CENTRE FOR LAND WARFARE STUDIES

ROUND TABLE DISCUSSION

WINNING THE INVISIBLE WAR: SPECTRUM DOMINANCE, AUTONOMY AND THE NEW GRAMMAR OF ELECTRONIC WARFARE (EW)

Wednesday, 13th May 2026, CLAWS, New Delhi

Report prepared by: Khushboo Sen Dhuruv, Research Assistant, CLAWS

The Centre for Land Warfare Studies (CLAWS), in collaboration with The Strategic Research and Growth Foundation (SRGF), organised a Round Table Discussion on "Winning the Invisible War: Spectrum Dominance, Autonomy and the New Grammar of Electronic Warfare (EW)" on 13 May 2026 at Chanakya Hall, New Delhi. The discussion brought together senior military leaders, cyber and EW specialists, and industry representatives to deliberate on the growing importance of EW, cyber-electromagnetic convergence, artificial intelligence (AI), autonomy, and spectrum dominance in future conflicts. Lt Gen Dushyant Singh, PVSM, AVSM (Retd), DG CLAWS delivered the welcome remarks and highlighted the transformational nature of warfare, stressing the importance of spectrum control and integrated national preparedness. Lt Gen Vineet Gaur, PVSM, AVSM, DG CD delivered a special address, followed by a keynote address by Maj Gen KTG Krishnan, ACIDS, Jt Ops, HQIDS on "Use of EW in Combined Operations".

Session I on "EW in Drone and Swarm Warfare, "moderated by Rear Admiral Mohit Gupta, VSM (Retd), focused on counter-UAS jamming, anti-swarm spectrum saturation, and the trade-offs between autonomy and jamming resilience. The speakers highlighted the growing threat posed by drones and autonomous swarms and stressed the need for layered and adaptive counter-drone systems. Session II on "Cyber-EW Convergence," moderated by Air Marshal Daljit Singh, PVSM, AVSM, VM (Retd), examined the integration of cyber and electronic warfare capabilities, particularly the use of RF-based attacks to inject false data and manipulate adversary networks. Session III on "AI-Driven Cognitive EW," moderated by Lt Gen Sanjay Verma, PVSM, AVSM, VSM** (Retd), discussed autonomous threat detection, real-time spectrum management, and machine-speed decision loops, emphasising the transformative role of AI in future EW operations. The discussion concluded that future conflicts will increasingly be defined by spectrum dominance, AI-enabled systems, and integrated cyber-electromagnetic operations.

Executive Summary

The seminar deliberated upon the evolving landscape of modern warfare, underscoring that conflict has fundamentally shifted toward invisible, spectrum-centric operations encompassing Electronic Warfare, cyber operations, and AI-driven cognitive systems. Drone swarms, Global Navigation Satellite System (GNSS) spoofing, and electromagnetic spectrum saturation represent escalating threats demanding integrated counter-measures beyond conventional jamming. The convergence of Cyber-Electromagnetic Activities has created a new operational frontier requiring autonomous, adaptive systems capable of machine-speed decision-making. India must urgently pursue spectrum sovereignty through indigenous capability development, integrated EMSO frameworks, and AI-enabled Cognitive EW. Effective defence demands layered counter-UAS architectures encompassing both soft- and hard-kill measures, as well as resilient warfighting systems, transitioning decisively from legacy kinetic models toward algorithmic and intelligence-driven battlefield dominance.

Global Challenges

- Warfare has evolved into a contest for electromagnetic (EM) spectrum dominance, where highly connected forces with inbuilt redundancy remain vulnerable to jamming, spoofing, and cyberattacks, making connectivity both a strength and a critical liability.

- Swarms are distributed, mesh-networked, and increasingly autonomous, making them extremely difficult to counter through traditional single-point defensive measures, with GPS-denied navigation and mass saturation attacks remaining critically unsolved across all modern militaries.

- Severe electromagnetic spectrum stress is degrading radar and EW effectiveness, while a significant and growing rise in GNSS spoofing incidents have created a serious operational and strategic challenge across all modern military systems globally.

- Low-cost SDRs and open-source signal processing have made advanced EW capabilities accessible even to non-state actors, fundamentally and permanently altering the global threat landscape beyond the exclusive domain of well-funded militaries.

- Adversaries integrating EW and cyber into unified attacks, combined with AI-enabled machine-speed decision cycles, have rendered legacy jamming models and human-in-

the-loop response capacity structurally obsolete, a challenge no military in the world has yet fully resolved.

Implications for India

- India is fighting an invisible war without full preparedness. The outcome of future conflicts will favour forces that are cyber-resilient, possess robust command-and-control networks, maintain layered and resilient air defence systems encompassing both hard- and soft-kill capabilities, and exercise effective spectrum management with the ability to deny the electromagnetic (EM) spectrum to the adversary.

- India lacks unified doctrine, shared architecture, and dual-trained operators to counter this convergence. It also lacks a clearly defined roadmap for indigenous EW development, gaps in technology ownership, source codes, and electronic intelligence platforms remain critically unaddressed.

- Limited indigenous hardware and software ecosystems create dependence on vulnerable foreign technology, making operational sovereignty a key strategic vulnerability.

- Legacy jamming-centric models, as exposed in the Ukraine conflict, are insufficient against adaptive, frequency-hopping, and autonomously coordinated adversary systems.

- India currently lags significantly in High Power Microwave technology and lacks a unified Cyber Electromagnetic Activities (CEMA) doctrine, creating structural gaps in integrated cyber-EW planning.

- Traditional military structures continue to view EW as a technical support function rather than a critical operational capability, requiring urgent doctrinal transformation.

Key Recommendations by Speakers

- **Sense, Shield and Strike Framework**: EW must encompass a broader operational framework beyond spectrum dominance, built on the integrated principles of Sensors (Active & Passive), EM spectrum management and Shooters (Hard & Soft kill)

- **Electromagnetic Battlefield Management Systems (EMBS)**: Deploy functional software and AI enabled EMBS at Corps and Command levels to operationalise EMSO in its true sense.

- **Layered Counter-UAS Architecture**: Establish Vayu Raksha Ghera comprising a Detection Layer, Kinetic and Non-Kinetic Engagement Layer, and Centralised Command and Control with integrated EW management.

- **AI-Driven Cognitive EW**: Transition from static jamming models to dynamic AI-driven spectrum operations capable of real-time adaptation and machine-speed decision-making.

- **Five Pillars of Spectrum Sovereignty**: Pursue dominance through Cognitive EW, Trusted indigenous ecosystems, Multi-domain operations, Rapid innovation cycles, and Resilient warfighting architectures.

- **Directed Energy Weapons**: Future Counter-UAS systems must incorporate High Power Microwave Systems, laser-based systems, and Electromagnetic Pulse payloads to enhance the counter-UAS ability.

Future Outlook

- Adopt "Fuse Development" Model: Link trial regiments directly with R&D organisations and industry to rapidly test, improve, and field defence systems without lengthy procurement delays.

- Restructure Future Warfare Commands: Upgrade the Defence Cyber Agency into a Space & Cyber Command and modernise the Signals Corps into a joint Spectrum and Electronic Warfare Command

- Build a Five-Layer Counter-Swarm Defence Architecture: Develop integrated layers ranging from long-range kinetic interception to decentralised EW, lasers, and spectrum-denial systems against drone swarms.

- Develop AI-Driven Cognitive EW Systems: Use AI and ML for autonomous threat detection, classification, adaptation, and real-time countermeasures against evolving threats.

- Implement the “Think–Learn–Adapt–Act” Autonomous Loop: Enable machine-speed warfare by allowing systems to continuously learn from operational data and act with minimal human intervention.

- Build a unique Indian Multi-Domain Operations framework integrating land, air, maritime, cyber, space, electromagnetic, and cognitive warfare domains based on India’s strategic needs.

Suggestions by Speaker. Strategic Way forward for India, as suggested by the speakers during the Round Table Discussion is given at appendix 1.

Appendix I

S. No	Recommended Action	Ministry of Defence	Indian Defence Forces	Industry & Startups	Academia & Research
1	Fast-Track Indigenous EW Procurement	Redesign DAP to enable six-month contact-to-delivery cycles; create dedicated EW procurement fast-track channel	Define operational requirements clearly; participate in rapid prototyping trials	Commit to accelerated delivery timelines; establish dedicated EW manufacturing lines	Support prototype testing through IIT and DRDO labs
2	GNSS-Independent Navigation Development	Fund indigenous NavIC-GPS integration programme; mandate IRNSS in all defence platforms	Operationalise NavIC-GPS combined navigation across all field platforms; train operators	Develop AI-powered computer vision navigation alternatives commercially	IITs to research and prototype alternative navigation algorithms
3	GCS-Independent Drone Mesh Networking	Fund dedicated R&D programme for indigenous mesh-network drone communication	Define operational requirements for GCS-independent drone operations; conduct field trials	Develop indigenous mesh-networking protocols and autonomous drone coordination systems	Research decentralised drone communication architectures in collaboration with DRDO
4	Establish Unified CEMA Doctrine	Direct creation of unified Indian Cyber Electromagnetic Activities doctrine; establish inter-agency CEMA coordination body	Embed EW expertise within cyber agencies; integrate CEMA into joint operational planning	Contribute technical expertise to doctrine formulation	Support doctrinal development through strategic and technical research
5	Deploy Electromagnetic Battlefield Management Systems	Fund and prioritise EMBS deployment at Corps and Command levels	Operationalise software-driven EMBS at Corps and Command levels; train commanders on spectrum management	Develop indigenous EMBS software platforms	Research adaptive spectrum management algorithms for battlefield application
6	Develop AI-Driven Cognitive EW Systems	Allocate dedicated funding for AI-driven EW development; include in Defence AI roadmap	Define operational requirements for machine-speed autonomous EW systems; conduct trials	Develop AI-powered adaptive jamming systems capable of real-time frequency-agile responses	IITs and research institutions to develop foundational AI-EW algorithms and libraries
7	Build Directed Energy Weapons Capability	Prioritise HPM, laser, and EMP systems in Long Term Integrated Perspective Plan; fund DRDO programmes	Define DEW operational requirements; integrate into Counter-UAS architecture planning	Establish indigenous DEW manufacturing capability; collaborate with DRDO	Research HPM and laser technologies; support DRDO in prototype development
8	Establish Layered Counter-UAS Architecture	Fund Vayu Raksha Ghera layered Counter-UAS programme nationally	Deploy Detection, Kinetic-Non-Kinetic Engagement, and C2 layers operationally across all commands	Develop indigenous sensors, interceptors, and EW components for layered architecture	Research swarm detection algorithms and anti-swarm spectrum congestion technologies
9	Indigenous Defence Ecosystem Development	Create dedicated defence innovation fund for EW startups; expand iDEX challenges in EW domain	Actively participate in startup trials; provide operational feedback for product refinement	Establish EW-focused startup clusters; collaborate with IITs for technology transfer	Formalise academia-industry-defence collaboration frameworks for EW research
10	Change of Mindset at Command Level	Mandate EW literacy programmes for senior policymakers and strategists	Embed EW training into all command and staff courses; integrate EW into operational planning at all levels	Conduct industry awareness programmes on emerging EW operational requirements	Develop EW curriculum for military education institutions and staff colleges