ISSN 23939729

CLAWS

No. 140

2026

MANEKSHAW PAPER

Electronic Warfare in Joint Operations: Achieving Spectrum Dominance in Multi-Domain Warfare

SRR Aiyengar

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 140, 2026

Electronic Warfare in Joint Operations: Achieving Spectrum Dominance in Multi-Domain Warfare

SRR Aiyengar

Centre for Land Warfare Studies
New Delhi

Editorial Team : CLAWS

ISSN : 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone +91-11-25691308 Fax: +91-11-25692347
Email: **landwarfare@gmail.com**, website: **www.claws.co.in**
CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Published in Bharat by

Sabre & Quill Publishers, New Delhi, India
www.sabreandquill.com / sabreandquill@gmail.com

Contents

Electronic Warfare in Joint Operations: Achieving Spectrum Dominance in Multi-Domain Warfare

Abstract

The character of warfare is undergoing a profound transformation as advances in artificial intelligence (AI), cyber operations, autonomous systems, space capabilities, and information technologies reshape the conduct of military operations. At the heart of this transformation lies the electromagnetic spectrum, which has evolved from a supporting medium for communications and radar into a contested operational domain critical to success across land, maritime, air, cyber, space, and information environments. Electronic Warfare (EW), once regarded primarily as a combat support function, is increasingly emerging as a decisive enabler of Multi-Domain Operations (MDO).

This paper examines the evolving role of EW within the broader framework of MDO, highlighting the growing convergence of EW, Cyber-Electromagnetic Activities (CEMA), AI, cognitive technologies, autonomous systems, and Electromagnetic Spectrum Operations (EMSO). Drawing upon lessons from contemporary conflicts, including Ukraine, Nagorno-Karabakh, the Middle East, and recent Indian operational experiences, the paper analyses the changing nature of spectrum warfare and the increasing importance of electromagnetic superiority in determining operational outcomes.

The paper argues that future military success will depend not merely upon possessing advanced EW equipment but upon developing integrated doctrinal, organisational, technological, and human capabilities capable of achieving sustained spectrum dominance. It further examines emerging concepts such as AI-enabled Cognitive EW, adaptive spectrum management, counter-unmanned aerial systems, software-defined radios, and intelligent decision-support systems. The paper concludes by recommending a comprehensive framework for strengthening India's joint Electronic Warfare capability through doctrinal reform, organisational integration, indigenous technological innovation, enhanced professional military education, and closer integration of EW with cyber, space, intelligence, and information operations. Such an approach will be essential if India is to achieve credible spectrum dominance in future MDO.

Introduction

EW has emerged as one of the defining determinants of military effectiveness in the twenty-first century. The increasing digitisation of warfare, proliferation of sensors, widespread employment of drones, integration of cyber capabilities, and growing dependence on space-based systems have fundamentally altered the conduct of military operations. Modern armed forces communicate, navigate, detect, target, coordinate, and fight through the Electromagnetic spectrum (EMS). Consequently, they are simultaneously empowered and vulnerable through it.

The importance of controlling information in warfare has long been recognised. However, in contemporary conflicts, information is generated, transmitted, processed, and exploited primarily through the EMS. The EMS therefore constitutes the invisible foundation upon which modern military power rests. Disruption of this foundation can degrade command and control, isolate formations, impair intelligence collection, reduce combat effectiveness, and ultimately influence strategic outcomes.

As General K. Sundarji, former Chief of Army Staff of the Indian Army (1986 to 1988), observed:

"*Future wars will be won by those who can control information, communications, and the electromagnetic spectrum*."

Recent conflicts have reinforced this reality. Operations in Ukraine, the Middle East, and other contemporary theatres have demonstrated that the side capable of sensing first, understanding the operational environment faster, protecting its networks, and disrupting the adversary's electromagnetic dependencies gains a significant advantage. EW is therefore no longer merely a technical support function; it has become a critical instrument of operational and strategic power.

Simultaneously, warfare is increasingly moving towards MDO, wherein military effects are generated through the integrated employment of land, maritime, air, cyber, space, and electromagnetic capabilities. In such an environment, EW acts as a force multiplier and an integrating mechanism connecting multiple domains. It contributes to decision superiority, operational tempo, survivability, and precision engagement while enabling commanders to synchronise effects across the battlespace.

For India, these developments carry particular significance. The Indian Armed Forces are progressing towards Integrated Theatre Commands, greater jointness, network-enabled operations, and indigenous defence technologies. At the same time, India faces increasingly sophisticated threats from unmanned systems, cyber-attacks, electronic intelligence capabilities, precision-guided weapons, and space-enabled surveillance networks. These realities demand a comprehensive understanding of EW as a joint operational capability rather than a specialised technical function.

This paper argues that EW has become indispensable to Joint and MDO and that spectrum superiority will increasingly influence military success in future conflicts. It further contends that India's military transformation must incorporate EW, Cyber-Electromagnetic Activities (CEMA), Cognitive EW, and Spectrum management as integral elements of operational planning, force development, and military education

I. Joint Operations and Multi-Domain Operations (MDO): The Indian Perspective

"Multi-Domain Operations seek to integrate and synchronise actions across all domains, in sync with multiple military and non-military partners."

— India's Joint Doctrine for Multi-Domain Operations (MDO)- 2025

The nature of military operations has evolved significantly from the largely service-specific campaigns of the past. Contemporary military success increasingly depends upon the coordinated employment of capabilities across multiple domains and services. This evolution has given rise to the concepts of Joint Operations and MDO, both of which seek to achieve synergy through integration rather than through the independent employment of military power.

Joint Operations involve the coordinated use of land, maritime, and air forces under unified operational objectives. Their purpose is to generate effects that exceed what individual services can achieve independently. Jointness enhances operational flexibility, optimises resource utilisation, improves responsiveness, and allows commanders to exploit complementary strengths across services.

The concept has gained renewed importance as military operations have become increasingly interconnected and technology-intensive. Modern commanders must simultaneously coordinate intelligence assets, air support, long-range fires, cyber capabilities, space-based services, logistics networks, and information operations. Effective integration of these capabilities demands a level of joint planning and execution that transcends traditional service boundaries.

MDO represents the next stage in this evolution. Whereas Joint Operations focus primarily upon integrating military services, MDO seeks to synchronise effects across all operational domains—land, maritime, air, cyber, space, and the electromagnetic spectrum. The objective is to create multiple dilemmas for the adversary, exploit vulnerabilities across domains, and generate decision superiority.

A central feature of MDO is the recognition that warfare no longer unfolds sequentially within discrete domains. Actions in one domain immediately influence activities in others. A cyber intrusion may disrupt an air defence network; an electronic attack may enable a precision strike; a space-based sensor may support ground manoeuvre; and a drone swarm may influence both kinetic and information operations simultaneously.

The fundamental objective of MDO is to accelerate the observe–orient–decide–act (OODA) cycle while disrupting the adversary's OODA cycle. The side capable of generating superior situational awareness, making decisions faster, and coordinating effects across multiple domains gains a significant operational advantage.

EW plays a pivotal role in this process. Every operational domain relies extensively upon the electromagnetic spectrum for communications, sensing, navigation, targeting, and command and control. EW therefore acts as a critical enabler of multi-domain integration by protecting friendly access to the spectrum while denying the same to adversaries.

For India, the movement towards Integrated Theatre Commands reflects recognition of these realities. Future Indian military operations are likely to involve simultaneous employment of land, maritime, air, cyber, and space capabilities across multiple theatres. Such operations will require resilient communications, protected networks, integrated intelligence systems, and effective electromagnetic battle management. Consequently, EW must be viewed not as an isolated technical discipline but as an essential component of joint operational effectiveness.

II. EMS as an Operational Battlespace

The EMS has become one of the most strategically significant operational environments in modern warfare. Unlike physical terrain, the spectrum is invisible, dynamic, and shared by military and civilian users. Yet it supports virtually every aspect of contemporary military activity.

Communications systems, radars, navigation aids, satellite links, data networks, intelligence sensors, missile guidance systems, unmanned platforms, and command-and-control architectures all rely upon electromagnetic emissions. Consequently, the spectrum has emerged as a critical enabler of military power and a primary target for adversary action.

Historically, military planners viewed the spectrum largely as a technical resource supporting communications and radar operations. Today, however, it is increasingly recognised as operational terrain that must be contested, defended, exploited, and managed. Control of the spectrum can significantly influence battlefield awareness, command effectiveness, operational tempo, and combat outcomes.

The operational importance of the EMS arises from several factors.

Enhanced Situational Awareness

Modern military forces depend heavily upon sensors operating across multiple portions of the spectrum. Radar systems, electronic support measures, communication intercept platforms, satellite sensors, and unmanned aerial systems collectively generate the intelligence required for informed decision-making.

The side capable of sensing first and understanding the operational environment faster gains a substantial advantage. Access to the spectrum therefore directly influences situational awareness and battlefield transparency.

Accelerated Decision Cycles

Information superiority depends upon the ability to collect, process, disseminate, and exploit information rapidly. Communications networks and data links operating within the EMS enable commanders to coordinate forces, distribute intelligence, and respond to emerging threats.

John Boyd's concept of the OODA loop remains particularly relevant in this context. The force capable of cycling through observation, orientation, decision, and action more rapidly than its adversary can impose operational dilemmas and seize the initiative.

Precision Engagement

Modern precision-guided weapons rely extensively upon electromagnetic systems for navigation, targeting, and guidance. Satellite navigation, radar seekers, data links, and sensor fusion architectures all depend upon spectrum access.

Spectrum superiority therefore contributes directly to the effectiveness of precision strike capabilities while enabling the disruption of adversary targeting systems.

Command and Control Resilience

Military effectiveness depends upon the ability of commanders to communicate, coordinate, and direct forces under combat conditions. Communications networks form the nervous system of modern military organisations.

Adversaries increasingly seek to disrupt these networks through jamming, spoofing, cyber-attacks, and electromagnetic interference. The protection of spectrum-dependent command-and-control systems has therefore become a central requirement for operational resilience.

Logistics and Sustainment

Modern logistics systems depend upon digital tracking, satellite communications, automated inventory management, and network-enabled coordination. Sustaining military operations increasingly requires uninterrupted access to the spectrum.

In prolonged campaigns, the ability to maintain reliable communications and information flows may prove as important as the availability of ammunition, fuel, or transportation assets.

Disruption of Adversary Operations

Electronic attack capabilities allow military forces to degrade, deceive, disrupt, or deny adversary use of the spectrum. Communications jamming, radar deception, navigation spoofing, and electromagnetic attack can generate operational effects without necessarily resorting to kinetic action.

Such capabilities offer commanders scalable and reversible response options while creating opportunities for manoeuvre, deception, and precision engagement.

Conversely, loss of spectrum access can produce confusion, isolation, degraded coordination, reduced morale, and operational paralysis. Forces unable to communicate, navigate, or understand the battlespace may suffer severe degradation even in the absence of significant physical destruction.

The EMS must therefore be regarded as a contested operational environment requiring continuous monitoring, protection, and management. In contemporary warfare, spectrum superiority increasingly underpins information superiority, decision superiority, and ultimately combat effectiveness.

Challenges in Achieving Spectrum Dominance

While the importance of the electromagnetic spectrum is widely acknowledged, achieving and sustaining spectrum dominance remains an increasingly complex challenge. Unlike traditional physical domains, the electromagnetic spectrum is finite, shared, dynamic, and continuously contested. The rapid proliferation of military and civilian emitters has created unprecedented levels of spectrum congestion, particularly in urbanised and technologically advanced environments.

A major challenge arises from the increasing sophistication of adversary electronic capabilities. Modern military forces employ frequency-agile radios, low probability of intercept (LPI) radars, adaptive waveforms, mesh networks, and autonomous systems specifically designed to reduce vulnerability to traditional Electronic Attack measures. The widespread adoption of software-defined radios and cognitive communication systems further complicates detection and exploitation.

The growing dependence on satellite communications, GPS-based navigation, and network-centric operations has simultaneously expanded the attack surface available to adversaries. Jamming, spoofing, cyber intrusion, and electromagnetic deception can produce operational effects disproportionate to the resources employed. The conflict in Ukraine has repeatedly demonstrated how relatively inexpensive electronic systems can disrupt communications, navigation, and drone operations over extensive areas.

Another challenge lies in balancing offensive and defensive spectrum operations. Excessive use of jamming may interfere with friendly systems, create electromagnetic fratricide, or reveal the location of friendly emitters. Achieving the correct balance between spectrum exploitation, protection, and attack requires sophisticated planning, coordination, and electromagnetic battle management.

Future spectrum dominance will therefore depend not merely upon possessing superior technology, but upon achieving organisational agility, dynamic spectrum management, resilient communications architectures, and the ability to adapt faster than an adversary in a continuously evolving electromagnetic environment. As military operations become increasingly dependent upon spectrum-enabled capabilities, the pursuit of spectrum dominance is emerging as a central objective of modern warfare.

Spectrum Dominance: The Operational Objective

The growing importance of the electromagnetic spectrum has given rise to the concept of Spectrum Dominance, which may be broadly defined as the ability to secure sufficient freedom of action within the electromagnetic spectrum for friendly forces while simultaneously denying, degrading, disrupting, deceiving, or exploiting an adversary's use of the spectrum.

Spectrum Dominance extends beyond the traditional objectives of EW. It encompasses not only Electronic Support, Electronic Attack, and Electronic Protection, but also spectrum management, cyber-electromagnetic integration, space-enabled capabilities, intelligence collection, communications resilience, and information superiority. In contemporary operations, spectrum dominance is achieved not through the complete denial of adversary spectrum access, which may often be impractical, but through the ability to gain and sustain a decisive operational advantage within the electromagnetic environment at critical times and places.

The concept may be viewed as analogous to air superiority in the air domain or sea control in the maritime domain. Just as military forces seek freedom of manoeuvre in physical domains, they increasingly seek freedom of action within the electromagnetic domain. The side capable of sensing first, communicating securely, protecting its networks, disrupting adversary systems, and adapting rapidly to changing spectrum conditions is likely to gain significant operational and decision-making advantages.

In the context of Joint and MDO, spectrum dominance serves as a foundational enabler of information superiority and decision superiority. Without effective control and exploitation of the electromagnetic environment, the ability to integrate effects across land, maritime, air, cyber, and space domains may be severely constrained.

It is therefore increasingly appropriate to regard spectrum dominance not merely as a technical objective of Electronic Warfare but as a strategic prerequisite for success in modern warfare.

III. EW-Foundations for Spectrum Dominance

EW encompasses military actions undertaken to exploit, control, protect, and deny the use of the electromagnetic spectrum. Although technological developments have transformed the character of EW, its conceptual foundations continue to rest upon three interrelated functions: Electronic Support (ES), Electronic Attack (EA), and Electronic Protection (EP). Together, these functions provide the framework through which military forces seek to achieve spectrum superiority and operational advantage.

While conceptually distinct, these functions increasingly overlap within modern operations. The rapid pace of warfare, proliferation of sensors, and integration of cyber and information capabilities have blurred traditional boundaries, requiring commanders to view EW as a continuous and integrated operational activity rather than a collection of isolated technical tasks.

Electronic Support (ES)

ES constitutes the intelligence backbone of EW. It involves the interception, detection, identification, analysis, geo-location, and exploitation of electromagnetic emissions in order to provide information concerning adversary capabilities, intentions, and dispositions.

Modern military forces emit a vast range of electromagnetic signatures through radars, communication systems, navigation aids, data links, electronic sensors, and unmanned systems. These emissions create opportunities for detection and analysis. ES systems exploit such signatures to develop situational awareness and generate actionable intelligence.

The value of ES extends beyond traditional intelligence collection. Contemporary battlefield commanders increasingly require real-time awareness of hostile emitters, drone-control stations, missile batteries, air defence systems, communication nodes, and electronic surveillance assets. Tactical ES capabilities therefore contribute directly to battlefield transparency and operational decision-making.

In recent conflicts, ES has often provided the first indication of adversary activity. Detection of radar activation, communications surges, or drone-control transmissions can reveal enemy intentions long before physical contact occurs. Consequently, ES plays a vital role in enabling early warning, targeting, force protection, and operational planning.

The growing importance of ES reflects a broader reality of modern warfare: the side that can sense first, understand faster, and exploit information more effectively gains a decisive advantage.

Electronic Attack (EA)

EA encompasses actions undertaken to degrade, disrupt, deceive, manipulate, or neutralise adversary capabilities through electromagnetic means. Its purpose is to deny the enemy effective use of the spectrum while preserving freedom of action for friendly forces.

Traditional EA activities focused largely upon jamming communications and radar systems. Contemporary EA, however, has expanded significantly in scope and sophistication. Modern systems can disrupt command networks, deceive sensors, spoof navigation systems, manipulate data flows, interfere with drone operations, and create false operational pictures.

One of the principal advantages of EA is its ability to generate operational effects without necessarily resorting to kinetic destruction. A radar system may be blinded rather than destroyed. A communication network may be disrupted rather than physically attacked. A drone may be diverted from its intended mission through spoofing rather than shot down.

Such effects provide commanders with flexible response options and enhanced escalation control. Because many EA effects are reversible, they offer opportunities to shape the battlespace while limiting collateral damage and preserving strategic flexibility.

Recent conflicts have demonstrated that EA can significantly influence operational outcomes. Communications jamming, GPS denial, drone disruption, and radar deception have become routine features of contemporary military operations. The increasing dependence of modern militaries upon networked systems has simultaneously increased the potential effectiveness of EA.

Electronic Protection (EP)

EP comprises those measures designed to ensure that friendly forces can continue operating effectively despite adversary attempts to disrupt spectrum-dependent systems.

Modern military effectiveness depends heavily upon communications networks, navigation systems, surveillance sensors, data links, and command-and-control architectures. Adversaries therefore seek to target these systems through jamming, spoofing, electromagnetic interference, cyber-attacks, and other forms of disruption.

EP seeks to mitigate such vulnerabilities through a combination of technological, procedural, and operational measures. These include frequency agility, anti-jam communications, hardened networks, emission control procedures, electromagnetic shielding, protected wave forms, navigation resilience measures, and spectrum management practices.

The importance of EP continues to increase as military operations become more network-centric. In many respects, preserving spectrum access is becoming as important as protecting physical infrastructure. A force that loses communications, navigation, or situational awareness may become operationally paralysed even if its physical assets remain intact.

EP should therefore be viewed not merely as a technical responsibility but as a fundamental component of combat survivability. Future military success will depend as much upon preserving electromagnetic coherence as upon protecting physical platforms and infrastructure.

The traditional ES-EA-EP construct remains conceptually valid and continues to provide an essential doctrinal foundation. However, the increasing complexity of modern warfare has highlighted certain limitations in its operational application.

The ES-EA-EP framework primarily describes functions performed by EW specialists. Commanders, however, increasingly require a more operationally focused perspective that links spectrum activities directly to battlefield outcomes. This requirement has given rise to the Sense–Strike-Shield (S3) construct.

The **Sense** component encompasses the detection, collection, fusion, analysis, and dissemination of information derived from electromagnetic, cyber, space-based, and other sensor systems. Its purpose is to generate a comprehensive understanding of the operational environment and support decision superiority.

The **Strike** component integrates both kinetic and non-kinetic effects. These may include jamming, spoofing, deception, cyber actions, directed-energy effects, precision fires, counter-drone systems, and other capabilities designed to disrupt, degrade, or destroy adversary combat potential.

The **Shield** component extends beyond traditional EP. It includes spectrum management, network resilience, cyber protection, electromagnetic hardening, deception measures, anti-jam communications, and operational procedures designed to preserve combat effectiveness under contested conditions

The Sense–Strike-Shield construct is particularly relevant to Joint and MDO because it aligns more closely with the manner in which commanders perceive and employ military capabilities. Rather than focusing upon technical functions, it emphasises operational outcomes and integrated effects.

At a strategic level, the S3 construct reflects an important shift in military thinking. EW is no longer viewed merely as a specialist capability supporting combat operations. Instead, it is increasingly recognised as a core component of sensing, protecting, and striking within a contested and interconnected battlespace.

IV. EW-The Integrator of Joint Operations

The effectiveness of Joint Operations depends fundamentally upon the ability to integrate diverse military capabilities into a coherent and mutually supporting operational framework. EW plays a central role in achieving this integration because every operational domain relies extensively upon the electromagnetic spectrum.

Communications, intelligence systems, navigation networks, surveillance platforms, targeting architectures, and command-and-control structures all depend upon access to the EMS. Consequently, EW functions as the connective tissue linking military activities across land, maritime, air, cyber, space, and special operations domains.

Land Forces

Modern land operations occur within increasingly transparent and contested battle spaces. Ground formations face persistent observation from drones, satellites, radar systems, electronic sensors, and communication intercept platforms.

EW provides land forces with the means to detect hostile emitters, protect friendly communications, disrupt adversary networks, and counter unmanned systems. Organic EW capabilities have become particularly important at tactical levels where commanders must operate under conditions of constant surveillance and electronic contestation.

Recent conflicts have demonstrated the growing necessity of tactical EW support for counter-drone operations, force protection, artillery survivability, and battlefield awareness. The ability to identify and disrupt hostile drone-control links can significantly reduce the effectiveness of enemy reconnaissance and targeting efforts.

Air Forces

Air operations depend heavily upon electromagnetic dominance. Modern aircraft rely upon radar systems, data links, electronic countermeasures, satellite navigation, airborne early warning systems, and networked command-and-control architectures.

EW enables air forces to suppress enemy air defences, deceive hostile sensors, protect strike packages, and maintain freedom of manoeuvre within contested airspace. Increasingly, air superiority is closely linked to spectrum superiority.

Contemporary suppression of enemy air defence (SEAD) operations often combines EA, cyber effects, deception measures, and precision strikes to create windows of operational advantage. Consequently, EW has become indispensable to modern air campaigns.

Maritime Forces

Naval warfare is inherently dependent upon electromagnetic systems. Warships continuously rely upon radar, satellite communications, navigation systems, electronic surveillance equipment, and missile guidance technologies.

Maritime EW contributes to fleet protection, sea control, maritime domain awareness, and anti-missile defence. Emission control procedures reduce detectability, while electronic countermeasures enhance survivability against hostile surveillance and precision-guided weapons.

For India, maritime EW assumes particular significance within the Indo-Pacific region, where long distances, extensive sea lanes, and increasing strategic competition elevate the importance of maritime spectrum dominance.

Cyber Forces

The convergence of cyberspace and the electromagnetic spectrum have created unprecedented opportunities and vulnerabilities. Military networks increasingly depend upon wireless communications, software-defined systems, cloud architectures, and interconnected digital infrastructures.

EW and cyber operations therefore reinforce one another. ES can reveal network structures and communication patterns. Cyber capabilities can exploit information derived from spectrum monitoring. EA can isolate targets, while cyber tools exploit resulting vulnerabilities.

The integration of cyber and EW capabilities has become a central requirement for effective MDO. This aspect is being covered subsequently in the Paper

Space Support

Space-based systems underpin many of the critical capabilities required for modern warfare. Communications satellites, navigation systems, ISR platforms, missile warning systems, and timing services all contribute to military effectiveness across domains.

These systems are themselves vulnerable to jamming, spoofing, interference, and other forms of electromagnetic attack. Consequently, spectrum resilience has become an essential component of space-enabled military operations.

Protection of satellite-dependent services is increasingly critical to sustaining operational reach, command effectiveness, and decision superiority.

Space-based offensive capabilities for Anti-Space (AS) and Anti-Terrestrial Electro-Magnetic (EM) operations aim to disrupt, degrade, deceive, or deny an adversary's space and electromagnetic systems. These include satellites capable of jamming or spoofing communications, GPS, radar, and data links, as well as emerging concepts involving cyber payloads, directed-energy systems, and high-power microwave transmitters. Future AI-enabled satellite constellations could autonomously detect and neutralize hostile space assets while supporting terrestrial EM campaigns. Such capabilities offer global reach, persistence, and rapid response, but also raise concerns regarding escalation, attribution, space debris, and the long-term sustainability of the space environment.

Special Operations Forces

Special Operations Forces often operate deep within contested environments while relying upon secure communications, precision navigation, covert surveillance, and low-signature operations.

Their success depends upon maintaining connectivity without compromising concealment. Poorly coordinated spectrum activity can expose special operations teams or interfere with mission execution.

EW planning therefore plays a vital role in supporting special operations through careful spectrum management, electromagnetic de-confliction, and mission-specific protection measures.

Across all domains, a common conclusion emerges. EW is not merely another supporting function within Joint Operations. It is the mechanism that enables military forces to communicate, coordinate, sense, decide, manoeuvre, and fight effectively within an increasingly contested operational environment. In this sense, Electronic Warfare serves as the connective tissue that binds Joint and MDO into a coherent war-fighting system.

V. EW in the Era of Drones, Swarms and the Transparent Battlefield

The rapid proliferation of unmanned systems has transformed the character of modern warfare. What was once the preserve of technologically advanced militaries is now available to state and non-state actors alike. Small commercial drones, tactical unmanned aerial systems (UAS), loitering munitions, autonomous platforms, and increasingly sophisticated drone swarms have become ubiquitous across contemporary battlefields. Their widespread availability, relatively low cost, and operational effectiveness have fundamentally altered the relationship between surveillance, targeting, and strike operations.

Perhaps the most significant consequence of this transformation is the emergence of the "transparent battlefield." Persistent surveillance from drones, satellites, electronic sensors, and networked intelligence systems has made it increasingly difficult for military forces to conceal movements, concentrations, logistics nodes, headquarters, and weapon systems. The traditional advantages of surprise, concealment, and manoeuvre are becoming progressively more difficult to achieve.

In this environment, EW has emerged as one of the most effective means of countering unmanned systems and preserving operational freedom of action. Unlike kinetic solutions, which may be expensive and unsustainable against large numbers of drones, EW offers scalable, non-kinetic, and often reversible options for disrupting adversary operations.

Counter-UAS Operations and EW

Modern drones depend heavily upon the electromagnetic spectrum. Communications links connect drones to operators. Navigation systems rely on satellite signals. Data links transmit intelligence and targeting information. Sensors employ electromagnetic emissions to detect and track targets. These dependencies create opportunities for EW.

An effective Counter-UAS framework generally involves four interrelated functions:

Detection. ES systems detect and identify drone-control signals, telemetry transmissions, navigation emissions, and other electromagnetic signatures.

Classification. Advanced sensors and signal analysis tools determine drone type, capabilities, operating frequencies, and threat level.

Decision. Information from multiple sensors is fused to support rapid command decisions.

Action. EA systems jam, spoof, deceive, disrupt, or take control of hostile drones, while kinetic systems remain available against more resilient threats.

This detect–classify–decide–act cycle illustrates how EW has become central to modern Counter-UAS operations.

Particularly significant is the growing use of navigation spoofing and communication disruption. Rather than physically destroying a drone, operators may induce it to land, return to its launch point, or deviate from its intended mission. Such approaches provide cost-effective responses to increasingly numerous drone threats.

Swarm Warfare and Emerging Challenges

Drone swarms represent the next stage in unmanned warfare. Unlike individual platforms, swarms employ large numbers of autonomous or semi-autonomous systems operating cooperatively to achieve common objectives.

The military advantages of swarms are substantial. They can saturate defences, overwhelm sensors, complicate targeting decisions, and generate multiple simultaneous threats. Their distributed nature reduces vulnerability to the loss of individual platforms while increasing operational resilience.

From an EW perspective, swarms present both opportunities and challenges. Military forces must prioritise a counter to drone swarming tactics with which inexpensive, mass-produced drones can overwhelm defences. What is needed is a layered defensive system that includes systems that can neutralise many threats within seconds. One such solution is now becoming available: the contemporary high-energy, high-power microwave (HPM) weapon.

HPM weapons work by emitting directed bursts of electromagnetic energy, disabling the electronics of drones in mid-flight. In the most basic sense, they do in fact work rather like your microwave oven at home and even use similar radio-energy frequencies, but they act over hundreds, or low thousands, of metres. Unlike traditional kinetic systems, which must intercept and physically destroy each target individually, high-energy HPMs can adjust their beam to incapacitate massive swarms of drones in a single engagement.

On one hand, swarm coordination frequently depends upon communications networks, navigation signals, and data exchange, creating potential vulnerabilities that can be exploited through EW measures.

On the other hand, future swarms may employ adaptive communications, artificial intelligence, distributed decision-making, and autonomous navigation systems that reduce reliance on traditional control links. Such developments may significantly complicate conventional jamming approaches.

Consequently, future counter-swarm operations are likely to require integrated solutions combining EW, cyber capabilities, artificial intelligence, directed-energy weapons, kinetic interceptors, and advanced command-and-control systems.

Beyond technological advances, tactics are evolving rapidly. The war in Ukraine has demonstrated a brisk cycle of countermeasures and counter-countermeasures. Battlefield adaptations are happening in weeks rather than years. For example, recent adaptations to counter the protection afforded by jammers include the use of drones enabled by artificial intelligence and drones flown by fibre-optic cable.

But HPM is not a silver bullet. It must be integrated into a layered approach that combines kinetic, electronic warfare and directed energy systems to maximise the adaptability of defences against evolving threats.

Maintaining an edge in counter-drone technology is not optional; it is imperative. Because failure to adapt to these rapid changes will leave military forces dangerously exposed, speed in acquiring, deploying and adapting counter-drone capabilities is now critical.

Alongside the DRDO-developed D4 *(Drone Detect, Deter, Destroy*) system, India's anti-drone capabilities have rapidly expanded to counter modern battlefield threats. These include *Bhargavastra* (developed by Indian private sector), *Saksham* and *Adani Vehicle-Mounted System.*

Spectrum Congestion and Electromagnetic Complexity

The increasing number of unmanned systems operating within confined battlespaces has created new challenges in spectrum management. Modern military operations involve thousands of emitters, including radios, radars, navigation systems, drones, electronic support systems, jammers, sensors, and civilian communications networks.

The result is a highly congested and contested electromagnetic environment.

Excessive electromagnetic activity can generate mutual interference, reduce system effectiveness, and increase the risk of fratricide. Poorly coordinated EA measures may inadvertently disrupt friendly communications or interfere with civilian infrastructure.

Effective spectrum management therefore becomes a critical operational requirement. Commanders must balance offensive and defensive EW activities while ensuring uninterrupted support to friendly operations.

The future battlespace will increasingly require dynamic spectrum management systems capable of allocating frequencies, prioritising users, mitigating interference, and adapting to rapidly changing operational conditions.

Lessons from Contemporary Conflicts

Recent conflicts provide important insights into the evolving role of EW in drone-centric warfare.

Ukraine

The conflict in Ukraine has demonstrated the pervasive influence of EW on modern military operations. Both sides have employed extensive jamming, communications disruption, navigation denial, drone interception, and electronic intelligence collection. The conflict has illustrated that drones and EW exist in a continuous cycle of adaptation, with each side seeking to overcome the countermeasures of the other.

One of the most significant lessons from Ukraine is that spectrum superiority often proves as important as firepower. Forces unable to protect communications, navigation systems, and drone networks rapidly lose situational awareness and operational effectiveness.

Nagorno-Karabakh

The conflict between Armenia and Azerbaijan highlighted the devastating effectiveness of integrating drones, precision weapons, intelligence systems, and EW. Electronic suppression of air-defence systems created opportunities for unmanned platforms to conduct reconnaissance and strike operations with considerable effectiveness.

The conflict demonstrated the importance of integrating EW into broader operational designs rather than employing it as an isolated capability.

Middle East Operations

Recent operations involving missile and drone threats in the Middle East have highlighted the growing importance of integrated electronic defence systems. Naval forces have relied heavily upon electronic surveillance, jamming, deception, and electromagnetic protection measures to counter increasingly sophisticated threats.

These operations underscore the continuing relevance of EW in maritime security and power projection.

Operation Sindoor and the Indian Context

Emerging lessons from Operation Sindoor reinforce the growing significance of EW in contemporary Indian military operations. The ability to preserve communications, protect networks, counter unmanned threats, and maintain command coherence under contested electromagnetic conditions has become increasingly important.

These experiences underline a broader lesson: EW is no longer a specialised support function. It has become an operational necessity directly influencing mission success, force protection, and decision superiority.

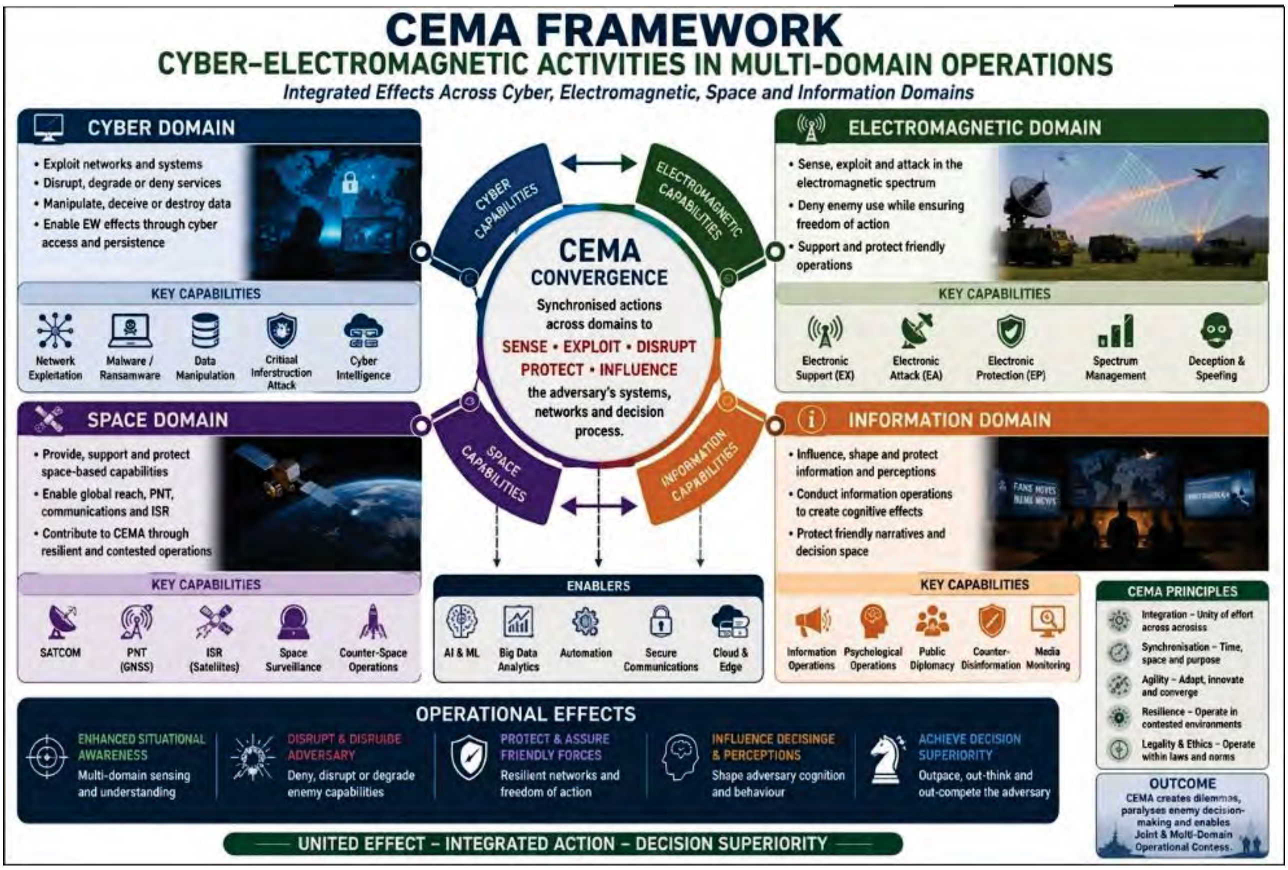
The proliferation of drones, loitering munitions, autonomous systems, and persistent surveillance platforms suggests that future battlefields will become even more transparent and electronically contested. Success in such environments will increasingly depend upon the ability to dominate the electromagnetic dimension of warfare.

VI. Cyber-Electromagnetic Convergence and the Emergence of CEMA

The traditional concept of EW has expanded into the broader framework of Electromagnetic Spectrum Operations (EMSO), recognizing the electromagnetic spectrum as a contested operational domain rather than merely a medium supporting military operation. EMSO integrates EW, cyber operations, spectrum management, electromagnetic battle management, intelligence, and space capabilities, providing the conceptual foundation for Cyber-Electromagnetic Activities (CEMA) and multi-domain operations.

The traditional separation between cyberspace operations and EW is rapidly disappearing. Modern military networks rely upon wireless communications, software-defined architectures, cloud-based services, satellite links, and interconnected digital systems that operate through the electromagnetic spectrum. Consequently, actions within cyberspace increasingly influence activities within the electromagnetic domain and vice versa.

This convergence has given rise to the concept of CEMA, which seeks to integrate cyber operations, EW spectrum management, and information-related capabilities into a unified operational framework.



The emergence of CEMA reflects a fundamental reality of contemporary warfare: adversaries no longer distinguish clearly between cyber and electromagnetic targets. Communications networks, command systems, sensors, satellites, data centres, and autonomous platforms exist within a connected operational ecosystem. Attacks against one element frequently produce cascading effects across multiple domains.

Effective CEMA demands close integration between military capabilities and national civilian infrastructure. As critical communication networks, cloud computing, satellite services, AI platforms, and cyber infrastructure are predominantly owned or operated by the civil sector, success in future conflicts will depend on seamless coordination among the armed forces, government agencies, intelligence organizations, technology companies, telecom providers, and academia. Establishing resilient public–

private partnerships, shared situational awareness, and unified command mechanisms will be essential to ensure spectrum dominance, cyber resilience, and rapid response across the electromagnetic battlespace.

The Logic of Cyber-Electromagnetic Integration

Cyber operations and EW possess complementary strengths.ES capabilities can identify adversary emitters, map communication networks, and reveal operational patterns. This information may subsequently support cyber exploitation. EA can disrupt communications, isolate targets, or create vulnerabilities that facilitate cyber operations. Conversely, cyber capabilities can manipulate data, compromise software, alter system behaviour, and enhance the effectiveness of electronic attack measures. When employed together, cyber and EW capabilities can generate effects that neither capability could achieve independently.

The convergence of these capabilities significantly expands the range of options available to commanders while increasing the complexity faced by adversaries.

CEMA and MDO

The growing importance of MDO has accelerated interest in CEMA. Modern military commanders increasingly require the ability to coordinate effects across cyber, electromagnetic, space, information, and physical domains.

CEMA provides a mechanism for achieving such integration.

By combining EW, cyberspace operations, spectrum management, and information activities within a unified framework, commanders can generate synchronised effects that support decision superiority and operational tempo.

The objective is not merely to attack adversary systems but to influence how adversaries perceive, decide, communicate, coordinate, and act.

In this sense, CEMA contributes directly to the broader goal of shaping the adversary's decision-making process.

Operational Benefits of CEMA

Integrated Cyber–Electromagnetic Capability	Operational Advantage	Military Impact
Shared Intelligence and Sensor Fusion	Enhanced situational awareness through integrated collection and analysis of cyber and electromagnetic data	Provides a comprehensive operational picture, enabling faster and more accurate decision-making
Integrated Cyber–Electromagnetic Intelligence	Improved target identification, prioritisation, and engagement	Enables precision targeting while reducing collateral effects and increasing mission effectiveness
Multi-Domain Attack Options	Greater operational flexibility by synchronising cyber and EW effects	Allows commanders to choose the most effective means of disrupting, degrading, deceiving, or denying adversary capabilities
Coordinated Defensive Measures	Increased resilience through integrated cyber defence and electromagnetic protection	Enhances survivability of networks, communications, sensors, and command systems against complex attacks

Integrated Cyber–Electromagnetic Capability	**Operational Advantage**	**Military Impact**
Integrated Spectrum Management	More effective allocation, monitoring, and protection of the electromagnetic spectrum	Maximises spectrum availability, reduces interference, and ensures uninterrupted mission-critical communications
AI-Enabled Decision Support	Faster decision cycles and improved command effectiveness	Accelerates the Observe–Orient–Decide–Act (OODA) loop, enabling commanders to exploit fleeting opportunities
Cross-Domain Synchronisation	Greater ability to create operational dilemmas for adversaries	Simultaneously challenges adversaries across cyber and electromagnetic domains, complicating their decision-making and increasing operational uncertainty

Table 1: Operational Advantages of Integrating Cyber and Electromagnetic Capabilities

These advantages explain why major military powers increasingly regard CEMA as a critical component of future warfare.

Relevance for India

For India, the growing convergence of cyber and electromagnetic operations has important implications. Future military operations are likely to occur within highly contested information environments characterised by sophisticated cyber threats, electronic attacks, autonomous systems, and space-enabled capabilities.

The transition towards Integrated Theatre Commands, network-centric warfare, and MOD will require corresponding advances in cyber-electromagnetic integration.

This will necessitate the development of integrated doctrines, joint command arrangements, common operational procedures, shared intelligence architectures, and indigenous technological capabilities.

Most importantly, it will require a cultural shift that recognises cyberspace and the electromagnetic spectrum not as separate technical domains but as interconnected dimensions of modern warfare.

As military operations become increasingly information-centric, the ability to integrate cyber and electromagnetic effects into a coherent operational framework will become a decisive determinant of combat effectiveness. CEMA therefore represents not merely an organisational innovation but a fundamental evolution in the conduct of warfare.

Barriers to Effective CEMA Integration

Although the logic of CEMA appears compelling, practical implementation remains challenging. Most military organisations continue to manage Cyber operations, EW, Spectrum management, Intelligence, and Information operations through separate organisational structures. These institutional boundaries often inhibit information sharing, coordinated planning, and unified execution.

Differences in doctrine, command relationships, operational culture, and technical architectures can further complicate integration efforts. Cyber operators frequently focus on networks, software vulnerabilities, and data exploitation, whereas EW specialists concentrate on spectrum access, emitters, and electromagnetic effects. Bridging these differing professional perspectives requires deliberate doctrinal development and sustained joint training.

The problem is compounded by differing operational timelines. Electronic effects may be generated within seconds, whereas cyber operations often require prolonged preparation and intelligence collection. Effective synchronisation therefore demands common planning mechanisms and integrated command structures.

A further challenge involves legal authorities and escalation management. Certain cyber-electromagnetic actions may affect civilian infrastructure, critical information systems, or dual-use networks, creating strategic and political implications that extend beyond the tactical battlespace.

Consequently, successful implementation of CEMA requires more than technological integration. It demands organisational adaptation, common doctrine, shared situational awareness, and an institutional culture that recognises cyberspace and the electromagnetic spectrum as interconnected operational domains.

VII. AI-Driven Cognitive EW

The emergence of AI is transforming EW from a largely reactive and platform-centric discipline into a dynamic, adaptive, and intelligence-driven warfighting capability. Modern military operations generate enormous volumes of data from radars, communications networks, intelligence sensors, cyber systems, satellites, unmanned platforms, and open-source information. The sheer volume, velocity, and complexity of this data increasingly exceed the capacity of human operators to process and exploit in real time.

Cognitive Electronic Warfare (Cognitive EW) seeks to address this challenge by integrating AI, machine learning, advanced analytics, and automation into the conduct of spectrum operations. Unlike conventional EW systems, which typically operate using pre-programmed responses and predefined threat libraries, Cognitive EW systems possess the ability to learn, adapt, and respond dynamically to changing operational conditions.

The significance of this transformation extends beyond technological innovation. It represents a fundamental shift in the relationship between information, decision-making, and military power. Future conflicts are likely to be characterised by rapidly evolving threats, autonomous systems, contested communications, and compressed decision cycles. In such an environment, the ability to sense, understand, decide, and act faster than an adversary may prove decisive.

The defining characteristic of future warfare will be the capacity to learn and adapt faster than the adversary in an increasingly dynamic operational environment. Cognitive Electronic Warfare represents this paradigm by continuously analysing the electromagnetic spectrum, learning from evolving threats, and autonomously adapting its responses to maintain spectrum superiority and operational advantage.

From Conventional EW to Cognitive EW

Traditional EW systems are generally designed around known threats and predefined responses. Threat libraries are developed in advance, and operators employ established techniques to detect, identify, and counter hostile systems.

While highly effective against known adversaries, such approaches may be less effective against adaptive opponents employing novel waveforms, agile communications, autonomous systems, and rapidly changing tactics.

Cognitive EW seeks to overcome these limitations by employing artificial intelligence and machine learning algorithms capable of recognising patterns, identifying anomalies, and generating adaptive responses in near real time.

The comparison can be presented in the following table:

Aspect	Conventional Electronic Warfare (EW)	Cognitive Electronic Warfare (Cognitive EW)
Operational Approach	Rule-based responses	Adaptive, context-aware responses
Threat Handling	Relies on known threat libraries	Learns from experience and evolving threat patterns
Decision-Making	Human-intensive decision-making	AI-assisted decision support with human oversight
Operational Posture	Reactive in nature	Predictive and proactive
Architecture	Platform-centric	Network-centric and collaborative
Adaptability	Limited adaptation to new threats	Continuous learning and self-improvement
Spectrum Management	Static spectrum management	Dynamic spectrum optimisation and real-time spectrum agility

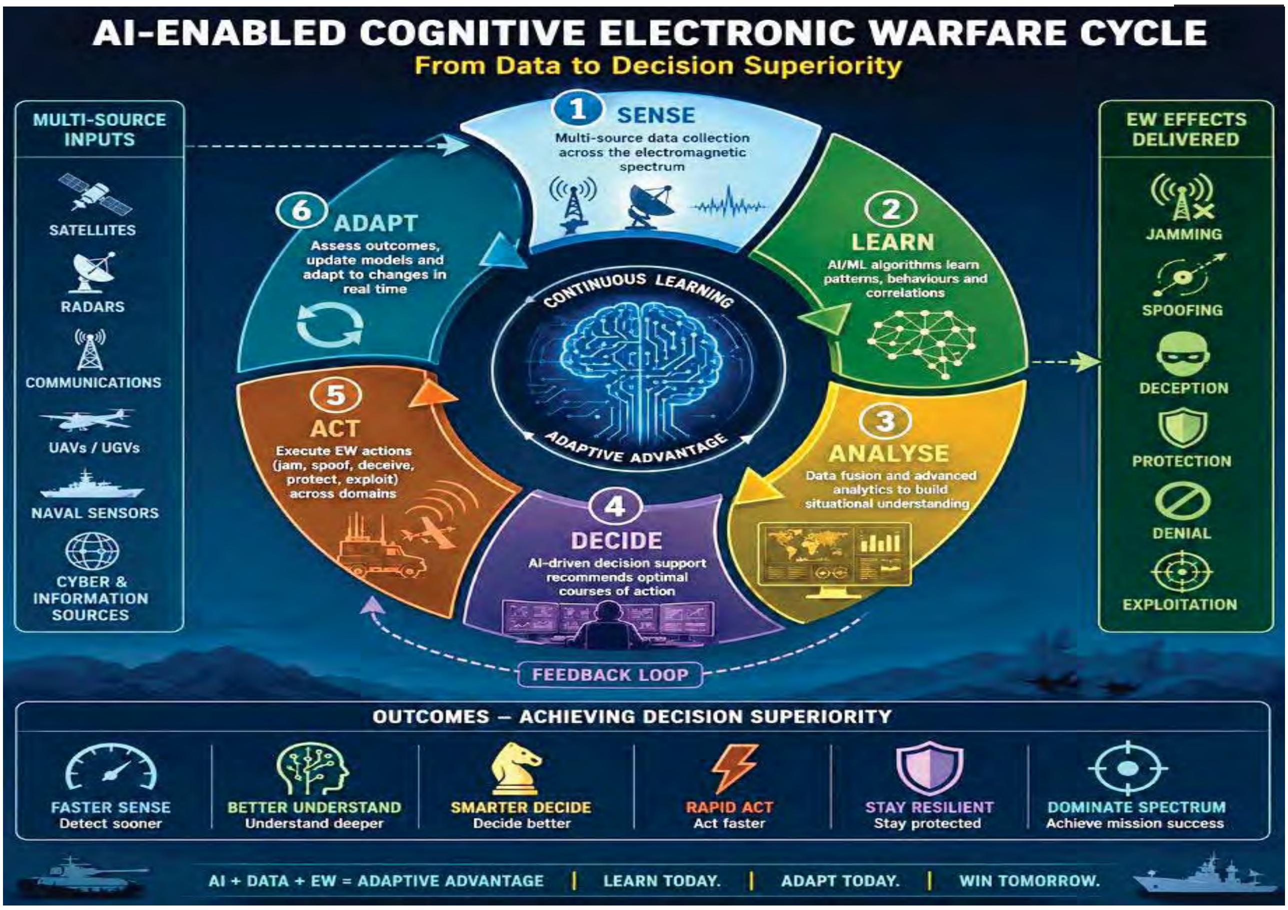
Table 2: Conventional Electronic Warfare versus Cognitive Electronic Warfare

The transition from conventional to Cognitive EW therefore mirrors the broader evolution of warfare from platform-centric operations to information-centric and decision-centric warfare.

The Cognitive EW Cycle

At the heart of Cognitive EW lies a continuous learning and adaptation cycle. This process may be described as:

Sense → Learn → Analyse → Decide → Act → Adapt



Sense

The first stage involves collecting information from a wide range of sources, including radar emissions, communications signals, cyber networks, satellite systems, unmanned platforms, and intelligence databases. Advanced sensors and ES systems continuously monitor the electromagnetic environment and generate large volumes of data.

Learn

Machine learning algorithms analyse collected information to identify patterns, correlations, and emerging threats. Unlike traditional systems that rely solely on predefined threat databases, Cognitive EW systems can recognise previously unseen behaviours and adapt accordingly.

Analyse

AI-enabled analytics fuse information from multiple sources to develop a comprehensive understanding of the operational environment. This process enhances situational awareness and supports more informed decision-making.

Decide

Decision-support systems evaluate available options and recommend courses of action. Depending upon operational requirements and rules of engagement, human operators may remain within the decision loop or supervise automated responses.

Act

The selected response may involve EA, spectrum reallocation, communications protection, cyber actions, deception measures, or other operational effects.

Adapt

The outcome of each action is continuously evaluated. Lessons learned are incorporated into future responses, allowing the system to improve performance over time. This continuous learning cycle enables Cognitive EW systems to operate effectively within rapidly changing and highly contested electromagnetic environments.

AI and Spectrum Superiority

The increasing complexity of the electromagnetic environment has made traditional spectrum management approaches increasingly inadequate. Modern military operations involve thousands of emitters competing for access to finite spectrum resources.

AI offers significant opportunities to optimise spectrum utilisation. AI-enabled systems can:

- Detect emerging interference patterns.
- Predict spectrum congestion.
- Recommend frequency allocations.
- Optimise electromagnetic emissions.
- Identify adversary vulnerabilities.
- Support dynamic spectrum management.
- Improve communications resilience.

These capabilities contribute directly to spectrum superiority by ensuring efficient utilisation of available resources while reducing vulnerability to adversary actions.

Future military operations may increasingly rely upon AI-enabled spectrum management systems capable of autonomously allocating frequencies, prioritising users, mitigating interference, and adapting to operational requirements in real time.

Cognitive EW and Decision Superiority

One of the most important contributions of Cognitive EW lies in its ability to support decision superiority.

Modern warfare increasingly involves competition between opposing decision cycles. Commanders who can understand situations faster, anticipate developments more accurately, and coordinate responses more effectively gain a significant operational advantage.

AI-enabled EW contributes to decision superiority by:

- Accelerating intelligence processing.
- Reducing information overload.
- Improving situational awareness.
- Enhancing threat identification.
- Supporting predictive analysis.
- Facilitating faster response times.

The result is an enhanced ability to operate inside an adversary's decision cycle and create operational dilemmas that disrupt planning and execution.

In many respects, Cognitive EW represents the practical application of John Boyd's OODA-loop concept within the electromagnetic domain.

Cognitive EW and Cognitive Warfare

EW and Cognitive Warfare represent two interconnected dimensions of modern conflict. EW seeks control of the electromagnetic spectrum, while Cognitive Warfare seeks influence over human cognition and decision-making. Together, they form a powerful framework for achieving information and decision superiority.

For India, the challenge is not merely technological but strategic. Building indigenous AI-enabled EW capabilities, strengthening cyber and information resilience, fostering jointness among the Services, and developing expertise in cognitive operations will be essential. Future wars may be won not only by those who possess superior weapons, but by those who can best control the spectrum, shape perceptions, and dominate the decision-making process of their adversaries.

The implications of Cognitive EW extend beyond traditional spectrum operations. Increasingly, military thinkers are examining its relationship with the broader concept of Cognitive Warfare. Whereas conventional EW seeks to influence systems, Cognitive Warfare seeks to influence human perception, understanding, judgement, and decision-making. The two concepts are becoming increasingly interconnected.

EW can shape the information available to commanders. AI can influence how information is prioritised and interpreted. Information operations can shape perceptions. Cyber operations can manipulate data. Together, these activities may influence the adversary's understanding of reality itself. Consequently, future conflicts may involve competition not only for control of the electromagnetic spectrum but also for control of information, perception, and decision-making processes. This evolution highlights the growing strategic significance of Cognitive EW within modern warfare.

Limitations and Risks of AI-Enabled Cognitive EW

Despite its transformative potential, Cognitive EW is not without limitations. AI systems are fundamentally dependent upon the quality, diversity, and reliability of the data used for training and operation. Poor-quality datasets, incomplete threat libraries, or biased learning algorithms may produce inaccurate assessments and inappropriate responses.

Adversaries may also attempt to manipulate AI systems through deception, spoofing, false signal generation, or adversarial machine learning techniques designed to corrupt algorithmic decision-making. As Cognitive EW systems become increasingly autonomous, they may themselves become attractive targets for cyber intrusion and electronic manipulation.

Another challenge concerns transparency and trust. Many advanced AI models function as "black boxes," making it difficult for operators to understand how specific decisions are reached. In high-tempo military operations, commanders may hesitate to rely fully upon recommendations that cannot be easily explained or verified.

Human-machine interaction presents an additional concern. Excessive reliance on automation may reduce operator proficiency, while insufficient trust in AI systems may negate potential operational advantages. Achieving the appropriate balance between human judgement and machine-assisted decision-making will remain a critical challenge.

Finally, AI-driven EW systems demand significant computational resources, secure data infrastructures, resilient communications, and continuous software updates. Nations unable to sustain these requirements may find it difficult to exploit the full potential of Cognitive EW.

Future success will therefore depend not only upon technological innovation but also upon robust governance, human oversight, algorithmic transparency, and resilient operational design.

Strategic Implications for Joint and MDO

The emergence of Cognitive EW has profound implications for Joint and MDO

First, it strengthens the ability of commanders to integrate effects across multiple domains by providing a more comprehensive understanding of the battlespace.

Second, it enhances interoperability between intelligence, cyber, electronic warfare, space, and kinetic capabilities.

Third, it improves resilience within contested electromagnetic environments by enabling rapid adaptation to emerging threats.

Fourth, it supports the employment of autonomous systems, drone swarms, and network-enabled operations that depend upon rapid information processing and spectrum access.

Most importantly, Cognitive EW contributes directly to the central objective of MDO-decision superiority.

The side capable of sensing first, understanding faster, deciding better, and adapting more rapidly is likely to gain a decisive operational advantage.

For India, the growing importance of AI, Integrated Theatre Commands, autonomous systems, and network-centric warfare underscores the need to develop indigenous Cognitive EW capabilities. Investments in artificial intelligence, machine learning, data analytics, software-defined systems, mission data libraries, and advanced spectrum management technologies will be essential for maintaining military effectiveness in future conflicts.

VIII. Planning and Command of EW in Joint Operations

The increasing importance of EW demands corresponding changes in operational planning and command structures. Spectrum superiority cannot be achieved solely through technological acquisition. It requires deliberate planning, coordinated execution, effective command arrangements, and continuous integration with broader operational objectives.

Historically, EW was often viewed as a specialised technical activity conducted by dedicated units. Contemporary military operations, however, require EW considerations to be integrated into operational planning at every level of command.

As military forces become increasingly dependent upon spectrum-enabled systems, EW must be incorporated into campaign design, mission planning, intelligence preparation, targeting processes, force protection measures, and operational assessments.

Spectrum Dependency Analysis

Effective EW planning begins with understanding the extent to which friendly and adversary operations depend upon the electromagnetic spectrum.

Commanders must identify critical communications systems, surveillance networks, navigation aids, data links, and command-and-control architectures that support operational objectives.

Similarly, analysis of adversary spectrum dependencies can reveal vulnerabilities that may be exploited through EA, cyber operations, deception measures, or kinetic action.

Such assessments enable commanders to prioritise resources and develop more effective operational plans.

Electromagnetic Order of Battle (EOB)

Just as military planners develop an order of battle for conventional forces, they must also construct a detailed understanding of the adversary's electromagnetic posture.

This Electromagnetic Order of Battle (EOB) includes:

- Communications systems.
- Radar networks.
- Navigation infrastructure.
- Data links.

- Electronic surveillance assets.
- Spectrum management practices.
- Cyber-electromagnetic dependencies.

A comprehensive EOB provides the foundation for targeting, force protection, deception, and operational planning.

Electromagnetic Battle Management (EMBM)

The growing density of electromagnetic activity within modern battle spaces has increased the importance of EMBM.

EMBM involves the planning, coordination, monitoring, and control of spectrum-dependent activities to ensure operational effectiveness while minimising interference and fratricide.

Effective EMBM enables commanders to synchronise communications, intelligence collection, EA activities, navigation services, and unmanned systems within a common operational framework.

As military operations become increasingly dynamic, future EMBM systems are likely to incorporate artificial intelligence and automation to support real-time spectrum management.

Operating in a Degraded Environment

A fundamental principle of military planning is the expectation that adversaries will contest spectrum access. Consequently, forces must be prepared to operate under conditions of degraded communications, denied navigation, disrupted data links, and contested information environments.

This requires resilient systems, alternate communications pathways, mission command principles, and regular training under degraded conditions. The ability to continue operating effectively despite electronic disruption may prove decisive in future conflicts.

Command Responsibility and Joint Integration

EW cannot remain the exclusive responsibility of specialist units. Commanders at all levels must understand its implications and integrate EW considerations into operational decision-making.

Joint operations further increase this requirement because spectrum activities undertaken by one service may influence operations conducted by another. Effective coordination therefore requires common doctrine, shared situational awareness, integrated planning processes, and clearly defined command responsibilities.

The movement towards Integrated Theatre Commands provides an opportunity to institutionalise such arrangements and strengthen joint spectrum operations.

Legal, Ethical and Escalation Considerations

The growing sophistication of EW also raises important legal, ethical, and strategic considerations. Certain EW actions may affect civilian infrastructure, commercial communications systems, navigation networks, or critical national services. Others may generate unintended escalation or produce cascading effects across interconnected systems.

Commanders must therefore balance operational effectiveness with legal obligations, strategic objectives, and broader national interests. Appropriate rules of engagement, oversight mechanisms, and policy frameworks will remain essential for responsible employment of Electronic Warfare capabilities.

Ultimately, successful EW is not simply a function of technology. It is a function of planning, leadership, integration, training, and operational understanding. As warfare becomes increasingly dependent upon the electromagnetic spectrum, the ability to plan, command, and synchronise EW activities effectively will become a critical determinant of military success.

IX. Strategic Implications for India

The evolving character of warfare presents both challenges and opportunities for India. The increasing integration of cyber capabilities, autonomous systems, artificial intelligence, space-based assets, and long-range precision weapons has elevated the importance of the electromagnetic spectrum as a critical enabler of military power. Consequently, EW must occupy a central place in India's ongoing military transformation.

The movement towards Integrated Theatre Commands provides a unique opportunity to institutionalise EW as a truly joint capability. Rather than viewing EW as a specialised function confined to individual services, it must be integrated into operational planning, command structures, training methodologies, and force development processes across the Armed Forces.

Towards a Joint Electronic Warfare Doctrine

A fundamental requirement is the development and continuous refinement of a Joint Electronic Warfare Doctrine aligned with the principles of Joint and MDO. Such a doctrine should establish common terminology, operational concepts, command relationships, planning procedures, and spectrum management responsibilities.

Equally important is the integration of EW with cyber operations, space support, intelligence activities, information operations, and precision targeting systems. A doctrinally coherent approach will ensure greater interoperability and more effective employment of spectrum-dependent capabilities.

Strengthening Theatre-Level EW Structures

Future Integrated Theatre Commands will require dedicated EW planning and coordination mechanisms capable of synchronising spectrum operations across services and domains.

These structures should support:

- EMBM.
- Joint spectrum planning.
- Integrated intelligence support.
- Cyber-electromagnetic coordination.
- Counter-UAS operations.
- Spectrum resilience measures.

Such arrangements will help ensure unity of effort while reducing duplication and operational fratricide.

Indian Capability Gaps and Future Priorities

While India has made considerable progress in EW, significant capability gaps remain when assessed against the requirements of future MOD. The challenge is not merely one of equipment acquisition but of achieving integration across doctrine, organisation, training, technology, and operational concepts.

At the organisational level, EW capabilities remain distributed across the Services with varying degrees of interoperability. The transition towards Integrated Theatre Commands provides an opportunity to establish common spectrum management procedures, integrated planning mechanisms, and theatre-level electromagnetic battle management capabilities.

At the technological level, emerging challenges include AI-enabled spectrum operations, cognitive EW, autonomous systems, advanced mission data libraries, anti-drone technologies, and dynamic spectrum management. Rapid advances by major powers, particularly in the fields of intelligentized warfare and human-machine teaming, underscore the importance of sustained indigenous innovation.

Human capital development remains equally important. Future commanders must understand the operational implications of cyberspace, space, information warfare, and electronic warfare as interconnected dimensions of conflict rather than isolated technical disciplines. Professional Military Education institutions will therefore need to place greater emphasis on MDO, CEMA, AI, and spectrum-centric warfare.

India's long-term objective should be the creation of a fully integrated Joint Electromagnetic Spectrum Operations framework capable of supporting theatre-level operations across land, maritime, air, cyber, and space domains. Such a capability would significantly enhance deterrence, operational effectiveness, and strategic resilience.

Building Indigenous Technological Capabilities

Technological self-reliance remains critical for sustained military effectiveness. Dependence on external sources for critical EW systems may create vulnerabilities during crises or conflicts.

India should therefore continue to strengthen indigenous capabilities in:

- Electronic Support systems.

- Electronic Attack technologies.
- Electronic Protection solutions.
- Software-defined radios.
- Mission data libraries.
- Cognitive EW systems.
- Artificial intelligence applications.
- Counter-drone technologies.
- Electromagnetic battle management systems.

The growing emphasis on self-reliance under the national vision of Atmanirbhar Bharat provides a strong foundation for such efforts.

AI and Cognitive EW Development

AI is likely to become one of the most important drivers of future Electronic Warfare capabilities.

India must invest in:

- Machine learning applications.
- AI-enabled signal analysis.
- Autonomous spectrum management.
- Advanced data fusion.
- Decision-support systems.
- Adaptive EW algorithms.

Such capabilities will be essential for operating effectively within highly contested and rapidly changing electromagnetic environments.

Human Capital and Professional Military Education (PME)

Technology alone cannot guarantee success. Future commanders must understand the operational implications of spectrum warfare and appreciate the growing interdependence of cyber, space, information, and electronic capabilities.

PME institutions should therefore incorporate greater emphasis on:

- EW.
- CEMA.
- AI.
- MDO.
- Spectrum management.
- Information warfare.

Building a cadre of leaders capable of operating effectively within complex information-centric environments will be as important as acquiring advanced technologies.

Ultimately, India's military effectiveness in future conflicts will depend not only upon platforms and weapon systems but also upon its ability to sense, protect, exploit, and dominate the electromagnetic spectrum.

X. Challenges and Constraints in achieving Spectrum Dominance

While EW offers significant operational advantages, it is not a panacea. Its growing importance is accompanied by several challenges, risks, and limitations that must be carefully addressed.

Technological Complexity

Modern EW systems are increasingly sophisticated and require significant investment in research, development, testing, integration, and maintenance. Rapid technological change can shorten system lifecycles and create continuous modernisation requirements.

Adversary Adaptation

History demonstrates that military technologies rarely remain dominant for long. Adversaries continuously adapt tactics, techniques, and procedures to counter new capabilities.

Frequency-agile communications, autonomous navigation systems, distributed networks, artificial intelligence, and cognitive technologies may reduce the effectiveness of traditional EA measures. This reality underscores the importance of continuous innovation.

Spectrum Congestion

The proliferation of military and civilian users has made the electromagnetic environment increasingly crowded.

Uncoordinated operations can create interference, degrade friendly systems, and reduce overall operational effectiveness. Effective spectrum management will therefore remain essential.

Fratricide and Unintended Consequences

Electronic effects do not always remain confined to intended targets. Jamming or disruption measures may inadvertently affect friendly forces, civilian systems, or critical infrastructure.

Careful planning, coordination, and electromagnetic de-confliction are therefore essential components of successful EW operations.

Organisational Challenges

The integration of EW, cyber operations, space support, intelligence activities, and information operations often encounters institutional and organisational barriers.

Differences in culture, doctrine, command arrangements, and resource allocation can complicate efforts to achieve effective integration.

Addressing these challenges will require sustained leadership attention and organisational reform.

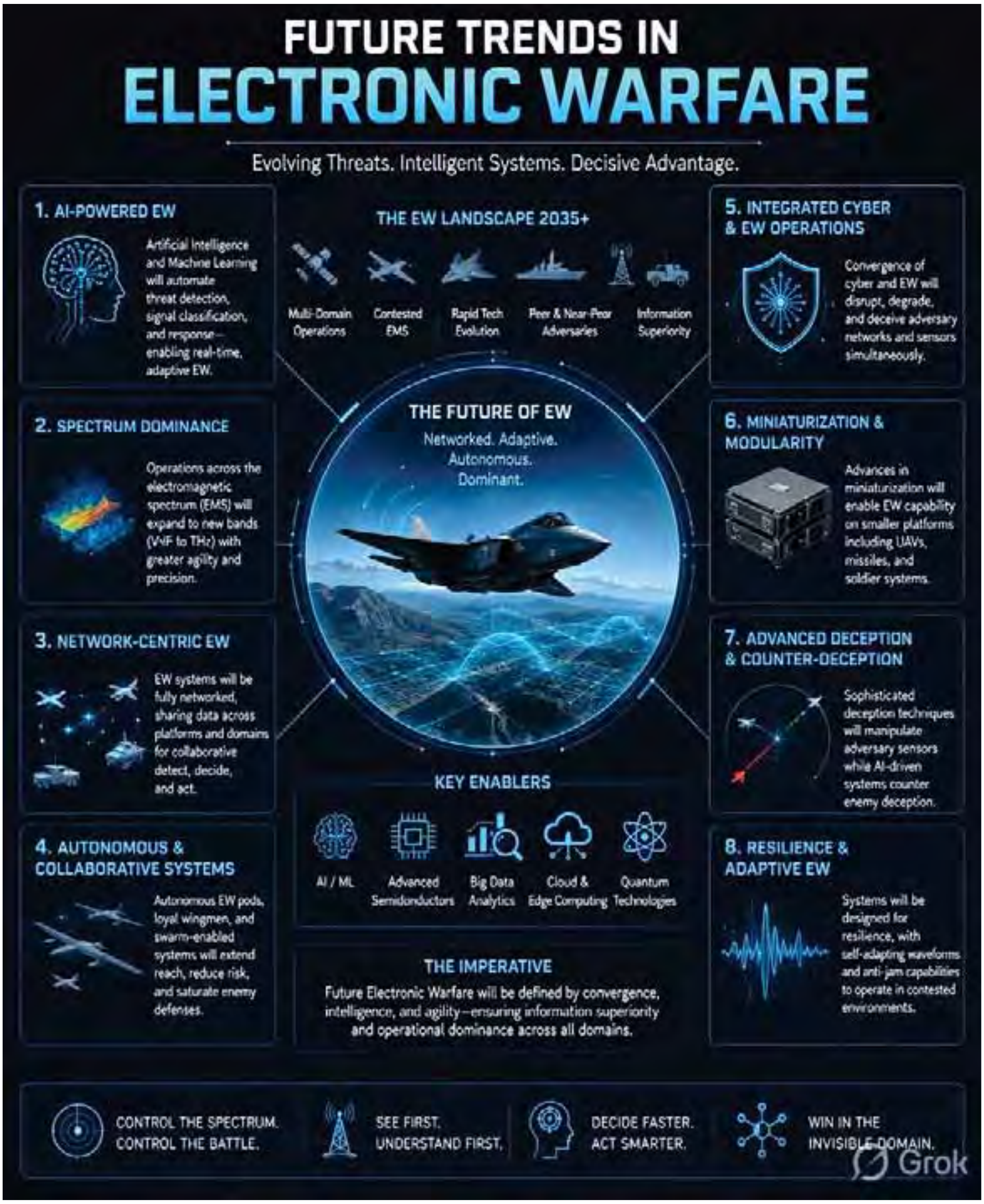
Dependence on Technology

An overreliance on technology may itself become a vulnerability.

Future adversaries will seek to deny access to communications, navigation systems, satellites, and information networks. Forces must therefore retain the ability to operate effectively under degraded or denied conditions.

Resilience, redundancy, and mission command will remain indispensable.

XI. Future Trends in Electronic Warfare



EW is poised for profound transformation over the coming decades. Advances in AI, autonomous systems, cyber capabilities, cloud computing, advanced semiconductors, space technologies, and directed energy weapons are fundamentally reshaping the electromagnetic battlespace. Recent conflicts—particularly the Ukraine war and the 2026 US & Israel–Iran conflict, including U.S.

strikes on Iranian nuclear facilities—demonstrate that spectrum superiority is emerging as a decisive factor, comparable to air superiority. Future wars are unlikely to rely solely on kinetic force; instead, they will involve continuous competition for dominance of the electromagnetic spectrum, cyberspace, and the information environment.

EW as the First Battle

The traditional sequence of *detect–engage–destroy* is increasingly giving way to *sense–jam–disrupt–destroy*. Contemporary operations routinely employ cyber-attacks, electronic attack, GPS denial, communications disruption, deception, and electromagnetic manoeuvre before kinetic strikes to blind, isolate, and disorient the adversary. The EMS has effectively become the opening battlefield, setting the conditions for subsequent military operations.

Drones Have Become the Primary EW Battlefield

The war in Ukraine has demonstrated that tactical drones have become indispensable battlefield assets, but also the primary targets of intense EW Virtually every drone mission is contested through GPS jamming, command-link disruption, spoofing, electronic deception, and cyber-enabled interference. This has triggered a rapid technological race to improve drone survivability and mission effectiveness through frequency-hopping communications, encrypted data links, autonomous navigation, optical and terrain-referenced guidance, AI-assisted target recognition, and sophisticated anti-jamming techniques. Russia's extensive employment of fibre-optic-controlled First Person View (FPV) drones, which are largely immune to conventional radio-frequency jamming, illustrates how quickly drone technology is evolving to overcome electronic countermeasures and maintain operational effectiveness in heavily contested electromagnetic environments.

The recent Iran–Israel conflict, together with the military involvement of the United States, has further reinforced the growing importance of drones across the full spectrum of military operations. Long-range one-way attack drones, loitering munitions, reconnaissance UAVs, and collaborative drone swarms have been employed extensively for intelligence gathering, precision strikes, suppression of air defences, and strategic attacks against military infrastructure. Their effectiveness has depended not only on advanced payloads but also on their ability to survive sophisticated electronic attack and navigation denial. These conflicts demonstrate that future drone warfare will be defined by a continuous contest between increasingly autonomous, AI-enabled unmanned systems and equally sophisticated electronic warfare capabilities. Consequently, the development of resilient, low-cost, anti-jam, and electronically adaptive drones will become a decisive determinant of battlefield success.

AI-Enabled Electronic Warfare and Human–Machine Teaming

AI is becoming integral to both offensive and defensive EW operations. AI can rapidly identify emitters, optimise jamming techniques, recommend spectrum allocation, analyse vast volumes of electromagnetic data, and assist autonomous platforms in recognising targets despite degraded communications. Future cognitive EW systems will continuously sense, analyse, and adapt by autonomously modifying frequencies, waveforms, power levels, and countermeasure techniques in near real time. Rather than replacing human decision-makers, AI will increasingly complement them through human–machine teaming, providing speed and analytical support while human operators retain judgement and operational control. AI-enabled autonomous swarms capable of operating in heavily contested electromagnetic environments are likely to become a defining feature of future warfare.

From Platform-Centric to Distributed Network-Centric EW

EW is no longer confined to specialised aircraft or dedicated ground stations. Fighters, unmanned systems, naval platforms, satellites, ground vehicles, and even individual soldiers are becoming interconnected nodes within a distributed EW architecture. Miniaturised sensors, processors, and software-defined modules will embed advanced EW capabilities across virtually every combat platform. Modular payloads will permit rapid mission-specific reconfiguration without extensive hardware modification, while real-time sharing of electromagnetic intelligence will enable coordinated sensing, electronic attack, and spectrum management across multiple domains. This distributed architecture will enhance survivability, scalability, and operational resilience by reducing dependence on a few high-value EW assets.

Cloud, Edge Computing and Software-Defined EW

Cloud and edge computing will fundamentally transform EW by enabling rapid processing and dissemination of vast volumes of electromagnetic data across the battlespace. Cloud-based architectures will support centralised analytics, AI model training, and mission planning, while edge computing will process data close to sensors and weapon platforms, enabling near real-time decision-making even in communication-denied environments. Coupled with software-defined radios and rapidly updateable threat libraries, this hybrid architecture will compress innovation cycles from years to weeks, allowing forces to respond quickly to evolving threats while significantly accelerating the sensor-to-shooter cycle.

Advanced Deception and Counter-Deception

Future conflicts are likely to witness an increasingly sophisticated contest between deception and counter-deception.

Artificial Intelligence, digital signal processing, and cognitive EW will enable highly realistic false targets, spoofed communications, manipulated navigation signals, deceptive electromagnetic signatures, and synthetic sensor inputs designed to mislead adversary commanders. Equally, advanced signal analytics, machine learning, and multi-sensor data fusion will improve the ability to detect, attribute, and neutralise such deception in near real time. Victory will depend not merely on denying information to the adversary but on shaping his perception of the battlespace and compressing his decision cycle.

Integration of EW, Cyber, Space and Cognitive Warfare

The boundaries separating EW, cyber operations, space capabilities, information operations, and psychological influence activities are steadily disappearing. Modern campaigns increasingly seek to disrupt communications, navigation, satellite links, digital networks, and decision-making processes simultaneously. Electromagnetic operations will therefore become increasingly integrated with cyber and cognitive warfare, enabling coordinated effects across all domains and creating multiple dilemmas for the adversary.

Layered Counter-Drone Defence

Experience from recent conflicts confirms that neither electronic jamming nor kinetic interception alone provides an adequate defence against unmanned systems. Effective counter-drone operations increasingly depend upon a layered approach integrating electronic attack, cyber effects, high-power microwave weapons, directed-energy lasers, interceptor drones, conventional guns and missiles, and distributed sensor networks. Such integrated defences provide greater resilience against increasingly diverse and evolving aerial threats.

Navigation Warfare (NAVWAR)

Heavy dependence on satellite-based navigation has emerged as a significant operational vulnerability. Extensive use of GPS denial and spoofing has renewed emphasis on resilient Positioning, Navigation and Timing (PNT) through inertial navigation, terrain-referenced navigation, celestial navigation, and multi-constellation satellite navigation systems. Assured navigation will remain indispensable for future operations in contested electromagnetic environments.

Low-Cost Sensors and Distributed EW

Recent conflicts have demonstrated the effectiveness of inexpensive acoustic sensors, passive RF detectors, commercial technologies, and distributed sensing networks. Future EW architectures are therefore likely to favour numerous low-cost, networked sensors rather than a few highly sophisticated platforms, improving survivability, affordability, and electromagnetic situational awareness while enhancing the resilience of distributed force structures.

Advanced Semiconductors

Advances in semiconductor technologies will underpin the next generation of Electronic Warfare capabilities. Wide-bandgap materials such as Gallium Nitride (GaN) and Silicon Carbide (SiC), together with emerging photonic and quantum-enabled devices, will deliver higher power output, greater efficiency, wider frequency coverage, and faster signal processing while reducing size, weight, and power requirements. These technologies will significantly enhance radars, jammers, electronic support systems, software-defined radios, and directed-energy weapons. For India, indigenous semiconductor design, fabrication, and trusted supply chains will be essential to achieving technological self-reliance and sustaining long-term spectrum dominance

Protection of Civilian Infrastructure

Recent conflicts have demonstrated that power grids, communications networks, transportation hubs, ports, airports, and financial systems have become integral elements of the battlespace. EW, cyber-attacks, and precision kinetic strikes are increasingly synchronised to disrupt critical national infrastructure, undermine societal resilience, and constrain an adversary's ability to sustain military operations.

Quantum Technologies and Directed Energy Weapons(DEWs)

Emerging quantum technologies and Directed Energy Weapons (DEWs) are expected to reshape the future electromagnetic battlespace. Quantum sensing promises unprecedented precision in navigation, timing, detection, and electronic intelligence, while quantum communications offer significantly greater resilience and security for military networks. Simultaneously, high-energy lasers and high-power microwave systems provide rapid, precise, and scalable means of disrupting or neutralising drones, missiles, sensors, and communication systems with minimal collateral damage. Together, these technologies will substantially expand the scope of EMSO.

Spectrum Dominance as a Joint Operational Imperative

The overarching lesson from recent conflicts is that EW can no longer remain a specialised support function. It must be fully integrated into operational planning and execution at every level of command. Future joint commanders will require continuous awareness of the electromagnetic environment, seamless integration of EW, cyber, space, information, and kinetic capabilities, resilient and adaptive command networks, and the agility to respond rapidly to changing spectrum conditions. The future of EW will therefore be characterised by greater autonomy, miniaturisation, software-defined adaptability, distributed architectures, cognitive influence, and AI-enabled decision support, making spectrum dominance an indispensable prerequisite for success in multi-domain operations

Implications for India

The lessons emerging from recent conflicts have significant implications for India's evolving Joint Force structure and future warfighting doctrine. As the Armed Forces progress towards Integrated Theatre Commands and MDO, Electronic Warfare (EW) must transition from a specialist enabling function to a core operational capability. Priority areas include:

- Developing a Joint Electromagnetic Spectrum Operations (JEMSO) framework.
- Expanding AI-enabled Cognitive Electronic Warfare capabilities.
- Investing in resilient Positioning, Navigation and Timing (PNT) systems for GPS-denied environments.
- Building layered Counter-UAS architectures integrating EW, directed-energy weapons, interceptor drones, and conventional air defence.
- Accelerating indigenous software-defined EW systems with rapid waveform and mission-data updates.
- Strengthening integration among EW, cyber, space, intelligence, and air defence.
- Enhancing spectrum-centric training and realistic multi-domain exercises at all command levels.

Developing Human Capital and Knowledge Networks.

Sustained spectrum dominance will depend as much on skilled professionals as on advanced technology. India should establish visible career pathways enabling personnel to move between the Armed Forces, DRDO, academia, industry, and start-ups, thereby nurturing and retaining specialised EW expertise. Equally important is an institutional framework for the secure exchange of operational data, research, and technical knowledge across military and civilian domains to accelerate innovation, strengthen indigenous capability, and enhance national resilience.

XII. Strategic Recommendations

The analysis presented in this paper suggests that achieving and sustaining spectrum dominance requires a comprehensive national approach extending well beyond technological superiority. Accordingly, the following strategic priorities merit consideration:

- **Institutionalise EW as a Joint Warfighting Capability:** Institutionalise EW as a truly joint capability within the framework of Integrated Theatre Commands by establishing Theatre EW Cells and EMBM structures for unified planning, coordination, and execution.

- **Develop a Joint Electromagnetic Spectrum Operations (JEMSO) Framework:** Develop a comprehensive Joint Electromagnetic Spectrum Operations (JEMSO) framework integrating spectrum management, EW, cyber, space-enabled capabilities, information operations, and electromagnetic battle management into a unified operational architecture.

- **Establish a National Spectrum Operations Management (NoSuM) Framework:** Establish a National Spectrum

Operations Management (NoSuM) framework, modelled on the aviation Notice to Airmen (NOTAM) system, as an integral component of national spectrum policy. A dynamic NoSuM mechanism should provide near real-time information on spectrum availability, restrictions, priority allocations, interference, and contested electromagnetic conditions, thereby enabling spectrum deconfliction, dynamic allocation, and coordinated civil-military spectrum governance.

- **Accelerate cyber-Electromagnetic Integration:** Accelerate the integration of CEMA through common doctrine, interoperable command arrangements, and shared operational procedures linking EW, cyber, intelligence, space, and information operations.

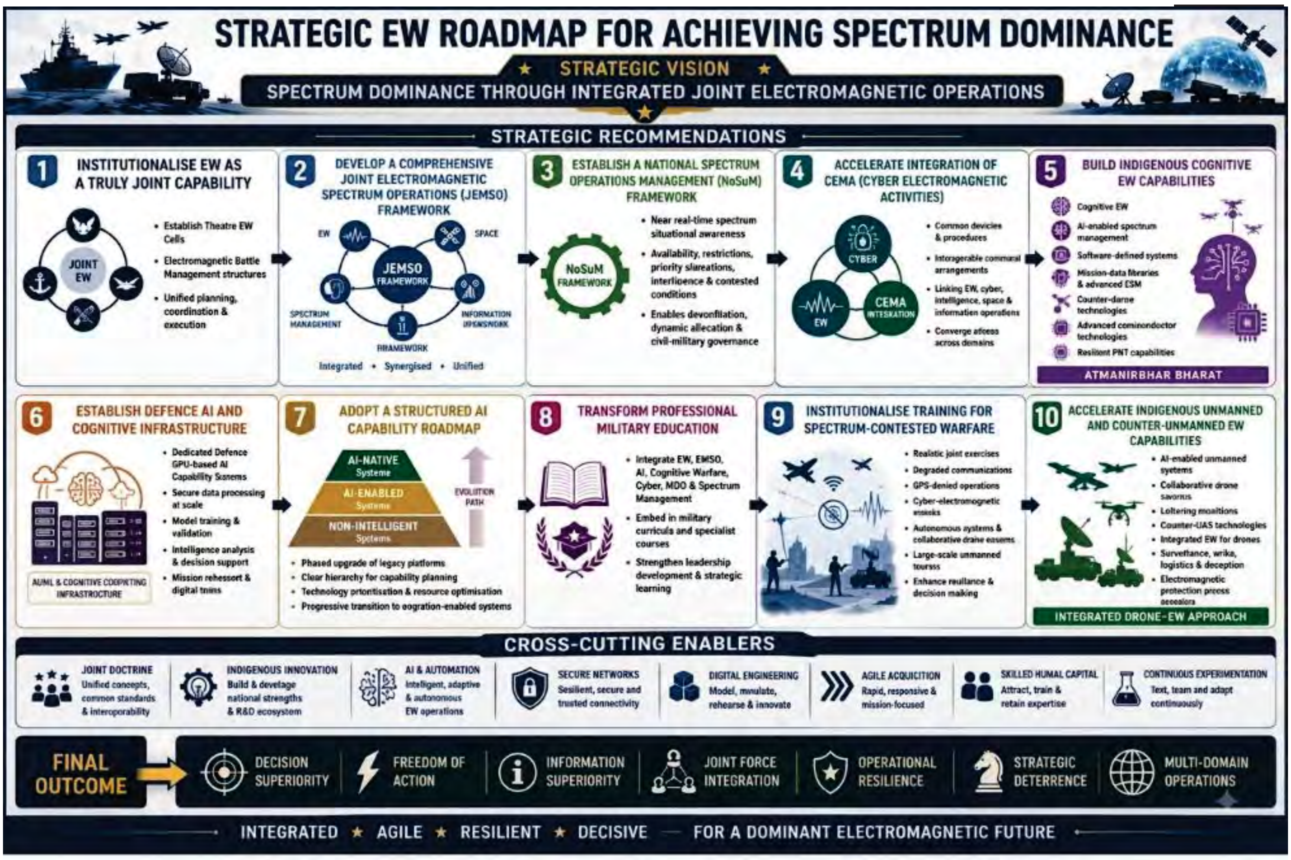
- **Establish Defence AI and Cognitive Infrastructure:** Establish a dual-use AI/ML and cognitive computing infrastructure, complemented by dedicated Defence GPU-based AI Capability Centres for secure large-scale data processing, model training, intelligence analysis, mission rehearsal, digital twins, and operational decision support.

- **Adopt a Structured AI Capability Roadmap:** Establish a clear capability hierarchy distinguishing AI-native, AI-enabled, and non-intelligent systems, and implement a phased roadmap for upgrading legacy platforms into AI-enabled and, where feasible, cognition-enabled systems. This structured approach will facilitate capability planning, technology prioritisation, and the systematic evolution of the Armed Forces towards intelligent, adaptive, and future-ready operational capabilities.

- **Transform Professional Military Education:** Strengthen Professional Military Education by integrating EW, EMSO, AI, Cognitive Warfare, Cyber Operations, MDO, and Spectrum management into military curricula, specialist training, and leadership development programmes.

- **Institutionalise Training for Spectrum-Contested Warfare:** Institutionalise spectrum-contested training through realistic joint exercises incorporating degraded communications, GPS-denied operations, cyber-electromagnetic attacks, autonomous systems, collaborative drone swarms, and large-scale unmanned threats to enhance operational resilience and decision-making under contested electromagnetic conditions.

- **Accelerate Indigenous Unmanned and Counter-Unmanned EW Capabilities:** Accelerate the development and induction of AI-enabled unmanned systems, collaborative drone swarms, loitering munitions, counter-UAS technologies, and associated electronic warfare capabilities. Future conflicts have demonstrated that drones and EW are inseparable; therefore, India's force modernisation should adopt an integrated "Drone–EW" approach encompassing surveillance, strike, logistics, deception, and electromagnetic protection across all domains.



Ultimately, future wars are unlikely to be won solely through superior platforms or greater firepower. Decisive advantage will belong to the force that can integrate its capabilities faster and more effectively than its adversary—leveraging EW to sense first, understand faster, decide better, adapt continuously, and dominate the electromagnetic spectrum. As warfare becomes increasingly networked, multi-domain, and data-driven, EW will emerge as a central pillar of military power, enabling information superiority, operational agility, and decision dominance through its integration with cyber, space, AI-enabled systems, and conventional combat capabilities. In this environment, the ability to achieve and sustain spectrum dominance will be a defining determinant of both operational success and strategic advantage. For India, the imperative is no longer whether EW should be integrated into joint operations, but how rapidly it can develop the doctrine, organisational structures, technologies, human capital, and institutional mechanisms required to secure enduring electromagnetic spectrum dominance.

Conclusion

The evolution of warfare in the twenty-first century has fundamentally transformed the electromagnetic spectrum from a supporting medium into a decisive operational battlespace. Contemporary conflicts demonstrate that military success is no longer determined solely by the employment of kinetic force, but increasingly by the ability to achieve information superiority, dominate the electromagnetic spectrum, and integrate effects seamlessly across the land, maritime, air, space, cyber, and cognitive domains. In this environment, EW has evolved far beyond its traditional role of electronic support, electronic attack, and electronic protection. It has emerged as a strategic capability that underpins MDO and enables decision superiority across the entire spectrum of conflict.

The operational lessons from recent conflicts, particularly in Ukraine, Nagorno-Karabakh, and the Middle East, reaffirm that spectrum superiority is indispensable for successful military operations. The widespread employment of unmanned systems, precision-guided munitions, resilient communications, satellite-enabled networks, and AI-driven decision support has intensified competition within the electromagnetic domain. At the same time, the convergence of EW with CEMA, EMSO, AI, autonomous systems, and cognitive operations is reshaping the character of warfare. The electromagnetic spectrum has become a continuously contested environment in which the ability to sense, deceive, disrupt, protect, and exploit spectrum-dependent systems often determines the outcome of military operations long before kinetic engagement begins.

The strategic recommendations presented in this paper are intended to strengthen India's ability to operate effectively in this increasingly contested environment. Their successful implementation will depend not merely upon technological modernisation, but equally upon doctrinal innovation, institutional integration, inter-service synergy, investment in indigenous research and development, and the cultivation of a highly skilled cadre of EW professionals. The ongoing transformation of the Indian Armed Forces through integrated theatre commands presents a unique opportunity to institutionalise EW as a truly joint capability and to embed spectrum operations as an integral component of future operational planning and execution.

Looking ahead, the future trajectory of EW will be shaped by advances in cognitive EW, AI, machine learning, software-defined radios, quantum technologies, advanced electronic deception, autonomous systems, and resilient cloud- and edge-enabled architectures. These technologies will enable increasingly adaptive, intelligent, and autonomous spectrum operations while simultaneously demanding new approaches to doctrine, organisation, training, and capability development. As the pace of technological change accelerates, maintaining electromagnetic superiority will require continuous innovation, rapid adaptation, and close collaboration between the military, academia, industry, and the national scientific ecosystem.

The central argument advanced in this paper is that EW has become one of the principal enablers of MDO and a decisive determinant of future military effectiveness. Nations that successfully integrate EW with cyber operations, AI, space capabilities, intelligence systems, and cognitive operations within a coherent operational framework will possess a significant strategic and operational advantage in future conflicts.

Ultimately, EW is no longer merely a specialised combat support function; it is rapidly becoming the operational nervous system of MDO. In an era where every sensor, shooter, network, autonomous platform, and decision-maker depends upon assured access to the electromagnetic spectrum, the ability to achieve and sustain spectrum dominance will increasingly determine military success. The future of warfare will therefore belong not simply to those who possess superior platforms or greater firepower, but to those who can perceive, control, exploit, and defend the electromagnetic spectrum faster, more intelligently, and more comprehensively than their adversaries. Recognising this reality and translating it into doctrine, organisation, technology, and operational practice will be central to preserving India's military advantage and ensuring preparedness for the challenges of future warfare.

Bibliography

Books

Adamy, David L. *EW 101: A First Course in Electronic Warfare*. 1st ed. Boston, MA: Artech House Publishers, 2001.

Adamy, David L. *EW 102: A Second Course in Electronic Warfare*. 1st ed. Boston, MA: Artech House Publishers, 2004.

Binnendijk, Hans, and James Johnson, eds. *Artificial Intelligence and International Security*. Santa Monica, CA: RAND Corporation, 2020.

Boyd, John R. *A Discourse on Winning and Losing*. Maxwell Air Force Base, AL: Air University Press, 2018.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Kallenborn, Zachary. *The Era of the Drone Swarm: The Coming Age of Autonomous Unmanned Systems*. Carlisle, PA: U.S. Army War College Press, 2021.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press, 2007.

Libicki, Martin C. *Cyber deterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Poisel, Richard A. *Modern Communications Jamming: Principles and Techniques*. 2nd ed. Norwood, MA: Artech House, 2011.

Price, Alfred. *Instruments of Darkness: The History of Electronic Warfare*. New expanded and updated ed. London: Macdonald and Jane's, 1977.

Russell, Stuart, and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed. Hoboken, NJ: Pearson, 2021.

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. 1st ed. New York: W. W. Norton & Company, 2018.

Probhal DasGupta, *General Brasstacks, The Sundarji Story,* Penguin Random SHouse, India, 2026.

Journal Articles, Monographs, Issue Briefs and Reports

Centre for Land Warfare Studies. *Issue Briefs, Monographs and Occasional Papers on Multi-Domain Operations*. New Delhi: Centre for Land Warfare Studies, Indian Army. Accessed April 20, 2026.

CLAWS. *Round Table Discussion on "Winning the Invisible War: Spectrum Dominance, Autonomy, and the New Grammar of Electronic Warfare."* New Delhi: Centre for Land Warfare Studies, May 13, 2026.

Dayton, Alan. "Winning the Invisible Fight: The Need for Spectrum Superiority." *Defense360*. Center for Strategic and International Studies. December 21, 2016.

Haykin, Simon. "Cognitive Radar: A Way of the Future." *IEEE Signal Processing Magazine* 23, no. 1 (January 2006): 30–40.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures*. Washington, DC: Center for Strategic and International Studies, July 13, 2023.

Narang, Anshuman. *Key Drones and Counter UAS Technologies*. Monograph. New Delhi: Centre for Joint Warfare Studies, 2026.

Doctrinal Publications

Department of the Army. *FM 3-12: Cyberspace and Electromagnetic Warfare Operations*. Washington, DC: Headquarters, Department of the Army, August 24, 2021.

Department of Defense. *Joint Publication 3-85: Joint Electromagnetic Spectrum Operations*. Washington, DC: Joint Chiefs of Staff, May 22, 2024.

Headquarters Integrated Defence Staff, Ministry of Defence, Government of India, New Delhi, Joint *Doctrine for the Indian Armed Forces*. 2nd ed, 2017.

Headquarters Integrated Defence Staff, Ministry of Defence, Government of India, New Delhi, *Joint Doctrine for Multi-Domain Operations, 2025*

Integrated Headquarters, Ministry of Defence (Army). New Delhi *Land Warfare Doctrine,*2018.

Fulghum, David A. "Electronic Warfare Returns to the Forefront of Modern Combat." *Journal of Electronic Defense* 45, no. 7 (2022): 18–25.

Cheatham, Michael J., Angelique M. Geyer, Priscella A. Nohle, and Jonathan E. Vazquez. "Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone." *Joint Force Quarterly*, no. 114 (3rd Quarter 2024): 83–91.

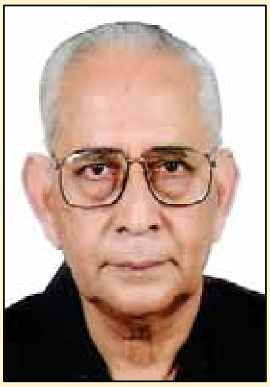
Perkins, David G. "Multi-Domain Battle: Driving Change to Win in the Future." *Military Review* 97, no. 4 (July–August 2017): 6–12.

Perkins, David G., and James M. Holmes. "Multidomain Battle: Converging Concepts toward a Joint Solution." *Parameters* 48, no. 3 (Autumn 2018): 49–54.

Colom Piella, Guillem, and Cristina Marzal Ruano. "Has Russian Electronic Warfare Underperformed in the Ukrainian Conflict?" *Journal of Strategic Security* 18, no. 4 (2025): 78–95. https://doi.org/10.5038/1944-0472.18.4.2369

Electronic Warfare (EW) has evolved from a combat support function into a decisive enabler of Joint and Multi-Domain Operations (MDO), with control of the electromagnetic spectrum emerging as a prerequisite for information and decision superiority. This paper argues that future conflicts will be characterised by intense competition for spectrum dominance, driven by the convergence of EW, Cyber operations, Artificial Intelligence (AI), Autonomous systems, Space capabilities, and Cognitive Electronic Warfare. Drawing on lessons from Ukraine, Nagorno-Karabakh, the Middle East, and recent Indian operational experience, it highlights the growing importance of Cyber-Electromagnetic Activities (CEMA), Counter-drone capabilities, AI-enabled spectrum management, and resilient command-and-control systems. The paper recommends a comprehensive transformation of India's EW capability through joint doctrine, integrated theatre-level structures, indigenous technological innovation, enhanced professional military education, and closer integration of EW with cyber, space, intelligence, and information operations to achieve sustained spectrum dominance in future warfare.

• • •



Lieutenant General SRR Aiyengar, PVSM, AVSM, VSM (Retd) was commissioned in the Corps of Signals, Indian Army on 11 June 1961.Graduated from National Defence Academy, Pune and later Indian Military Academy, Dehradun, the officer had an illustrious career in the Indian Army spanning nearly four decades. He has rich experience in serving in almost all types of Signal units to include Infantry, Mountain and Mechanized formations. Graduate of the prestigious 'Defence Services Staff College'. He obtained his MSC and MPhil degrees in Defence Studies from Tamil Nadu University. Recipient of three awards by the President -VSM (1989), AVSM (1993) and PVSM (1999). He has had the privilege of commanding the Armed Forces, three premier Training Institutions namely MCTE, DSSC and NDC. He has authored till date twelve books and two Monographs on a variety of topics.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in Contact us: landwarfare@gmail.com

SABRE & QUILL

MRP: ₹ 100.00 US$ 5.00