CENJOWS

ISSUE BRIEF
IB/14/26

ELECTRONIC WARFARE IN THE AI ERA: FROM SPECTRUM CONTROL TO SPECTRUM INTELLIGENCE

MR DHRUVA SHAW

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Electronic Warfare in the AI Era: From Spectrum Control to Spectrum Intelligence

Dhruva Shaw is a technical research assistant at CENJOWS

The contemporary battlespace is undergoing a seismic shift, transitioning from kinetic dominance to cognitive and spectral superiority. As the Indian defence establishment navigates the mid-21st century, the Electromagnetic Spectrum (EMS) has evolved from a supportive medium for communication and sensing into a primary domain of manoeuvre and warfare. This report, "Electronic Warfare in the AI Era: From Spectrum Control to Spectrum Intelligence," provides an exhaustive analysis of this paradigm shift within the Indian strategic context. It evaluates the transition from the legacy doctrine of "Spectrum Control" characterised by static jamming, denial, and brute-force dominance to "Spectrum Intelligence," a dynamic, AI-driven state where cognitive systems predict, adapt, and exploit the electromagnetic environment in real-time.

The analysis is grounded in the operational realities of the post-2025 security environment, specifically drawing lessons from the "Operation Sindoor" and "Operation Bunyan al-Marsus" exchange, which exposed critical vulnerabilities and validated

emerging indigenous capabilities. It examines the dual-front threat posed by the People's Republic of China's (PRC) "Intelligentised Warfare" doctrine and Pakistan's asymmetric integration of AI via the Centre for Artificial Intelligence and Computing (CENTAIC).

Crucially, this report dissects the internal mechanisms of India's response, from the Defence Research and Development Organisation's (DRDO) "Project Himshakti" and "Samyukta" upgrades to the private sector's breakthrough with the "ALAAS" cognitive engine. It further addresses the civil-military friction regarding spectrum allocation in the 5G/6G era, analysing the implications of the National Frequency Allocation Plan (NFAP) 2025. The document concludes with a comprehensive strategic roadmap for the Ministry of Defence (MoD), Department of Telecommunications (DoT), and the Armed Forces, recommending the establishment of a Joint Electromagnetic Spectrum Operations (JEMSO) Command and a National EW Data Bank to secure spectrum sovereignty.

Introduction: The Cognitive Turn in Electronic Warfare

The Erosion of Traditional Spectrum Control

For decades, the philosophy of Electronic Warfare (EW) was predicated on control. In this paradigm, dominance was achieved by overpowering the adversary's emissions. Electronic Attack (EA) meant high-power jamming to deny access; Electronic Protection (EP) meant frequency hopping to evade detection; and Electronic Support (ES) involved building static libraries of threat signatures. This approach was effective against analogue adversaries but is rapidly becoming obsolete in the digital age.[1]

The modern electromagnetic environment is characterized by unprecedented congestion and complexity. The proliferation of 5G networks, the Internet of Things (IoT), and ubiquitous commercial satellite constellations has created a "noise floor" so high that distinguishing a hostile signal from civilian traffic is akin to finding a needle in a stack of needles. Furthermore, the adversary is no longer static. Modern radars and communication systems utilize Active Electronically Scanned Arrays (AESA) and software-defined radios (SDR) that can alter their waveforms thousands of times per second. A rule-based system, which relies on a pre-programmed library to identify a

threat, cannot keep pace with an AI-driven adversary that generates novel waveforms on the fly.[2]

Defining Spectrum Intelligence

"Spectrum Intelligence" represents the necessary evolution from this static posture. It is not merely about controlling the spectrum but understanding it at a cognitive level. It leverages Artificial Intelligence (AI) and Machine Learning (ML) to process the totality of the electromagnetic environment.

Unlike traditional systems that ask, "Is this signal in my threat library?", Spectrum Intelligence asks, "What is the intent of this anomaly?" It utilises deep reinforcement learning to identify subtle patterns in the noise, the "breathing" of a stealth aircraft's data link or the micro-Doppler signature of a hovering drone.[3] This transition shifts the operational focus from *reaction* to *prediction*. A Spectrum Intelligence system anticipates jamming attempts before they occur, dynamically reallocating bandwidth to maintain link integrity, and even autonomously generating deceptive signals to confuse the adversary.[4]

The "Super OODA" Loop and Machine-Speed Warfare

The integration of AI into EW compresses the decision-making cycle the Observe-Orient-Decide-Act (OODA) loop to speeds beyond human cognition. In the Indian context, where reaction times in the mountainous terrain of the Himalayas are already minimal, this compression is vital. AI systems act as "complexity accelerants," capable of managing frequency hopping and adaptive jamming in milliseconds.[5]

However, this "Super OODA" loop introduces profound strategic risks. When opposing AI systems interact, one trying to jam, the other trying to evade the speed of their countermeasures, can spiral into an uncontrolled escalation, potentially triggering kinetic strikes based on automated threat assessments. The "Operation Sindoor" simulation highlighted this risk, where rapid automated signal shifts nearly led to unintended escalation, underscoring the need for "Man-on-the-loop" oversight rather than just "Man-in-the-loop" control. [6]

Operational Case Study: Lessons from the 2025 Conflict

The brief but intense multi-domain exchange in May 2025, referred to in defence circles as the "Operation Sindoor" (Indian offensive) and "Operation Bunyan al-Marsus" (Pakistani retaliation) sequence, serves as a critical crucible for understanding the realities of modern EW in South Asia.[7]

- **Operation Sindoor: The Efficacy of Indigenous EW**

  During "Operation Sindoor," the Indian Air Force (IAF) and Army engaged targets across the border. A key observation was the performance of indigenous EW systems against the Pakistan Air Force's (PAF) modern assets. Reports indicate that Indian EW suites effectively jammed the avionics of PAF J-10C fighters, preventing them from achieving radar locks. [8] This validated the "Systems-First" strategy of DRDO, where the electronic suite is prioritised over the platform itself.[9]

  The conflict demonstrated that superior platforms (like the J-10C) are vulnerable if their electromagnetic eyes are blinded. The "complexity accelerant" effect of AI-driven jammers meant that Pakistani pilots faced a "denial of service" attack on their situational awareness, forcing them to abort missions or rely on visual flight rules, thereby negating their technological edge. [10]

- **Operation Bunyan al-Marsus: Drone Swarms and Spectrum Saturation**

  Pakistan's retaliation, "Operation Bunyan al-Marsus," involved a complex drone offensive utilising Turkish (Bayraktar/Songar), Chinese (CH-3/4), and indigenous (Shahpur) platforms.[11] The attack utilised a "swarm" tactic intended to saturate India’s air defence radars.

  However, the operation revealed the critical role of Spectrum Intelligence in counter-drone warfare. India’s integrated air defence network, bolstered by AI-driven target recognition, successfully intercepted 90% of the incoming UAVs. [12] The ability to discriminate between the radar cross-section (RCS) of a bird, a commercial quadcopter, and a military loitering munition was made possible only through algorithmic processing of the spectrum data. This event marked the end

of the "swarm hype" as an unstoppable force, proving that with sufficient spectral awareness, mass can be countered by precision.

- **The "Fog of Electronics"**

  A significant lesson from the conflict was the "Fog of Electronics." The massive use of jamming on both sides led to a degradation of Global Navigation Satellite System (GNSS) signals, affecting not just military units but civil aviation and logistics.[13] This spillover effect highlighted the lack of effective "firewalls" in the spectrum domain. The rapid escalation of jamming protocols, driven by automated systems, meant that commanders often lost contact with forward units, forcing a reliance on pre-planned mission command protocols. This underscored the need for resilient, anti-jam communication networks like the "SAMBHAV" system.[14]

The Adversarial Threat Matrix

India’s transition to Spectrum Intelligence is driven by necessity. The threat landscape is defined by the modernisation trajectories of China and Pakistan, both of which are aggressively integrating AI into their EW architectures.

- **China: The Doctrine of Intelligentised Warfare**

  The People’s Liberation Army (PLA) views the spectrum not just as a domain of warfare but as the nervous system of modern combat. Their doctrine has evolved from "Informatised Warfare" (network-centric) to "Intelligentised Warfare" (algorithm-centric).[15]

  - **Structural Reform: The Information Support Force (ISF)**

    In April 2024, the PLA underwent a significant restructuring, dissolving the Strategic Support Force (SSF) and establishing the Information Support Force (ISF).[16] This move was designed to streamline the command and control of information warfare assets. The ISF is tasked with constructing and defending the information network, while the Cyberspace Force and Aerospace Force handle offensive operations. For India, this means facing

a more agile and integrated adversary where EW, cyber, and space operations are synchronised under a unified strategic vision.[17]

- **The Western Theatre Command (WTC) Capabilities**

  The WTC, responsible for the border with India, has become a testbed for these new concepts. The Joint Operations Command Centre (JOCC) of the WTC is described as the "smartest brain," using AI to simulate battlefield scenarios and optimise spectrum usage.[18]

Key assets deployed in the region include:

- **Y-9 Electronic Warfare Aircraft:** These platforms provide standoff jamming capabilities, capable of blinding Indian radars from deep within Tibetan airspace.[19] Their presence allows the PLA to mask the movement of ground forces and screen aerial incursions.
- **Dzong Electronic Warfare Stations:** The PLA has established permanent EW and SIGINT (Signals Intelligence) stations in Tibet, such as those at "Dzong" locations (e.g., Tsona Dzong). These high-altitude facilities provide a line-of-sight advantage, allowing them to monitor deep into Indian territory.[20]
- **Underground Infrastructure:** Extensive underground fibre-optic networks and missile storage facilities in Tibet reduce the electromagnetic signature of PLA communications, making them harder to detect and intercept.[21]
- **Cognitive EW and AI Targeting:** The PLA is actively developing "Cognitive Electronic Warfare" systems that use AI to analyse the spectrum and optimise jamming in real-time. Reports suggest that during the 2020 skirmishes and subsequent standoffs, the PLA used these systems to test the resilience of Indian communications.[22] The ultimate goal of Intelligentised Warfare is to use AI not just for targeting but for "cognitive dominance", manipulating the information environment to break the adversary's will to fight.[23]
- **Pakistan: Asymmetric Balancing and AI Integration:** Pakistan’s strategy relies on "balancing" India’s conventional superiority through asymmetric means and technological partnerships.

- **CENTAIC and the AI Push**

  The establishment of the Centre for Artificial Intelligence and Computing (CENTAIC) by the Pakistan Air Force (PAF) in 2020 marked a strategic pivot. [24] CENTAIC focuses on automating threat recognition, data fusion, and developing cognitive EW systems. While mostly focused on training and local development, the potential for integrating Chinese AI algorithms into Pakistani platforms remains a significant concern for Indian planners.[25]

- **The JF-17 Block III and Cyber-EW Convergence**

  The induction of the JF-17 Block III, equipped with AESA radars and advanced EW suites, provides the PAF with a platform capable of contesting the spectrum. [26] Furthermore, Pakistan has integrated cyber warfare into its military doctrine. The convergence of cyber and EW capabilities allows Pakistan to launch "hybrid" attacks, where electronic jamming is used to create an opening for cyber intrusions into Indian command and control networks.[27]

India's Indigenous Response: Aatmanirbhar Bharat in the Spectrum

In response to this formidable threat matrix, India has aggressively pursued indigenisation under the "Aatmanirbhar Bharat" (Self-Reliant India) initiative. This has resulted in a "Systems-First" approach, prioritising the development of sensors, seekers, and EW suites over the mere acquisition of foreign platforms. [28]

- **The DRDO Ecosystem: Pillars of Electronic Defence**

  The Defence Research and Development Organisation (DRDO) has spearheaded several high-value projects that form the backbone of India's EW capability.

  - **Project Himshakti**

    "Project Himshakti" represents a paradigm shift in mountain warfare EW. A ₹3,000 crore contract awarded to Bharat Electronics Limited (BEL), this system is specifically engineered for the treacherous terrain of the Himalayas.[29]

- **Capabilities:** It features integrated EW systems with ultraviolet VHF direction finders and high-power jammers.
- **Operational Role:** Designed to operate in deep valleys where signal propagation is erratic, Himshakti ensures that the Indian Army can detect and disrupt PLA communications even in "shadow zones".[30]
- **Strategic Significance:** Being an indigenous project involving MSMEs, it ensures that the source code and frequency libraries are fully under Indian control, eliminating the risk of "kill switches" or backdoors found in imported equipment.[31]

➢ **The Samyukta and its AI Upgrade**

The Samyukta Electronic Warfare System is a massive, mobile integrated EW complex comprising 145 vehicles. It creates an "electronic web" covering an area of 150 km by 70 km, capable of handling both communication (COMINT) and non-communication (ELINT/Radar) signals.[32]

The AI Pivot**:** Recent upgrades have integrated AI modules into Samyukta. These algorithms allow for the real-time classification of signals and the automated prioritisation of threats. Instead of a human operator manually tuning a jammer, the AI detects a hostile emitter and instantly assigns the optimal jamming resource from across the 145-vehicle network. [33]

➢ **Project Kautilya and Space-Based ELINT**

"Project Kautilya" is India’s answer to the need for strategic depth in spectrum intelligence. It involves the development of Space-Borne ELINT Systems, most notably the EMISAT satellite.[34]

- **Function:** EMISAT scans the electromagnetic terrain of Tibet and Pakistan from space, detecting the location and signature of enemy radars (such as the S-400 or HQ-9 batteries).
- **Integration:** This data is fed into the ground-based EW network,

allowing commanders to build a comprehensive "Electronic Order of Battle" (EOB) before a conflict even begins. [35]

The Private Sector Revolution: iDEX and Startups

The "Innovations for Defence Excellence" (iDEX) initiative has successfully democratized defense innovation, allowing startups to contribute cutting-edge technology.[36]

FleetRF: The Anti-Jamming Breakthrough

FleetRF, a Delhi-based startup, secured a landmark contract to supply the Indian Army with an indigenous anti-jamming drone communication system. [37]

- **Technology:** The system uses a tri-layer security architecture (advanced encryption, dynamic frequency hopping, and adaptive power control).
- **AI Module:** Its standout feature is an AI-driven spectrum intelligence module that predicts jamming attempts. By analyzing the "noise" in the spectrum, it can anticipate a jammer's activation and preemptively hop to a clear frequency, ensuring mission continuity in hostile EW environments.[38]

Adani Defence and the Drishti-10

Adani Defence’s delivery of the Drishti-10 Starliner (based on the Elbit Hermes 900) provides the Indian Navy with a critical high-altitude node.[39]

- **Role:** While primarily an ISR platform, its long endurance (36 hours) and high payload capacity make it an ideal platform for persistent ELINT operations. Flying at 30,000 feet, it can "listen" to maritime and coastal communications deep into the Indian Ocean Region (IOR), feeding data into the Navy's spectrum intelligence network.[40]

The AI Pivot: ALAAS and Cognitive Warfare

The most transformative development in India's EW arsenal is the deployment of ALAAS (Autonomous Learning Adaptive Artificial Intelligence System).[41] This system epitomizes the shift from Spectrum Control to Spectrum Intelligence.

ALAAS: The Cognitive Engine

Developed by the Defence Artificial Intelligence Project Agency (DAIPA) in collaboration with DRDO and private industry, ALAAS is a "strategic force multiplier" designed to compress the OODA loop. [42]

- **Deep Reinforcement Learning:** Unlike rule-based systems, ALAAS learns from every interaction. If an adversary uses a new jamming technique, ALAAS analyzes it, devises a countermeasure, and remembers the solution for future encounters.
- **Predictive Accuracy:** In simulations, ALAAS has demonstrated over 90% accuracy in predicting adversary intentions based on their electromagnetic posture. [43]
- **Swarm Coordination:** The system acts as a "hive mind" for drone swarms. It can coordinate the spectral emissions of hundreds of drones to mimic the signature of a large attack force (electronic deception) or to conduct synchronized jamming attacks on enemy radars. [44]

Cognitive Electronic Warfare (CEW) Operations

ALAAS enables true Cognitive Electronic Warfare. In a CEW scenario, the system continuously scans the spectrum. When it detects a hostile radar, it doesn't just blast noise. It analyses the radar's pulse repetition frequency (PRF) and scan pattern. It then constructs a specific waveform that enters the enemy radar's receiver and creates false targets (spoofing) or masks the friendly aircraft entirely. [45]

Cyber-Electromagnetic Activities (CEMA)

ALAAS also bridges the gap between EW and Cyber warfare. It can launch AI-driven cyber counterattacks via the RF spectrum. For example, by injecting malicious code into an enemy's wireless network through a high-power data stream, it can disrupt their command-and-control infrastructure from within. [46]

Spectrum Governance: The Civil-Military Conundrum

While military capabilities are advancing, the governance of the spectrum the very terrain of this warfare remains a point of friction. The explosive growth of civilian 5G and 6G

networks competes directly with military requirements for bandwidth.

The National Frequency Allocation Plan (NFAP) 2025

The Department of Telecommunications (DoT) released the NFAP-2025, effective December 30, 2025, to align India with global spectrum standards.[47]

- **Key Allocations:** The plan identifies the 6425–7125 MHz band for International Mobile Telecommunications (IMT), crucial for 5G Advanced and 6G.[48] It also allocates Ka, Q, and V bands for high-throughput satellites.
- **The Conflict:** The mid-band spectrum (3.3-3.6 GHz), vital for 5G, sits adjacent to frequencies used by naval radars and military satellite uplinks. This proximity raises the risk of interference. A 5G tower broadcasting at high power near a naval base could potentially "blind" a surveillance radar or desensitize its receiver.[49]

The Imperative for Dynamic Spectrum Sharing (DSS)

The traditional model of static allocation—"This slice is for the Army; this slice is for Jio" is inefficient and unsustainable. The solution lies in Dynamic Spectrum Sharing (DSS).

- **The Concept:** DSS allows military and civilian users to share the same frequency band. Access is prioritized based on time, location, and alert capability. For example, a band could be used for civilian 5G in New Delhi but reserved for military radars in the border districts of Rajasthan.
- **Global Precedents:** The US Department of Defence has initiated "moonshot" efforts to develop DSS technologies, recognizing that spectrum sharing is essential for maintaining economic leadership without compromising security.[50]
- **Indian Implementation:** NFAP-2025 begins to lay the groundwork for this, but fully operationalizing DSS requires real-time data exchange between Telcos and the MoD a capability currently lacking. [51]

Digital Public Infrastructure (DPI) for Defence

India’s success with Digital Public Infrastructure (DPI) like Aadhaar and UPI offers a unique model for solving this problem. The "India Stack" philosophy open APIs, interoperable standards, and modular architecture can be applied to defence spectrum

management.[52]

- **A "Defence Spectrum Stack":** By creating a unified, secure digital layer for spectrum management, the armed forces could share spectrum data seamlessly. This would allow an Army EW unit to request temporary bandwidth from a civilian network for a specific operation, managed automatically through a "smart contract" type protocol.

Institutional Architecture and Human Capital

Technological solutions are only as good as the institutions that manage them. India has made significant strides in modernizing its higher defence organization, but gaps remain.

The Chief of Defence Staff (CDS) and Jointness

The creation of the CDS and the Department of Military Affairs (DMA) was a watershed moment. In 2024, the CDS released the Joint Doctrine for Cyberspace Operations, which provides a unified framework for the Army, Navy, and Air Force.[53]

- **Impact:** This doctrine ends the era of "strategic ambiguity" and mandates a proactive posture. It directs the services to integrate their cyber and EW capabilities, moving away from siloed operations.[54]
- **Implementation:** The doctrine is being operationalized through the Defence Cyber Agency (DCyA), which coordinates joint operations and training.[55]

The Human Capital Crisis

Despite these structural reforms, India faces a critical shortage of specialized talent. The private sector absorbs the vast majority of AI and cybersecurity experts.

- **The Gap:** Less than 20% of cyber defence roles in the government are filled by qualified specialists.[56] The rigid recruitment and pay structures of the military make it difficult to attract top-tier talent.
- **Territorial Army Initiative:** To bridge this gap, the Territorial Army (TA) has launched Cyber Regiments, recruiting civilian experts as "Cyber Warriors".[57] These officers serve in a part-time capacity, bringing their industry expertise to the military. While a positive step, the scale (only a few specialized units) is insufficient

for the magnitude of the threat.

Data Standardization Challenges

A major hurdle for systems like ALAAS is the lack of a "Joint Data Standard." The Army, Navy, and Air Force often use different data formats for their legacy systems. This means that data from an IAF AWACS cannot be instantly fed into an Army air defence computer without complex transcoding.[58] Achieving interoperability requires a unified data language a "Military-IoT" standard that allows machines to talk to machines across services.[59]

Strategic Roadmap and Recommendations

To fully transition from Spectrum Control to Spectrum Intelligence and secure dominance in the cognitive era, the following recommendations are proposed for Indian agencies and ministries.

For the Ministry of Defence (MoD) & CDS

Recommendation 1: Establish a Joint Electromagnetic Spectrum Operations (JEMSO) Command

- **Rationale:** The spectrum is a unified domain. Fragmented management by the Army Corps of Signals, IAF EW wings, and Navy WEESE creates seams that adversaries can exploit.
- **Action:** Create a JEMSO Command under the CDS, equivalent to the Defence Cyber and Space Agencies. This command would be responsible for:
  - Unified spectrum management and manoeuvre.
  - Coordinating "soft kill" (EW) and "hard kill" (kinetic) effects.
  - Developing a Joint Electronic Order of Battle (J-EOB).

Recommendation 2: Implement "Project Spectrum-X" – A National EW Data Bank

- **Rationale:** AI systems like ALAAS are data-hungry. They need vast libraries of signals to learn and predict. Currently, data collected by the NTRO, RAW, and the three services sits in silos.
- **Action:** Establish a centralized, cloud-based "National EW Data Bank." Mandate

the sharing of raw spectrum logs from all border sensors, satellite feeds (EMISAT), and ISR platforms. This data lake will serve as the training ground for national defence algorithms.

Recommendation 3: Adopt a Doctrine of "Cognitive Denial"

- **Rationale:** To defeat China's "Intelligentized Warfare," India must attack the algorithm, not just the platform.
- **Action:** Fund research into "Adversarial AI." Develop techniques to "poison" the data streams that Chinese AI systems rely on, causing their automated targeting systems to misidentify friendly forces or ignore real threats (Cognitive Fluency Bias exploitation). [60]

For the Defence Research and Development Organisation (DRDO) & ANRF

Recommendation 4: Accelerate Neuromorphic Computing R&D

- **Rationale:** Edge computing is essential for drones and missiles that cannot rely on cloud links in a jammed environment. Neuromorphic chips, which mimic the human brain, offer the high efficiency required for onboard AI. [61]
- **Action:** The Anusandhan National Research Foundation (ANRF) should launch a "Grand Challenge" for neuromorphic chip design, funding university-industry consortiums to develop indigenous chips specifically for defence applications.[62]

Recommendation 5: Standardize the "Military-IoT" Protocol

- **Rationale:** To solve the interoperability crisis.
- **Action:** DRDO must lead the development of a secure, open-standard "Military-IoT" protocol. This should be mandated for all future procurement if a system cannot talk to the Joint Data Network, it cannot be bought.

For the Department of Telecommunications (DoT) & TRAI

Recommendation 6: Operationalize Dynamic Spectrum Sharing (DSS) Zones

- **Rationale:** To resolve the 5G vs. Radar conflict.
- **Action:** Designate 100km "Dynamic Spectrum Zones" along the LoC and LAC. In

these zones, military spectrum usage has automated priority. Implement a real-time data link between Telco Network Operations Centres (NOCs) and the JEMSO Command to automate the handover of spectrum during alerts.

Recommendation 7: Civil-Military Sensor Grid

- **Rationale:** India has thousands of civilian telecom towers. These can be used as a strategic asset.
- **Action:** Mandate that 5G infrastructure in border states be equipped with "passive sensing" capabilities. These towers can detect the disruption caused by low-flying drones or stealth aircraft, effectively turning the civilian cellular network into a massive, distributed radar system.

For Recruitment and Talent Management

Recommendation 8: Create a "Defence AI Corps" (DAIC)

- **Rationale:** The current recruitment model is failing to attract necessary talent.
- **Action:** Establish a "Defence AI Corps" as a distinct branch. Offer operational autonomy, market-competitive salaries, and lateral entry for mid-career professionals. Move beyond the Territorial Army model to a full-time, specialized professional cadre.

Recommendation 9: "Deep Tech" Scale-Up Fund under iDEX

- **Rationale:** Startups like FleetRF prove the capability exists, but they struggle to scale production.
- **Action:** Create a dedicated "Scale-Up Fund" within iDEX. This fund should provide large-ticket capital (₹50-100 Cr) to proven defence startups for setting up manufacturing lines, helping them cross the "valley of death" between prototype and induction. [63]

Conclusion

The transition to Spectrum Intelligence is not an option; it is a prerequisite for survival in the 21st-century battlefield. The events of 2025 have shown that a smaller, smarter force

can hold its own against a larger adversary if it controls the cognitive domain.

India stands at a pivotal moment. It possesses the raw ingredients for success: a world-class software industry, a reinvigorated defence manufacturing sector, and a strategic vision under Aatmanirbhar Bharat. However, realizing this potential requires a fundamental shift in mindset. It requires moving from protecting silos to sharing data, from buying hardware to building ecosystems, and from controlling the spectrum to understanding it. By implementing these recommendations, India can ensure that in the invisible wars of the future, its "Spectrum Intelligence" remains second to none.

Appendix: Comparative Data

Feature	**Traditional EW (Spectrum Control)**	**Cognitive EW (Spectrum Intelligence)**
Core Technology	Analog/Digital Signal Processing	Deep Reinforcement Learning / Generative AI
Response Time	Seconds to Minutes	Milliseconds to Microseconds
Countermeasure	Pre-programmed (Library Match)	Adaptive (Real-time Generation)
Operator Role	Man-in-the-loop (Control)	Man-on-the-loop (Oversight)
Primary Goal	Denial of Access	Information Dominance & Deception

Table 1: The Technological Shift from Control to Intelligence.

Capability	**China (PLA)**	**Pakistan (Armed Forces)**	**India (Armed Forces)**
Doctrine	Intelligentized Warfare	Tech-Balancing / Hybrid War	Joint Cyber Doctrine / Spectrum Intel
Key Assets	Y-9 EW, J-16D, ISF	JF-17 Blk III, CENTAIC	ALAAS, Himshakti, Samyukta
Spectrum Strategy	Centralized / State Control	Military Priority	Moving to Dynamic Sharing (DSS)
AI Integration	Systemic / Foundational	Asymmetric / Niche	Rapidly Scaling / Indigenous

Table 2: Regional Capability Comparison.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

[1] $1 billion Oron spy plane provides vital strategic advantage - The Jerusalem Post, accessed January 2, 2026, https://www.jpost.com/defense-and-tech/article-865208
[2] Modern Warfare: India's AI & ISR Boost in Military Capabilities ..., accessed January 2, 2026, https://claws.co.in/modern-warfare-indias-ai-isr-boost-in-military-capabilities/
[3] Defense & Security - LS Spectrum Solutions, accessed January 2, 2026, https://www.lstelcom.in/industries/defense-security/
[4] FleetRF Secures Indian Army Deal for Indigenous Anti-Jamming Drone Communication System - Shop SSBCrack, accessed January 2, 2026, https://shop.ssbcrack.com/blogs/blog/fleetrf-secures-indian-army-deal-for-indigenous-anti-jamming-drone-communication-system
[5] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[6] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[7] Indian Netizens Savage China's Ceasefire Claims by Exposing Catastrophic Failures of Its Weaponry in Op Sindoor, accessed January 2, 2026, https://defence.in/threads/indian-netizens-savage-chinas-ceasefire-claims-by-exposing-catastrophic-failures-of-its-weaponry-in-op-sindoor.16456/
[8] Indian Netizens Savage China's Ceasefire Claims by Exposing Catastrophic Failures of Its Weaponry in Op Sindoor, accessed January 2, 2026, https://defence.in/threads/indian-netizens-savage-chinas-ceasefire-claims-by-exposing-catastrophic-failures-of-its-weaponry-in-op-sindoor.16456/
[9] How DRDO's systems-first strategy is powering India's path to self-reliance, accessed January 2, 2026, https://etedge-insights.com/industry/defence-aerospace/inside-drdos-systems-first-strategy-driving-indias-defence-electronics-rise/
[10] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[11] Drone Warfare Yesterday, Today and Tomorrow - Part 2, accessed January 2, 2026, https://www.natstrat.org/articledetail/publications/drone-warfare-yesterday-today-and-tomorrow-part-240.html
[12] How DRDO's systems-first strategy is powering India's path to self-reliance, accessed January 2, 2026, https://etedge-insights.com/industry/defence-aerospace/inside-drdos-systems-first-strategy-driving-indias-defence-electronics-rise/

[13] India unveils ambitious 15-year defence modernization plan worth hundreds of billions of dollars, accessed January 2, 2026, https://www.indiasentinels.com/defence-ministry/india-unveils-ambitious-15-year-defence-modernization-plan-worth-hundreds-of-billions-of-dollars-7022
[14] India's Electronic Warfare Leap - The Study IAS, accessed January 2, 2026, https://thestudyias.com/blogs/indias-electronic-warfare-leap/
[15] Multi-Domain Warfare: How India Fits into the World's New Power Equation - CLAWS, accessed January 2, 2026, https://claws.co.in/multi-domain-warfare-how-india-fits-into-the-worlds-new-power-equation/
[16] Mapping the Recent Trends in China's Military Modernisation - 2025, accessed January 2, 2026, https://www.orfonline.org/research/mapping-the-recent-trends-in-china-s-military-modernisation-2025
[17] Military and Security Developments Involving the People's Republic of China 2024 - DoD, accessed January 2, 2026, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF
[18] Assessing Operations and 'Jointness' in the PLA Western Theater Command - Takshashila Institution, accessed January 2, 2026, https://takshashila.org.in/content/publications/assets/operations-PLA-WTC.pdf
[19] Assessing Operations and 'Jointness' in the PLA Western Theater Command - Takshashila Institution, accessed January 2, 2026, https://takshashila.org.in/content/publications/assets/operations-PLA-WTC.pdf
[20] India–Bhutan: Defence Infrastructure And Training Cooperation, accessed January 2, 2026, https://www.impriindia.com/insights/policy-update/india-bhutan-defence/
[21] Nuclear Threat, accessed January 2, 2026, https://tibetnature.net/en/nuclear-threats/
[22] Why China's military is the big winner from India-Pakistan attacks. India and Pakistan's biggest skirmish in decades is also a major testing ground for Chinese and Western jets and other military hardware. - Reddit, accessed January 2, 2026, https://www.reddit.com/r/LessCredibleDefence/comments/1kjpkd2/why_chinas_military_is_the_big_winner_from/
[23] synergy - CENJOWS, accessed January 2, 2026, https://cenjows.in/wp-content/uploads/2025/05/Synergy-Journal-Feb-Issue-2025_-23-5-25.pdf
[24] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[25] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[26] Next Generation Air Warfare in South Asia: Risks and Way Forward ..., accessed January 2, 2026, https://southasianvoices.org/sec-m-pk-r-next-gen-air-warfare-in-south-asia-1-1-2026/
[27] CYBERSPACE CYBERSPACE AS A AS A BATTLEFIELD BATTLEFIELD - CENJOWS, accessed January 2, 2026, https://cenjows.in/wp-content/uploads/2022/09/Cyberspace_as_a_battlefield.pdf
[28] Drone Warfare Yesterday, Today and Tomorrow - Part 2, accessed January 2, 2026, https://www.natstrat.org/articledetail/publications/drone-warfare-yesterday-today-and-tomorrow-part-240.html
[29] More Teeth for Army, Navy, Air Force, accessed January 2, 2026, https://www.spsnavalforces.com/experts-speak/?id=577&h=More-Teeth-for-Army-Navy-Air-Force
[30] India awards three contracts to Bharat Electronics without competition - Defense News, accessed January 2, 2026, https://www.defensenews.com/industry/2023/03/28/india-awards-three-contracts-to-bharat-electronics-without-competition/
[31] MoD signs Rs 3000 crore contract with BEL for procurement of two Integrated Electronic Warfare Systems 'Project Himshakti' - PIB, accessed January 2, 2026, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1910337
[32] Electronic Warfare – Denying Electromagnetic Advantage to Enemy - SP's Land Forces, accessed January 2, 2026, https://www.spslandforces.com/story/?id=698&h=Electronic-Warfare-Denying-Electromagnetic-Advantage-to-Enemy
[33] India unveils ambitious 15-year defence modernization plan worth hundreds of billions of dollars, accessed January 2, 2026, https://www.indiasentinels.com/defence-ministry/india-unveils-ambitious-15-year-defence-modernization-plan-worth-hundreds-of-billions-of-dollars-7022
[34] EMISAT: A Force Multiplier - Centre for Land Warfare Studies (CLAWS), accessed January 2, 2026, https://archive.claws.co.in/images/publication_pdf/584084619_184.EMISATAForce_CLAWS.pdf
[35] DoT releases National Frequency Allocation Plan 2025 (NFAP-2025) | Capital Market News, accessed January 2, 2026, https://www.business-standard.com/markets/capital-market-news/dot-releases-national-

frequency-allocation-plan-2025-nfap-2025-125123100115_1.html
[36] India's Defence Tech Gold Rush! Startups Soar as Innovation Meets War Chests!, accessed January 2, 2026, https://www.whalesbook.com/news/English/tech/Crypto-MandA-Record-Shattered-Then-COLLAPSED-dollar86B-Deals-Vanish-as-Prices-Plummet/6930e41d65a9badb9b76f103
[37] FleetRF Secures Indian Army Deal for Indigenous Anti-Jamming Drone Communication System - Shop SSBCrack, accessed January 2, 2026, https://shop.ssbcrack.com/blogs/blog/fleetrf-secures-indian-army-deal-for-indigenous-anti-jamming-drone-communication-system
[38] FleetRF to Supply Indigenous Anti-Jamming Drone Communication System, Wins Indian Army Contract - Raksha Anirveda, accessed January 2, 2026, https://raksha-anirveda.com/fleetrf-to-supply-indigenous-anti-jamming-drone-communication-system-wins-indian-army-contract/
[39] Navy Chief Unveils First Indigenous Aircraft Carrier - Adani Group, accessed January 2, 2026, https://www.adani.com/newsroom/media-releases/navy-chief-unveils-first-indigenously
[40] Adani Defence And Aerospace's Drishti-10 Starliner Drone Joins Indian Navy Fleet | Latest News - YouTube, accessed January 2, 2026, https://www.youtube.com/watch?v=YEf5XfoiA1E
[41] ALAAS Unleashed: Revolutionary AI for Battlefield Victory, accessed January 2, 2026, https://indiandefenceinstitute.com/alaas/
[42] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[43] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[44] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[45] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[46] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[47] DoT releases National Frequency Allocation Plan 2025 (NFAP-2025) | Capital Market News, accessed January 2, 2026, https://www.business-standard.com/markets/capital-market-news/dot-releases-national-frequency-allocation-plan-2025-nfap-2025-125123100115_1.htmL
[48] DoT earmarks upper 6GHz band for 5G, 6G services under NFAP 2025, accessed January 2, 2026, https://www.communicationstoday.co.in/dot-earmarks-upper-6ghz-band-for-5g-6g-services-under-nfap-2025/
[49] SIA-India - A Balanced Approach for Spectrum Allocation, accessed January 2, 2026, https://www.sia-india.com/wp-content/uploads/2022/03/SIA-India-Study-Paper-on-A-Balanced-Approach-for-Spectrum-Allocation.pdf
[50] Strategic Insights Memo - Atlantic Council, accessed January 2, 2026, https://www.atlanticcouncil.org/category/content-series/strategic-insights-memos/feed/
[51] AI-Powered Espionage: How India's Cybersecurity Strategy Must Evolve - CyberPeace, accessed January 2, 2026, https://cyberpeace.org/resources/blogs/ai-powered-espionage-how-indias-cybersecurity-strategy-must-evolve
[52] Decoding Digital Public Infrastructure - IIM Bangalore, accessed January 2, 2026, https://www.iimb.ac.in/cdpg/pdf/Monograph-Decoding-DPI.pdf
[53] Chief of Defence Staff releases 3 joint doctrines for armed forces | Current Affairs | Vision IAS, accessed January 2, 2026, https://visionias.in/current-affairs/news-today/2025-08-28/security/chief-of-defence-staff-releases-3-joint-doctrines-for-armed-forces
[54] India-Pakistan Cyber Skirmishes and the Challenge of Attribution - Stimson Center, accessed January 2, 2026, https://www.stimson.org/2025/india-pakistan-cyber-skirmishes-and-the-challenge-of-attribution/
[55] New Military Doctrine in India Centralizes Cyber Operations - BankInfoSecurity, accessed January 2, 2026, https://www.bankinfosecurity.asia/new-military-doctrine-in-india-centralizes-cyber-operations-a-25577
[56] AI-Powered Espionage: How India's Cybersecurity Strategy Must Evolve - CyberPeace, accessed

January 2, 2026, https://cyberpeace.org/resources/blogs/ai-powered-espionage-how-indias-cybersecurity-strategy-must-evolve

[57] JOIN TERRITORIAL ARMY AS AN OFFICER, accessed January 2, 2026, https://territorialarmy.in/uploads/downloads/downloads_1721330745.pdf

[58] OSD RDT&E BUDGET ITEM JUSTIFICATION (R2 Exhibit) - Office of the Under Secretary of Defense (Comptroller), accessed January 2, 2026, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2008/budget_justification/pdfs/03_RDT_and_E/Vol_3_OSD/BA-3.pdf

[59] OSD RDT&E BUDGET ITEM JUSTIFICATION (R2 Exhibit) - Office of the Under Secretary of Defense (Comptroller), accessed January 2, 2026, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2009/budget_justification/pdfs/03_RDT_and_E/Vol_3_OSD/E_OSD%20PB09%20RDTE%20BA%204.pdf

[60] India awards three contracts to Bharat Electronics without competition - Defense News, accessed January 2, 2026, https://www.defensenews.com/industry/2023/03/28/india-awards-three-contracts-to-bharat-electronics-without-competition/

[61] $1 billion Oron spy plane provides vital strategic advantage - The Jerusalem Post, accessed January 2, 2026, https://www.jpost.com/defense-and-tech/article-865208

[62] ANRF MISSION AI for Science and Engineering (AI-SE) - The Electronic Project Proposal Management System, For ANRF, accessed January 2, 2026, https://anrfonline.in/ANRF/aise_anrf

[63] DoT earmarks upper 6GHz band for 5G, 6G services under NFAP 2025, accessed January 2, 2026, https://www.communicationstoday.co.in/dot-earmarks-upper-6ghz-band-for-5g-6g-services-under-nfap-2025/