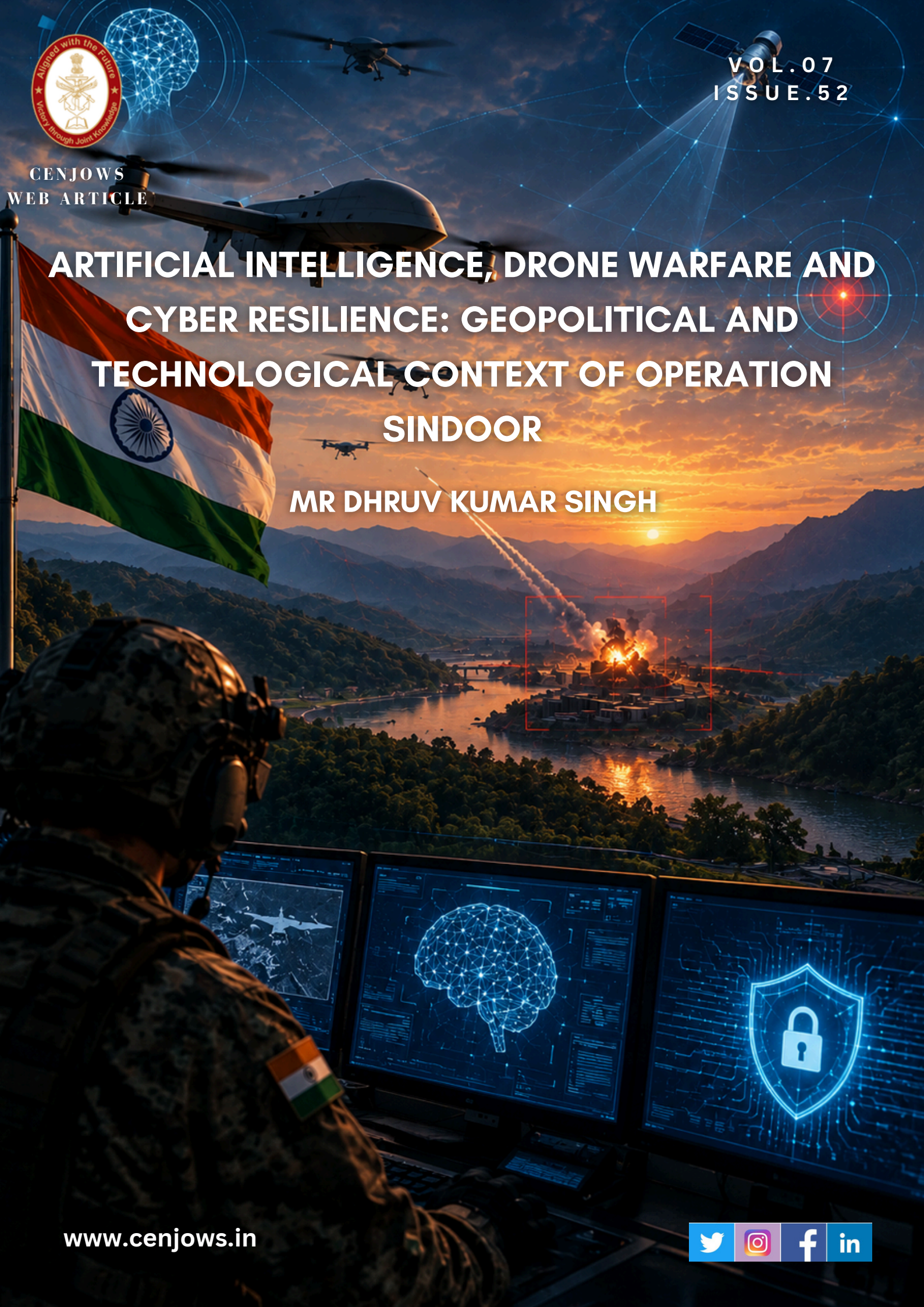
VOL.07
ISSUE.52

CENJOWS
WEB ARTICLE

ARTIFICIAL INTELLIGENCE, DRONE WARFARE AND CYBER RESILIENCE: GEOPOLITICAL AND TECHNOLOGICAL CONTEXT OF OPERATION SINDOOR

MR DHRUV KUMAR SINGH



www.cenjows.in

CENJOWS WEB ARTICLE

Volume 07 Issue 52 SEP 2026

CENJOWS

(Established: 2007)

Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan,
CGO Complex, Lodhi Road
New Delhi –110003 (INDIA)
Telephone Nos: 011-24364881, 24366485
Fax: 011-24366484
Website: www.cenjows.in
E-mail: cenjows@cenjows.in

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Starting Year : 2020

Year of Publication : 2026

Frequency : Weekly

Language : English

Publisher : Maj Gen (Dr) Ashok Kumar, VSM (Retd) Director General, CENJOWS
301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003

Editor : Maj Gen (Dr) Ashok Kumar, VSM (Retd) (dg@cenjows.in)

Deputy Editor : Dr Ulupi Borah, Distinguished Fellow (distinguishedfellow1@cenjows.in)

Editorial Board :

Brig K Ranjeev Singh, VSM (ddg@cenjows.in)

Col Ajay Kumar Rajak, SM (secy@cenjows.in)

Gp Capt Ashish Kumar Gupta (Retd) (seniorfellow2@cenjows.in)

Dr Ulupi Borah, Distinguished Fellow (distinguishedfellow1@cenjows.in)

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Dr Monojit Das, Senior Fellow, PRO (monojit.das@cenjows.in)

Publication Head : Ms Vaibhavi Katal

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS) 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484 e-mails: cenjows@cenjows.in / cenjows@yahoo.com Website: http://cenjows.in

Price: Rs 150/- INR

ARTIFICIAL INTELLIGENCE, DRONE WARFARE AND CYBER RESILIENCE: GEOPOLITICAL AND TECHNOLOGICAL CONTEXT OF OPERATION SINDOOR

CONTENTS

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Artificial Intelligence, Drone Warfare and Cyber Resilience: Geopolitical and Technological Context of Operation Sindoor

Mr Dhruv Kumar Singh is a PG Student at Rashtriya Raksha University

Abstract

Operation Sindoor, which was India's May 2025 tri-service response to the Pahalgam terror attack. And also offered a rare public window into how artificial intelligence, unmanned systems, and cyber resilience are converging within Indian military doctrine. This article situates the operation within that wider convergence: it examines what is publicly verifiable about Sindoor's intelligence-led, precision-oriented execution; surveys how AI, drone systems such as the indigenous DRDO D4 platform, and cyber-resilience institutions like CERT-In and the Defence Cyber Agency are being folded into Indian defence planning, and traces the doctrinal follow-through visible in PRAHAAR, the Ministry of Home Affairs' February 2026 National Counter-Terrorism Policy. Drawing on classical strategic thought alongside contemporary defence and technology literature, the article argues that India's post-Sindoor operational reality is defined less by any single new capability than by the attempted fusion of jointness, technological modernisation,

and codified doctrine into a coherent whole-of-government posture—a fusion whose depth remains difficult to verify from open-source material alone.

Keywords: Operation Sindoor, artificial intelligence, drone warfare, cyber resilience, PRAHAAR, jointness, hybrid warfare, India-Pakistan, counter-terrorism doctrine.

Operation Sindoor was conducted by the Indian Armed Forces in May 2025 in response to a terrorist attack at Pahalgam, in the Union Territory of Jammu and Kashmir. According to statements issued by the Government of India through the Press Information Bureau, the operation involved precision strikes on identified terrorist infrastructure and was executed as a coordinated tri-service effort involving the Indian Army, Navy and Air Force under a unified operational framework. The government has characterised this operation as intelligence-led, aimed at degrading terrorist capabilities operating across the border region.[1]

What is publicly confirmed at a factual level remains limited, though significant in scope: the operation's timing, its counter-terrorism objective, its precision-strike orientation, and its tri-service coordinated execution. Operational specifics such as platforms employed, technologies used, and tactical procedures remain classified or undisclosed in official public sources.[2] Subsequent statements by senior officers involved in the operation have, however, confirmed that artificial intelligence tools were used for multi-sensor data fusion and real-time intelligence processing, including an Electronic Intelligence Collation and Analysis System used to identify and prioritise threats.[3]

Geopolitical Context: South Asia and Beyond

The India-Pakistan relationship continues to be defined by long-standing strategic competition, recurring cycles of tension, and the persistent role of cross-border terrorism within this dynamic.

India's strategic environment is also shaped by broader geopolitical competition with China, extending into domains such as artificial intelligence, unmanned systems, cyber capabilities and electronic warfare. Contemporary defence policy discourse in India reflects a growing emphasis on jointness, technological modernisation and self-reliance.[4]

Globally, artificial intelligence is being incorporated into intelligence analysis and decision-support systems across multiple militaries. Unmanned aerial systems are now widely deployed across conflict theatres for surveillance and reconnaissance, and cyber operations have become a persistent feature of both peacetime and conflict environments.

Operation Sindoor and the Evolution of Joint Operations

Official statements confirm that the operation was conducted as a coordinated tri-service effort, with emphasis placed on precision targeting and intelligence integration.[5] This is consistent with the broader trajectory of India's military modernisation, which increasingly emphasises jointness and integrated command structures, reflected in the ongoing rollout of Integrated Theatre Commands under the Chief of Defence Staff.[6] [7]

The characterisation of the operation as intelligence-led is consistent with global military trends, in which modern operations rely on fused intelligence inputs drawn from multiple sources to enable improved situational awareness and faster decision-making cycles.[8]

Technological Transformation in Modern Warfare

Contemporary warfare is increasingly shaped by the convergence of artificial intelligence, unmanned systems, and cyber capabilities. These developments are observable across multiple conflict environments and are well documented in defence and security literature.[9] [10]

Artificial intelligence is increasingly used in defence contexts for intelligence analysis, surveillance data processing, decision support, and logistics optimisation.[11] In the Indian case, this is reflected in the work of DRDO's Centre for Artificial Intelligence and Robotics, which has developed more than seventy-five AI-enabled defence products spanning autonomous platforms, cyber defence and surveillance systems.[12]

Unmanned aerial systems have become widely adopted across modern militaries for reconnaissance, surveillance, and limited strike roles. Their utility derives from operational flexibility, scalability and reduced risk to personnel, while their effectiveness

remains dependent on digital connectivity, satellite navigation, and secure communication links.[13]

Cyber operations have emerged as a persistent domain of conflict that operates continuously across both peacetime and wartime conditions. Unlike kinetic operations, cyber activity can target communication networks, command systems, and critical infrastructure without physical presence in the battlespace.[14] [15] In India, the scale of this domain is illustrated by CERT-In's record of having handled over 2.9 million cyber incidents in 2025 alone, across sectors including defence, telecommunications and finance.[16]

Cyber Dependency and Systemic Vulnerability

Communication systems, satellite navigation networks, command-and-control architectures, and data-driven decision systems collectively form the backbone of contemporary military operations.[17] [18]

Dependence on satellite navigation creates susceptibility to signal disruption or spoofing. Reliance on communication networks introduces risks of interference or degradation. Increasing dependence on data-driven systems raises concerns regarding data integrity, system reliability, and adversarial manipulation.[19] [20]

Strategic Continuity in Classical Thought

In the Arthashastra, Kautilya emphasises intelligence gathering and information superiority as central to state security.[21] Sun Tzu, in The Art of War, highlights the importance of knowledge, deception and strategic foresight as decisive factors in warfare prior to physical engagement.[22] Machiavelli, in The Prince, underscores the necessity of adaptability in response to changing political and strategic conditions.[23]

Drone Warfare: System Architecture and Operational Dependence

Unmanned aerial systems (UAS) have become a defining feature of contemporary military operations across multiple theatres, including counter-terrorism, border

surveillance and conventional conflict environments. Their operational value lies in persistence, reduced risk to personnel and cost efficiency relative to manned platforms.[24]

Drones function as networked architectures dependent on multiple integrated subsystems, including satellite navigation, communication links, ground control stations and data-processing infrastructure. Artificial intelligence is increasingly embedded within these systems for object recognition, navigation assistance and mission optimisation.[25] [26]

India's own indigenous counter-drone platform, the DRDO-developed D4 (Detect, Deter, Destroy) system, illustrates this convergence directly: it combines radar, radio-frequency and electro-optical sensors with AI-based threat classification and integrates both jamming-based soft-kill and laser-based hard-kill mechanisms within a single architecture.[27]

Dependency on satellite navigation introduces susceptibility to spoofing and jamming; reliance on communication links introduces risks of signal degradation or interception; and software-defined architectures create exposure to cyber intrusion and firmware exploitation.[28] Independent reporting has indicated that the D4 system was used operationally to neutralise drone incursions during Operation Sindoor, underscoring how directly these subsystem dependencies translate into battlefield outcomes.[29]

Drone warfare therefore represents not merely a platform evolution but a broader shift toward cyber-physical interdependence in warfare systems.

Cyber Resilience as an Operational Requirement

Cyber resilience refers to the capacity of systems to maintain operational functionality under attack, recover from disruption and adapt to evolving threat environments. In military contexts, this encompasses command-and-control networks, communication infrastructure, navigation systems and intelligence-processing frameworks.[30] In India, this function is institutionally anchored in the Indian Computer Emergency Response Team (CERT-In), operating under the Ministry of Electronics and Information Technology, alongside the Defence Cyber Agency under the Ministry of Defence.[31] [32]

Digitisation has increased efficiency while simultaneously expanding exposure. Communication systems can be disrupted, data integrity can be compromised, and navigation systems can be degraded through electronic interference.[33] [34]

Artificial Intelligence: Integration and Systemic Constraints

Militaries are folding artificial intelligence into an increasingly wide range of functions — sifting intelligence, interpreting surveillance feeds, optimising logistics, and supporting the judgement calls that precede a decision to act.[35]

That integration does not come free of cost. AI systems fail in ways that older, non-adaptive systems generally do not: an adversary can feed them deliberately misleading inputs, poison the data they are trained on, or probe a model closely enough to reverse-engineer what it has learned, and in each case the system's dependence on the integrity of its training data becomes a point of failure rather than a source of strength. India has begun to address this institutionally rather than leaving it to individual programme offices through the Evaluating Trustworthy Artificial Intelligence (ETAI) framework that the Chief of Defence Staff and the DRDO Chairman jointly launched in October 2024 to assess AI systems before they are inducted into the armed forces.

Most of the defence literature surveyed for this article treats AI as a tool that augments human judgement rather than one that substitutes for it in high-risk operational settings, and that framing leads to augmentation rather than autonomy. Which is worth holding onto as India's own AI-enabled systems move from testing toward deployment.

Comparative Doctrine: Integrated Warfare and the Israeli Model

A frequently referenced contemporary model of integrated warfare is the Israeli operational approach, characterised by close coordination between intelligence, cyber operations, electronic warfare, and kinetic capabilities.[36]

This model is defined by compressed intelligence-to-strike cycles, in which information from multiple sensors and intelligence streams is rapidly processed and translated into

operational action, and reflects a convergence between cyber and electronic warfare functions.[37]

Economic and Industrial Foundations of Military Technology

Modern military capability is increasingly dependent on industrial ecosystems rather than isolated defence production capacity. Critical dependencies include semiconductors, communication hardware, AI computing infrastructure and precision electronics manufacturing.[38] India currently imports the substantial majority of its semiconductor requirements, with import costs having grown at approximately 23 per cent annually to reach roughly USD 30.3 billion in FY25.[39]

Disruptions in supply chains, or restrictions on access to advanced technologies, can directly affect operational readiness in unmanned systems, AI-enabled platforms and secure communication networks.[40]

Hybrid Warfare and Geopolitical Spillovers

Cyber operations now function as persistent instruments of statecraft, targeting both military and civilian infrastructure. Information operations similarly shape perception, narrative framing and strategic signalling in real time.[41] [42]

This hybridity is precisely what makes contemporary conflict harder to bound than earlier, more clearly demarcated wars. A cyber intrusion against a power grid, a coordinated disinformation campaign timed to a border skirmish, and the covert financing of a proxy group are not separate problems handled by separate ministries; in practice they arrive bundled, often deliberately, so that there is no single response. As in, diplomatic, military, or legal addresses the whole picture of the threat. For India, this bundling has a specific regional shape. The Pakistan-China relationship extends beyond conventional military cooperation into shared or parallel interests in cyber capability-building and information operations directed at Indian audiences, while domestically, encrypted communications, dark-web financing channels, and decentralised radicalisation networks have made older, centralised counter-terrorism models progressively less effective on their own.

Indian policy has begun to name this problem explicitly rather than treat it as an implicit backdrop. Post-Sindoor counter-terrorism doctrine explicitly refers to hybrid threats such as drones, cyberattacks, dark-web financing, information warfare and radicalisation. As a single, interconnected category requiring a single, coordinated institutional response rather than piecemeal handling by separate agencies.[43]

The spillover effects are not confined to the subcontinent. Disinformation and cyber activity linked to South Asian tensions have periodically surfaced in international monitoring of foreign information manipulation, illustrating how a regionally rooted conflict can generate effects that travel well beyond the immediate parties and complicate the diplomatic and narrative environment in which any future crisis has to be managed.

India's Emerging Operational Reality

Operation Sindoor, as officially described by the Government of India, reflects an institutional shift toward intelligence-led, precision-oriented and jointly executed operations under a unified framework.[44] [45] Operational specifics remain undisclosed.

The clearest evidence that this shift is doctrinal, and not just tactical, arrived roughly nine months after the operation itself. On 23 February 2026, the Ministry of Home Affairs unveiled PRAHAAR, India's first comprehensive national counter-terrorism policy and strategy. To be exact, it’s a framework that, unlike earlier ad hoc arrangements built up through legislation, executive practice, and informal inter-agency coordination, sets out a single codified doctrine spanning prevention, response, capacity aggregation, human-rights compliance, and the attenuation of the conditions that enable radicalisation in the first place.

PRAHAAR's most consequential institutional feature, for the purposes of this article, is its intelligence-led preventive model: the operationalisation of the Multi Agency Centre (MAC) and a new Joint Task Force on Intelligence (JTFI) is intended to strengthen real-time intelligence sharing between central and state agencies, shifting the operating posture from post-incident response toward pre-emptive disruption of plots before they mature.[46]

Analysts have read the doctrine as a deliberate consolidation of India's post-Sindoor "zero tolerance" posture, formalising the principle that a future terrorist attack traced to external sponsorship will be treated as an act of war rather than as an internal-security incident to be managed through diplomatic protest alone. Although critics of this reading note that PRAHAAR itself stops short of specifying clear thresholds for cross-border retaliation, leaving the exact trigger for escalation deliberately ambiguous.[47]

That ambiguity is arguably a feature rather than an oversight: commentary on the doctrine frames it as pursuing cumulative deterrence against a Pakistan-backed nexus of organised crime, terrorism and sleeper-cell infrastructure, rather than attempting to deter any single attack through a fixed, publicly known response threshold.[48]

AI-assisted intelligence fusion, indigenous counter-drone systems, and a hardening cyber-resilience architecture are mentioned in PRAHAAR, which suggests that India's operational reality after Sindoor is not simply "more of the same, done faster". It is a genuine attempt to fuse doctrine, technology and institutional reform into a single, whole-of-government posture, even if, as of this writing, the depth of that fusion in practice remains difficult to verify from open-source material alone.

Multi-Domain Integration and the Challenge of Jointness

India's movement toward integrated theatre commands reflect a recognition that future conflicts will not be confined to a single domain. Land, air, maritime, cyber, space, and information environments are increasingly interconnected in both planning and execution.[49] [50] As of mid-2026, the Chief of Defence Staff has reported that approximately ninety per cent of the groundwork for the Integrated Theatre Command framework has been completed, with the proposal forwarded to the Ministry of Defence for further approval.[51]

Global military experience indicates that the success of joint operations depends not only on organisational restructuring but also on the depth of data integration and real-time information-sharing between services.[52] [53]

Cyber Resilience as National Security Infrastructure

For India, this includes the protection of military communication networks, satellite navigation systems, defence logistics platforms, intelligence databases, and critical civilian infrastructure linked to defence readiness.[54] CERT-In's operational data illustrates the scale of this task: in 2025 the agency issued 1,530 security alerts and 390 vulnerability notes and conducted 122 cybersecurity drills involving participants from the defence, paramilitary, space and atomic energy sectors.[55]

Drone Warfare and India's Operational Environment

Drone systems are increasingly accessible, commercially available and adaptable for both surveillance and offensive roles, creating a security environment in which non-state actors may also acquire limited unmanned capabilities.[56] India's response has included the operational deployment of the D4 counter-drone system across all three services, developed with indigenous content reported at close to eighty per cent and involving more than fifty domestic industry partners and MSMEs.[57]

Artificial Intelligence and Decision-Making Structures

As AI moves deeper into military systems, it is not replacing the chain of command so much as reshaping the pace and texture of decisions made within it. Fusing intelligence streams, flagging likely threats, and pre-structuring options for a commander are all tasks AI-enabled systems now handle with growing competence, but the literature this article draws on is consistent in keeping the final judgement call with a human decision-maker rather than the system itself.

India has given this principle an institutional home in the Defence AI Council and the Defence AI Project Agency, both established in 2019 to coordinate how artificial intelligence is adopted across the three services, DRDO, the defence public-sector undertakings, and private industry.[58]

Strategic Autonomy and Supply Chain Security

The availability of semiconductors, secure communication hardware, AI compute infrastructure and sensor technologies directly affects operational readiness. India's push toward defence indigenisation and technological self-reliance reflects this understanding.[59] The India Semiconductor Mission, launched in December 2021 with an incentive outlay of approximately ₹76,000 crore, has approved ten fabrication and packaging projects as of December 2025, and a second phase of the mission announced in the Union Budget 2026-27 has extended this focus to equipment, materials and indigenous design intellectual property.[60] [61]

Information Warfare and the Expanded Battlespace

Modern conflicts increasingly extend into information ecosystems, where narratives, perception management and strategic communication play a significant role, encompassing media narratives, digital influence operations and real-time information dissemination across platforms.[62] [63]

Doctrinal Continuity and Strategic Thought

Kautilya's emphasis on intelligence and statecraft in the Arthashastra underscores the centrality of information to governance and security.[64] Sun Tzu's emphasis on knowledge and strategic advantage highlights the importance of positioning prior to conflict.[65] Machiavelli's focus on adaptability reinforces the necessity of institutional flexibility amid changing circumstances.[66]

Recommendations

These are forward-looking suggestions rather than documented findings and are not attributed to any source.

First, let's start with jointness and theatre command implementation, the momentum behind the Integrated Theatre Command framework that should be sustained beyond the groundwork stage. Which is a clear legal and administrative framework, the agreed timelines for the transfer of operational authority from service-specific commands, and an

expanded role for joint training institutions could help ensure that organisational reform translates into genuine operational integration rather than remaining a structure on paper alone.

Second is on cyber resilience and the institutional architecture already in place around institutions like CERT-In and the Defence Cyber Agency. That should be deepened specifically for military and defence-adjacent systems. This could also include expanding sector-specific incident response capacity for defence communication and navigation networks, conducting more frequent joint drills that simulate combined cyber and kinetic contingencies, and ensuring that smaller defence vendors and MSMEs in the supply chain are brought within the same audit and compliance standards applied to larger public sector undertakings. And boosting cyber resilience of the nation.

Third, artificial intelligence, as in the existing Evaluating Trustworthy Artificial Intelligence framework, should be extended with binding pre-induction testing requirements. Particularly for systems involved in surveillance interpretation and targeting support, and should be paired with sustained investment in indigenous data pipelines so that operational trust in AI-enabled systems does not become dependent on externally sourced models or datasets.

Fourth, on unmanned systems, the demonstrated success of indigenous counter-drone platforms should be used as a basis for accelerating the next generation of these systems, with particular attention to detection ranges, swarm-engagement capability, and integration with wider air-defence networks, while continuing to expand the domestic industrial base supporting their production.

Fifth, it is on institutionalising the counter-terrorism doctrine, PRAHAAR's Multi-Agency Centre and Joint Task Force on Intelligence structures should be resourced and staffed at a pace that matches the doctrine's ambition, with clear metrics for pre-emptive disruption rather than post-incident response, so that the shift from reactive to preventive counter-terrorism is measurable rather than declaratory.

Sixth, it will be on industrial and supply chain resilience; the semiconductor self-reliance agenda should be pursued with explicit defence-sector milestones, including a defined pathway for trusted, domestically fabricated components to be used in critical defence electronics, communication systems and AI compute infrastructure, so that strategic autonomy in this domain is measured not only by overall production capacity but by the share of defence-critical components sourced domestically.

Jointness without cyber resilience risks creating an integrated but fragile command structure. And AI adoption without supply chain security risks creating capability that cannot be sustained under disruption. And a counter-terrorism doctrine without resourced institutions risks remaining a statement of intent at large. The coherence of these efforts is likely to matter as much as progress on any single front.

Conclusion

Operation Sindoor, in the author's view, signifies more than a tactical response to a single incident. It appears to reflect a broader institutional shift in India's approach to military operations, one increasingly defined by intelligence integration, tri-service coordination and precision-based execution. The significance of this operation lies less in any disclosed tactical detail and more in what it suggests about the direction Indian military planning is taking. To be specific, a direction in the form of PRAHAAR, which has since given us the formal doctrinal name.

When read together, the trends discussed above point toward several broader conclusions. First, modern warfare appears to be defined less by individual platforms and increasingly by the integration of systems with one another; operational advantage seems to follow from interoperability and resilience rather than from any single capability. Second, cyber resilience appears to be moving from a supporting function toward a precondition for sustained military effectiveness, given how deeply digital infrastructure now underpins command, communication and intelligence functions. Third, technologies such as drones and artificial intelligence seem to be reshaping not the fact of human decision-making, but its tempo and complexity, by compressing the interval between information and action.

For India specifically, the central challenge appears to be systemic integration across services, domains and infrastructure, rather than technological adoption considered in isolation. The push toward jointness, indigenisation and digital integration, and now a codified counter-terrorism doctrine in PRAHAAR, suggest an institutional recognition of this challenge, though the depth of integration achieved in practice cannot be assessed from open-source material alone.

On balance, it is the author's assessment that the future effectiveness of Indian military power will depend substantially on the country's ability to sustain operational coherence within a contested, data-driven and multi-domain environment, and that this depends as much on institutional and organisational change as on the acquisition of new technology.

Declaration

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

ENDNOTES

---

[1] Government of India, Ministry of Defence, "Operation Sindoor: Indian Armed Forces Carried Out Precision Strike at Terrorist Camps," Press Information Bureau, May 7, 2025, https://www.pib.gov.in.

[2] ibid

[3] Cybernews, "India's Army Is Going Full AI: From Spy Drones to Smarter Battlefields," October 2025, citing Lt. Gen. Rajiv Kumar Sahni, former Director General of Information Systems, https://cybernews.com/ai-news/how-india-using-ai-advance-military/.

[4] Government of India, Ministry of Defence, official statements on defence modernization and jointness reforms, 2024–2025, https://www.mod.gov.in.

[5] Government of India, Ministry of Defence, "Operation Sindoor: Indian Armed Forces Carried Out Precision Strike at Terrorist Camps," Press Information Bureau, May 7, 2025, https://www.pib.gov.in.

[6] Government of India, Ministry of Defence, official statements on defence modernization and jointness reforms, 2024–2025, https://www.mod.gov.in.

[7] Ministry of Defence, "Armed Forces Shape Future Roadmap at Combined Commanders' Conference 2025," Press Information Bureau, Government of India, September 17, 2025, https://www.indiastrategic.in/artificial-intelligence-ai-in-indian-defence/.

[8] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[9] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[10] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[11] U.S. Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, DC, 2022), https://www.defense.gov.

[12] Observer Research Foundation, "AI in Modern Warfare: India's Strategic Challenges and Opportunities," February 2026, citing the Evaluating Trustworthy Artificial Intelligence (ETAI) Framework launched by the Chief of Defence Staff and DRDO Chairman, October 2024, https://www.orfonline.org/expert-speak/ai-in-modern-warfare-india-s-strategic-challenges-and-opportunities

[13] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[14] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[15] European Union External Action Service (EEAS), "Foreign Information Manipulation and Interference Reports" (Brussels, 2024), https://www.eeas.europa.eu.

[16] Government of India, Press Information Bureau / Ministry of Electronics and Information Technology, "CERT-In: India's Frontline Defender against Cyber Threats," January 2026, https://www.pib.gov.in.

[17] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[18] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[19] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[20] U.S. Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, DC, 2022), https://www.defense.gov.

[21] Kautilya, Arthashastra, various critical editions and translations, public domain text available via academic repositories such as https://sacred-texts.com.

[22] Sun Tzu, The Art of War, public domain editions available via academic archives such as https://sacred-texts.com.

[23] Niccolò Machiavelli, The Prince, public domain editions available via academic repositories such as https://www.gutenberg.org.

[24] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[25] ibid

[26] U.S. Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, DC, 2022), https://www.defense.gov.

[27] "DRDO To Soon Deploy Indigenous D4 System To Safeguard Cities Against Rogue Drones," Indian Defence News, March 2025, https://www.indiandefensenews.in.

[28] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[29] 'Impressive Counter Drones System': US Expert Praises India's D4 for Neutralising Pakistan's Drone Swarm," BusinessToday, May 2025, https://www.businesstoday.in.

[30] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[31] Government of India, Press Information Bureau / Ministry of Electronics and Information Technology, "CERT-In: India's Frontline Defender against Cyber Threats," January 2026, https://www.pib.gov.in.

[32] Carnegie Endowment for International Peace, "Mapping India's Cybersecurity Administration in 2025," September 2025, https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025.

[33] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[34] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[35] U.S. Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (Washington, DC, 2022), https://www.defense.gov.

[36] Israel Defense Forces (IDF), official publications and doctrine summaries, open-source material, https://www.idf.il.

[37] ibid

[38] John K. Tsan, "Integrated Warfare and Modern Operational Design," Journal of Strategic Studies 47, no. 2 (2024), https://www.tandfonline.com.

[39] NewKerala / NITI Aayog, "India's Semiconductor Push: Strategic Imperative, Self-Reliance Critical for Viksit Bharat," 2026, https://www.newkerala.com.

[40] European Union External Action Service (EEAS), "Foreign Information Manipulation and Interference Reports" (Brussels, 2024), https://www.eeas.europa.eu.

[41] World Economic Forum, Global Risks Report 2025 (Geneva: WEF, 2025), https://www.weforum.org.

[42] "PRAHAAR: India's New Counter-Terror Policy in a Hybrid Threat Era," Observer Research Foundation, February 26, 2026, https://www.orfonline.org/expert-speak/prahaar-india-s-new-counter-terror-policy-in-a-hybrid-threat-era.

[43] Government of India, Ministry of Defence, "Operation Sindoor: Indian Armed Forces Carried Out Precision Strike at Terrorist Camps," Press Information Bureau, May 7, 2025, https://www.pib.gov.in.

[44] Government of India, Ministry of Defence, official statements on defence modernization and jointness reforms, 2024–2025, https://www.mod.gov.in.

[45] "MHA Unveils 'PRAHAAR', India's First National Counter-Terrorism Policy," DD News, February 23, 2026, https://ddnews.gov.in/en/mha-unveils-prahaar-indias-first-national-counter-terror-policy/.

[46] "The PRAHAAR Doctrine: From Reactive Restraint to Proactive Compellence," Observer Research Foundation, May 7, 2026, https://www.orfonline.org/expert-speak/the-prahaar-doctrine-from-reactive-restraint-to-proactive-compellence.

[47] "India's PRAHAAR Blueprint: The Case for Cumulative Deterrence," Observer Research Foundation, March 16, 2026, https://www.orfonline.org/expert-speak/india-s-prahaar-blueprint-the-case-for-cumulative-deterrence.

[48] Government of India, Ministry of Defence, official statements on defence modernization and jointness reforms, 2024–2025, https://www.mod.gov.in.

[49] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[50] "1 Year of Operation Sindoor," Drishti IAS, May 7, 2026, https://www.drishtiias.com/daily-updates/daily-news-analysis/1-year-of-operation-sindoor.

[51] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[52] Israel Defense Forces (IDF), official publications and doctrine summaries, open-source material, https://www.idf.il.

[53] International Institute for Strategic Studies (IISS), The Military Balance 2025 (London: Routledge, 2025), https://www.iiss.org.

[54] Government of India, Press Information Bureau / Ministry of Electronics and Information Technology, "CERT-In: India's Frontline Defender against Cyber Threats," January 2026, https://www.pib.gov.in.

[55] North Atlantic Treaty Organization (NATO), "Emerging and Disruptive Technologies in Defence," NATO official publications, 2024, https://www.nato.int.

[56] "DRDO To Soon Deploy Indigenous D4 System To Safeguard Cities Against Rogue Drones," Indian Defence News, March 2025, https://www.indiandefensenews.in.

[57] Delhi Policy Group, "Implementing Artificial Intelligence in the Indian Military," citing the establishment of the Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA), 2019, https://www.delhipolicygroup.org.

[58] John K. Tsan, "Integrated Warfare and Modern Operational Design," Journal of Strategic Studies 47, no. 2 (2024), https://www.tandfonline.com.

[59] ibid

[60] NewKerala / NITI Aayog, "India's Semiconductor Push: Strategic Imperative, Self-Reliance Critical for Viksit Bharat," 2026, https://www.newkerala.com.

[61] Government of India, Press Information Bureau, "India Semiconductor Mission 2.0," February 2026, https://www.pib.gov.in.

[62] European Union External Action Service (EEAS), "Foreign Information Manipulation and Interference Reports" (Brussels, 2024), https://www.eeas.europa.eu.

[63] World Economic Forum, Global Risks Report 2025 (Geneva: WEF, 2025), https://www.weforum.org.

[64] Kautilya, Arthashastra, various critical editions and translations, public domain text available via academic repositories such as https://sacred-texts.com.

[65] Sun Tzu, The Art of War, public domain editions available via academic archives such as https://sacred-texts.com.

[66] Niccolò Machiavelli, The Prince, public domain editions available via academic repositories such as https://www.gutenberg.org.