ISSN 2319-5177

CLAWS JOURNAL

WINTER 2025

VOL. 18, NO. 2

CENTRE FOR LAND WARFARE STUDIES

CHANAKYA CONFERENCE HALL: RATE CHART

FULL DAY: INR 25,000/-

HALF DAY: INR 15,000/-

LED Data Wall: INR 10,000/-

CLAWS JOURNAL

ISSN: 2319 – 5177

JOURNAL OF THE
CENTRE FOR LAND WARFARE STUDIES (CLAWS)

Distributed by
Kalpana Shukla
KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road
Daryaganj, New Delhi, 110002
Email: kw@kwpub.in
Website: www.kwpub.in

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent think tank registered under Act XXI of 1860, it being an act for the Registration of Literary, Scientific and Charitable Societies. The Chief of the Army Staff is the Patron of CLAWS and CLAWS is governed by a Board of Governors (BoG) with the Vice Chief of the Army Staff as Chairman. The Director General of Strategic Planning at Integrated Headquarters of MoD (Army) is the President of the Executive Council. The Director, CLAWS is responsible for the functioning at CLAWS under the overall direction of Chairman, BoG.

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.

POSTAL ADDRESS
Centre for Land Warfare Studies
RPSO Complex, Parade Road
Delhi Cantt-110010, India
Tele: +91-11-25691308, Fax: +91-11-25692347
EMAIL ID(s): claws.publications@gmail.com | landwarfare@gmail.com

CLAWS Journal is the flagship journal of the Centre for Land Warfare Studies. It is a peer-reviewed journal and is published bi-annually under Summer and Winter Issues. The scholarly journal covers all aspects of India's national security, regional and global security, warfighting concepts, doctrine and military strategy, and defence technology acquisition. The aim of the Journal is to promote an informed discourse among national and international scholars, government, and security professionals concerning the complexity and emerging challenges to the constantly changing global security environment.

Mailing address
Managing Editor, CLAWS Journal
Centre for Land Warfare Studies
RPSO Complex, Parade Road
New Delhi 110010, India

SUBSCRIPTION RATES	
India	Rs. 500/- (Single Issue)
	Rs. 1000/- (2 Issues)
SAARC Countries	US$ 15 (Single Issue
All other Countries	US$ 20 (Single Issue)

PATRON CLAWS

General Upendra Dwivedi, PVSM, AVSM
Chief of the Army Staff

ADVISORY BOARD

ADVISORY BOARD (AB)	
Appointment	**Appointment in AB**
Chief of the Army Staff	Chairperson
Vice Chief of Army Staff	Vice Chairperson
GOC-in-Cs (All)	Member
Deputy Chief of Army Staff (Strat)	Member Secy

BOARD OF GOVERNOR(S) {BoG}

BOARD OF GOVERNOR(S) {BoG}	
Appointment	**Appointment in BoG**
Vice Chief of the Army Staff	Chairman
Deputy Chief of Army Staff (Strat)	Member
Deputy Chief of Army Staff (Information Systems & Coord)	Member
Deputy Chief of Army Staff (CD & S)	Member
Adjutant General (AG)	Member
Master General Sustenance (MGS)	Member
Military Secretary (MS)	Member
Engineer in Chief (E-in-C)	Member
Quarter Master General (QMG)	Member
Chief of Staff - HQ ARTRAC	Member
General Officer Commanding (GOC) Delhi Area	Member
Director General of Strategic Planning (DG SP)	Permanent Invitee
Director General of Financial Planning (DGFP)	Permanent Invitee

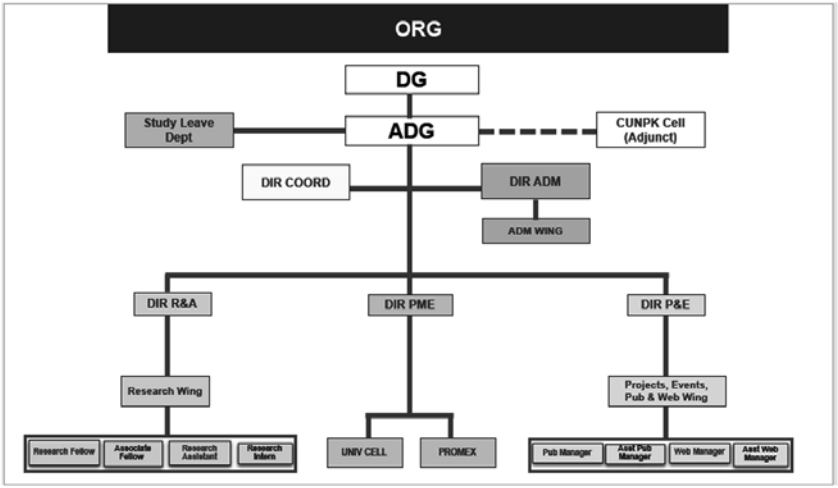
***The Director General, CLAWS will also be a member of the BoG and also act as Member Secretary of the BoG, CLAWS.**

EXECUTIVE COUNCIL (EC)

EXECUTIVE COUNCIL (EC)	
Appointment	**Appointment in EC**
Director General of Strategic Planning (DG SP)	President
Chief of Staff (COS), HQ Delhi Area	Member
Additional Director General of Financial Planning (ADG FP)	Member
Major General, General Staff (Approval & Planning) HQ ARTRAC	Member
Additional Director General of Strategic Planning	Member
Director General, CLAWS	Member

***The Additional Director General, CLAWS will act as Member Secretary. DG, CLAWS to act as Member Secretary in absence of ADG, CLAWS.**

ORGANISATION OF CLAWS



CLAWS VERTICALS

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Tel: 9311950042, Fax: 91-11-25692347
Email: landwarfare@gmail.com, director.claws@gmail.com,
Web: https://claws.co.in

MEMBERSHIP DETAILS

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 conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

The vision of the CLAWS is to develop a 'strategic culture' to bring about synergy in decision making both at national and operational levels. Since its inception, CLAWS has established itself as one of the leading 'think tanks' in the country. To achieve its vision, CLAWS conducts seminars (at Delhi and with commands), round table discussions and meetings with academia and intellectuals of strategic community both from India and abroad. CLAWS also comes out with a number of publications pertaining to national and regional security and various issues of land warfare.

Key Benefits of Individual Membership.

- Subsidised access to study material of all promotions as well as competitive exams (for offrs only)
- Access to capstone articles/ pub like Manekshaw Papers, Issue Briefs, Web articles and Occasional Papers on CLAWS website through membership login.
- Reg updates and invites for imp events at CLAWS through physical as well as online mode.

Eligibility:-

Individual Life Membership

- All serving and retired officers of the Indian Armed Forces.
- Civilian Dignitaries / Intellectuals
- Membership may be offered to civilian as well, especially to students and faculty of Instt of repute Universities.

Institutional Membership

Corporate / Institutional Membership

- All formations, units and establishments of the Indian Army.
- Representatives nominated by name accepted by the BoG/Trustees by any organization, institution, or diplomatic mission based in India.

Associate Membership

- Vice Chancellor of University and Heads of Departments of Defence Studies, military correspondents of Indian Newspapers, magazine and news agencies distinguished persons associated with the fields. Research fellows and media persons may be granted membership as approved by the BoG/ Trustees from time to time.

All members can also order CLAWS sponsored/commissioned books at a special discount of 25% on the MRP.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Tel: 9311950042, Fax: 91-11-25692347
Email: landwarfare@gmail.com, director.claws@gmail.com,
Web: https://claws.co.in

To
The Director General
Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road
Delhi Cantt, New Delhi –110010

Passport Size Photograph for Individual Member

APPLICATION FOR INDIVIDUAL LIFE MEMBERSHIP

Please tick any one:-

- ☐ **All Officer (Armed Forces) 1500/-**
- ☐ **Civilian Dignitaries / Intellectuals Rs 5000/-**
- ☐ **Students & Civilian faculty of reputed Universities Rs 2000/-**

Sir,

I would like to apply for Membership of the Centre for Land Warfare Studies. I understand that my membership is subject to the approval of the Director General. If approved, I will respect and follow the rules and regulations of the CLAWS (as amended from time to time).

Name of Individual (Service No) _____
Address: _____
_____
_____
Parent Arm/Service _____
Date of Birth _____Phone/Mobile:_____
Fax: _____**Email (Mandated)**_____

_____
(Counter Signature for Serving Offr only)

Mode of Payment

1. A Demand Draft/multi-city cheque No……dt…… of …… Bank for Rs.....in favour of **CLAWS payable at Delhi Cantt** is enclosed herewith.

OR

2. **NEFT** : Bank of Name – Canara Bank, 22 Thimmayya Marg, Delhi Cantonment, New Delhi 110010, Saving Account No – 91162010005981, IFS Code – CNRB0019008.

Dated …… ……
(Signature of Applicant)

Note:
1. **Please enclose one additional passport size photograph for membership card**
2. **Attached Aadhar Card and PAN Card (For Civilian). Student ID Card for Student.**
3. **The application form can also be forwarded through email at clawslibrary@yahoo.com).**

FOR OFFICE USE ONLY

Multi-city Cheque/DD Details: _____
Membership No.: _____Date of Issue of Membership Card:_____
Remarks of Director: _____
Remarks of Director General: _____

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Tel: 9311950042, Fax: 91-11-25692347
Email: landwarfare@gmail.com, director.claws@gmail.com,
Web: https://claws.co.in

To

The Director General
Centre for Land Warfare Studies
(CLAWS)
RPSO Complex, Parade Road
Delhi Cantt, New Delhi –110010

APPLICATION FOR INSTITUTIONAL MEMBERSHIP

Please tick any one:-

- ☐ **5 Years Institutional Membership (Rs 20,000/-)**
- ☐ **10 Years Institutional Membership (Rs 40,000/-)**

Sir,

I would like to apply for Membership of the Centre for Land Warfare Studies. I understand that my membership is subject to the approval of the Director. If approved, I will respect and follow the rules and regulations of the CLAWS (as amended from time to time).

Name of Institution _____
Address: _____
_____
_____
Phone/Mobile:_____ Fax: _____
Email:_____

Mode of Payment

1. A Demand Draft/multi-city cheque No.……dt…… of …… Bank for Rs.....in favour of **CLAWS payable at Delhi Cantt** is enclosed herewith.

OR

2. **NEFT** : Bank of Name – Canara Bank, 22 Thimmayya Marg, Delhi Cantonment, New Delhi 110010, Saving Account No – 91162010005981, IFS Code – CNRB0019008.

Dated ……
(With Institutional Seal)

……
(Signature of Applicant)

(Note: The Scanned application form can also be forwarded through email at clawslibrary@yahoo.com)

FOR OFFICE USE ONLY

Multi-city Cheque/DD Details: _____
Membership No.:_____Date of Issue of Membership Card:_____
Remarks of Director:_____
Remarks of Director General:_____

PROMOTION EXAM CORRESPONDENCE PRE-STAFF COURSE CELL
CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi-110010
Tel: 91-11-20893146, Army : 34156, Fax: 91-11-25692347
Email: clawscpsc@gmail.com, Web: http://claws.co.in

To,
Chief Instructor, PROMEX
c/o Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road
Delhi Cantt – 110010

APPLICATION FOR CLAWS STUDY MATERIAL FOR DSSC/ DSTC 2026

Sir,

I would like to apply for DSSC / DSTC 2026 Study Material prepared by CLAWS. I understand that my application is subject to approval and if approved, I will respect and follow the rules and regulations of the Centre.

IC No : ..... Rank and Name .....

Unit : Address for communication .....

PIN : .....c/o : .....

Contact No: Office ..... Mobile .....Email.....

Option Exercised: ☐ Mil History ☐ Current Affairs ☐ Science & Mil Tech
(Tick the choice)

Subscription Rate: Rs 4,500/- for all three subjects, Rs 3,000/- for any two subjects and Rs 2,000/- for any one subject. Previous years Study Material on SMT and CA is available on Rs. 1500/-.

Discount : 20% discount for subscription for DSSC / DSTC for individual officers taking CLAWS membership (3,600/- for all subject, 2,400/- for two & 1,600/- for one subject).

CLAWS Membership No: (If already a Member) .....

Note: Members can contact PROMEX Cell on tele for any clarification/ query during working hours any day or send the same through email.

Date: (Signature of Applicant)

Online transaction (NEFT/RTGS/IMPS) ref No ..... dt..... **OR**
Demand Draft/ multi-city cheque No.....dt..... for Rs.....
in favour of **PECPCC** payable at **Delhi Cantt** is enclosed herewith.

Bank Details for online transaction: Name of Acct Holder: **PECPCC**, Name of Bank : **HDFC** Bank, A/c No: **50100077341432** , IFSC : **HDFC0000139** , MICR : **110240020**
Eligibility: Serving Army officers.

FOR OFFICE USE ONLY

Multi-city Cheque/DD/online transaction Details .....
Membership No .....date of Issue of Membership Card .....
Remarks of Chief Instr, PROMEX .....

Note : **Study Material will be available from 15 Jan 2026 onward.**

RATE CHART OF CLAWS FOR STATE OF THE ART CONFERENCE HALLS
AVAILABLE FOR SEMINAR/DISCUSSION/TALK/TRAINING CAPSULE WEF 01 APRIL 2024

Sr. No.	Halls	Seating Capacity	Rate (In INR)		LED Data wall/ Projection System
			Full Day	Half Day	
(a)	Chanakya Hall	65	25,000/-	15,000/-	10000/- **(LED Data Wall)**
(b)	Chakravyuh Hall	35	7000/-	5000/-	3000/- **(Projection System)**
(c)	Kurukshetra Hall	50	10000/-	5000/-	3000/- **(Projection System)**

Note(s):-

- Space for Lunch and Tea will be provided as per availability.
- Catering will have to be organised under own arrangements. Available facilities will extended.

The booking will be subject to following terms and conditions:-

- 100% advance payment.
- Allotment is liable to be cancelled without prior notice if any imp visit is notified by Higher Authorities (COAS and VCOAS).
- Cancellation charges @ 20% will be levied if the cancellation is made with a notice less than three days.
- No refund is admissible if the cancellation made less than 24 hours.
- In case of damage to any existing infrastructure/items in Conference Hall/Seminar Hall during the course of functions, the damage for the same shall be paid as per actual amount.
- Organisers shall ensure that number of participants does not exceed the seating capacity of conference/ seminar hall. Also their guests /participants should strictly follow the instructions issued by Government of India from time to time and maintain sanctity of the premises.
- No eatables & tea/coffee will be served in Chanakya Hall.
- Water bottles (200ml) depending on Full/Half Day booking would be provided according to seating capacity only. Addl Charges would be levied for additional items.

For Queries Contact
landwarfare@gmail.com

ADVERTISEMENT RATE CARD : CLAWS PUBLICATIONS

Sr. No	Advertisement Placement Rate Card	CLAWS Journal (Bi-Annual) Per Issue	Scholar Warrior (Bi-Annual) Per Issue	Manekshaw Paper 4-5 Issues per year
	Standard Page Size	**225mm X 145mm**	**225mm X 145mm**	**225mm X 145mm**
1.0	**Back Cover (Colour)**	25,000/-	20,000/-	20,000/-
1.1	**Back Cover – Inside**	20,000/-	15,000/-	15,000/-
1.2	**Front Cover- Inside**	20,000/-	15,000/-	NA
1.3	**Full Page (both sides)- Inside content insert ad (Colour)**	5,000/-	5,000/-	NA
1.4	**Full Page (Single side) – Inside content insert ad (Colour)**	2,500/-	2,500/-	NA

- You are requested to indicate your preference for placement of the advertisement. The advertisements are available, on first come first serve basis.
- The advertisement material may please be sent as a soft copy, with the resolution of 300 dpi of more to claws.publications@gmail.com.

For Queries Contact: landwarfare@gmail.com

Contents

Articles

Book Reviews

Articles

India's Multi-Domain Operations Strategy: Navigating Hybrid Threats Through Jointness and Technological Convergence

Inderjeet Balotia

Abstract

Multi-Domain Operations (MDO) offer a transformative approach to modern warfare by integrating capabilities across land, air, maritime, space, cyber, and the electromagnetic spectrum to achieve decisive strategic advantage. For India, MDO is vital amid challenges posed by China's assertiveness along the LAC and Pakistan's asymmetric and proxy warfare. Recent reforms include creation of Integrated Theatre Commands, and dedicated Cyber and Space Commands etc. enhancing jointness and operational synergy. Advances in AI-enabled decision systems, cybersecurity, space-based ISR, and electronic warfare further strengthen readiness. This paper presents brief of MDO and its implementation strategy, SWOT analysis, implementation timeline,

Lieutenant Colonel **Inderjeet Balotia** was commissioned into the Corps of EME on 13 June 2009. The Officer has done advance course in Radars and completed his M.Tech in Network Management and Cyber Security. Views expressed are personal.

and the doctrinal, policy, and organisational changes required to institutionalise MDO for India's strategic superiority.

"Future conflicts will be won by those who can integrate and dominate across all domains—land, air, sea, cyber, and space—faster than their adversaries."

– General Charles Q. Brown Jr., Chief of Staff,
United States Air Force (2022)

Introduction

Modern warfare has moved beyond conventional battlefields, covering cyberspace, space, and the electromagnetic spectrum. Adversaries are increasingly using hybrid warfare, asymmetric tactics, and disruptive technologies to threaten India's national security. China's grey-zone tactics, cyber, and information warfare, along with Pakistan's cross-border terrorism and proxy threats, make it essential for India to adopt a well-coordinated and technology-driven approach to safeguard its sovereignty.

In response to these evolving challenges, India is strengthening its Multi-Domain Operations (MDO) strategy, which brings together the strengths of the Indian Army, Navy, and Air Force while incorporating cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning (ML), cybersecurity, space technology, Unmanned Aerial Vehicles (UAVs), and Electronic Warfare (EW). This approach is in line with India's recent defence reforms, including the appointment of the Chief of Defence Staff (CDS), formation of Integrated Theatre Commands (ITCs), and establishment of Cyber and Space Agencies, ensuring better coordination and a more unified approach to national security.

Russia-Ukraine Conflict

The Russia-Ukraine war showcases MDO in action, with Russia integrating kinetic and non-kinetic capabilities across land, air, sea, cyber,

space, and electromagnetic domains. Cyber attacks targeted Ukraine's power grid, financial systems, and government sites using malware (e.g. Black Energy, Industroyer), DDoS attacks, and disinformation to disrupt stability. In space, Russia disrupted satellite networks (e.g. Viasat) and jammed GPS to hinder UAVs. On land, conventional forces operated alongside separatists. At sea, a Black Sea blockade and missile strikes hurt Ukraine's economy. Electronic warfare jammed communications and air defences. Use of AI tools and proxy groups like Wagner highlighted MDO's effectiveness offering key lessons for India.

Armenia-Azerbaijan and Israel-Hamas conflict

The 2020 Armenia-Azerbaijan conflict further demonstrated EW's integration into MDO, with Azerbaijan combining electronic attacks and drone strikes to disable Armenian air defences and command structures. In another example, Israel employed "pager warfare" against Hezbollah, using targeted electronic messages to disrupt communications and morale. These cases reveal how EW, when embedded in an MDO framework, enables real-time disruption of adversary networks and complements kinetic and psychological operations, shaping the battlespace without direct confrontation.

Evolution of MDO

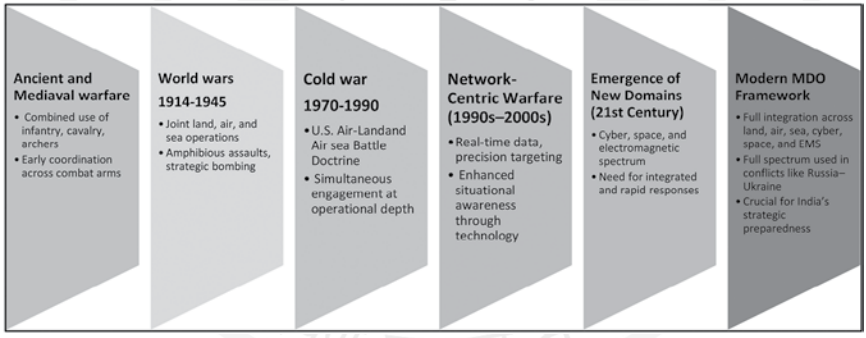
The concept of MDO has evolved as warfare expanded beyond traditional battlefields. Historically, even ancient armies combined combat arms for tactical advantage. In modern times, the World Wars highlighted the importance of joint land, air, and sea operations, especially in large-scale campaigns.

During the Cold War, the US introduced the Air-Land Battle doctrine, emphasising simultaneous multi-domain engagement. The 1990s saw Network-Centric Warfare, using real-time data, surveillance, and precision targeting for better decision-making.

In the 21st century, with growing cyber, space, and electromagnetic threats, MDO became a formal strategy—integrating all domains for dynamic, synchronized operations. Conflicts like the Russia-Ukraine war affirm MDO's strategic value.

India's need for MDO has grown amid rising challenges from China's cyber and grey-zone tactics and Pakistan's proxy warfare. Reforms like appointing the CDS, forming Integrated Theatre Commands, and establishing cyber and space agencies mark progress. Moving forward, India must focus on integrated doctrines, stronger jointness, and technological investments to prepare for the future. **Figure 1** illustrates the historical trajectory of MDO—from early joint operations to the AI-driven network-centric warfare of today.

Figure 1: Evolution of Multi-Domain Operations



Concept of MDO

Domain refers to a vital area of operation wherein gaining access and maintaining control are crucial for achieving mission objectives and operational flexibility. MDO emphasises the coordinated efforts of all military branches to challenge adversaries across these domains. Beyond tactics, MDO influences broader defence strategies, including equipment acquisition and recruitment and training of personnel (Farley, 2019).

MDO is not just conducting operations in all these domains separately, an actual MDO is when all domains collaborate and create effects as desired—"Using dominance in one domain or many, blending a few capabilities or many, to produce multiple dilemmas for our adversaries in a way that will overwhelm them."

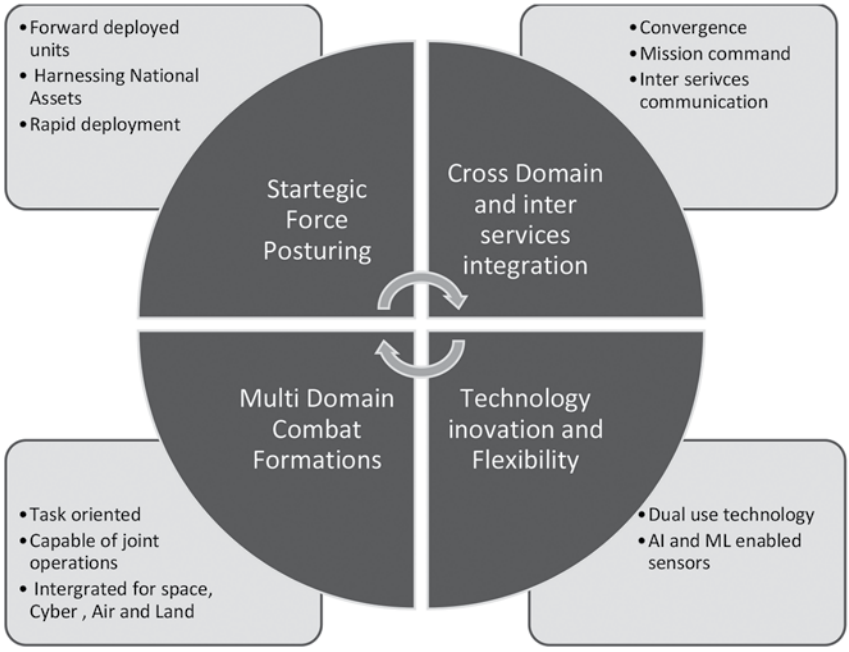
MDO is the Army's modern approach to warfare, focused on integrating capabilities across land, air, sea, space, cyber, and the electromagnetic spectrum. It seeks to gain a strategic edge by coordinating all elements of combat power to deter, defeat, or respond effectively to adversaries across the full range of conflict. Designed in response to emerging global threats, MDO enables forces to operate seamlessly across domains, ensuring flexibility and faster decision-making. It influences how the Army equips, trains, organizes, and deploys its forces.

Imperatives of MDO

- ***Strategic Force Posturing.*** This tenet involves the deliberate positioning of forward-deployed units, rapidly deployable expeditionary elements, and high-level national assets. The aim is to ensure readiness, enable quick escalation or de-escalation, and apply command authorities effectively across all theatres of operation.
- ***Cross-Domain and Inter-Service Integration.*** Defence forces must function as a single cohesive unit. Joint planning, integrated commands, and seamless information flow between services are vital. This tenet asserts that only MDO enables cross-domain synergy, layered options, and mission command to effectively counter adversaries.
- ***Technological Innovation and Flexibility.*** India needs multi-role, modular platforms for use across domains and services. Emphasis should be on indigenous development of AI-enabled systems, smart sensors, and adaptable weapon platforms.
- ***Multi-Domain Combat Formations.*** These are task oriented units capable of independent operations in contested environments. They

integrate joint fires across domains viz. land, air, sea, cyber, and space and are structured to exploit the full range of human capabilities, enhancing combat agility and resilience. **Figure 2** illustrates the four imperatives of MDO.

Figure 2: Imperatives of MDO



Initiatives Taken for Enabling MDO

Appointment of the Chief of Defence Staff (CDS) and Creation of DMA. The appointment of General Bipin Rawat as India's first Chief of Defence Staff (CDS) and creation of the Department of Military Affairs (DMA) in 2020 was a pivotal step in India's journey towards integrated military operations.

Progress Towards Integrated Theatre Commands (ITCs). The proposed Integrated Theatre Commands (ITCs) will unify command and control

structures across geographical and functional domains, enhancing India's ability to respond to threats effectively.

Proposed Theatre Commands:

(a) **Western Theatre Command:** Focused on countering threats from Pakistan including proxy warfare.

(b) **Northern Theatre Command:** Manages the China border with focus on high altitude readiness, satellite surveillance, real-time intelligence, and swift multi-domain coordination.

(c) **Maritime Theatre Command:** Supports naval-led missions in the Indian Ocean with Army contributions in coastal defence, UAV use, and amphibious preparedness.

(d) **Air Defence Command:** Brings together national air defence under one structure, with Army units enhancing radar coverage and ground-based aerial threat responses.

Raising of Niche Capability Structures. To address critical capability voids in the domains of Space, Cyber and Special Forces Capabilities, niche capability structures in terms of Defence Space Agency, Defence Cyber Agency & Armed Forces Special Operations Division have been raised in 2018-19.

Evolving Joint Doctrines and Protocols. India's 2017 Joint Doctrine laid the groundwork for integrated military operations, emphasising jointness among the three services. To advance towards comprehensive MDO, a more adaptive doctrine is necessary.

Integration of Emerging Technologies in MDO

Artificial Intelligence (AI) is central to Multi-Domain Operations (MDO), enabling rapid and accurate decisions across land, air, sea, cyber, and space. It enhances situational awareness and helps collate vast amount of sensor data. AI-powered autonomous systems respond faster than

humans in high threat scenarios, improving survivability. Some of the niche technology domains are discussed here:

(a) **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML are transforming military operations by enabling faster, data driven responses and smarter resource management. The Indian defence ecosystem is increasingly adopting these technologies to enhance MDO readiness. AI-driven Decision Support Systems (DSS) are being used to process large volumes of battlefield data to offer timely, actionable insights. Autonomous platforms equipped with AI are improving both surveillance and strike capabilities. Furthermore, machine learning models are being applied in cybersecurity to monitor networks and detect anomalies in real time, thus improving resilience against evolving digital threats.

(b) **Cyber and Electronic warfare:** Cyber and Electronic Warfare (EW) technologies are pivotal in enhancing the effectiveness of Multi-Domain Operations (MDO) by enabling seamless integration across various operational domains.

   (i) In the cyber domain, offensive and defensive operations serve as force multipliers. India is increasingly focusing on cyberspace operations, from both national and military perspectives, recognising their strategic importance in contemporary warfare. These operations are crucial for defending critical Information and Communication Technology (ICT) infrastructure and for achieving superiority in MDO.

   (ii) Recent conflicts have highlighted the vital role of Electronic Warfare (EW) in Multi-Domain Operations (MDO). In the Russia-Ukraine war, Russia deployed systems like Krasukha-4 and Leer-3 to jam GPS, disrupt UAVs, and interfere with communications. Ukraine, with NATO' support, used spectrum-monitoring tools and jammers to counter these

threats, showcasing the strategic value of electromagnetic dominance.

(iii) The integration of cyber and EW technologies into MDO frameworks ensures that India can effectively counter multifaceted threats by enabling real-time data sharing, disrupting adversary command & control structures, and safeguarding its own communication networks.

(c) **Space Technology as a Strategic Force Multiplier:** Space has the advantage of being the common frontier over land, sea and air, thus, it can act as an enabler and facilitator for implementing MDO. Space as a frontier can overlap various coordination functions (communications, ISR, etc.) of the three services; assist in greater jointness and integration lending to theaterisation functionality, cross domain operations, command and control (C2).

(d) **Advanced Communication Technologies:** Reliable and secure communication is vital in MDO. Technologies like software-defined radios and integrated sensor-shooter networks facilitate real-time data sharing and coordination across services and domains, ensuring cohesive and timely responses.

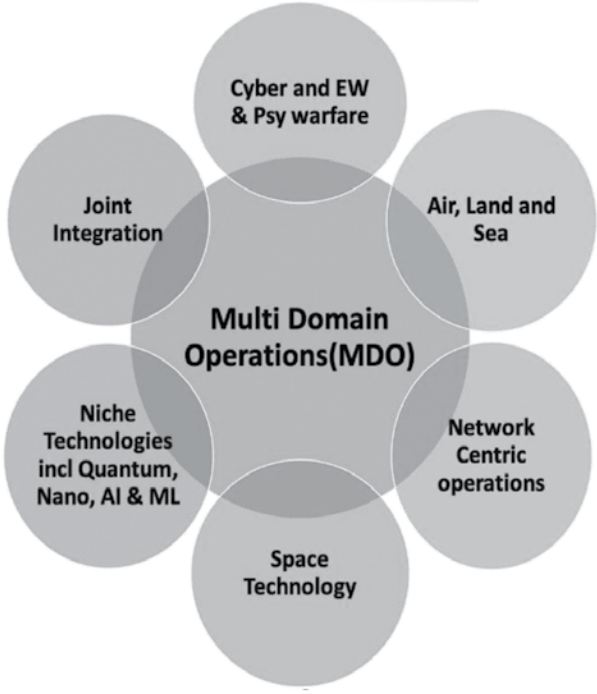
(e) **Hypersonic Weapons:** With unmatched speed and manoeuvrability, hypersonic weapons are highly destructive and difficult to intercept. Unlike traditional ballistic missiles, their ability to change trajectory mid-flight adds to their unpredictability, enhancing their effectiveness in striking high-value targets across domains.

(f) **Directed Energy Weapons (DEWs):** These systems, including high-energy lasers, provide precise targeting capabilities with minimal collateral damage. They are especially effective against fast-moving platforms like drones and missiles. DEWs also hold potential for targeting satellites and other space-based assets due to their near-instantaneous strike capability.

(g) **Nanotechnology:** Nano-enabled materials are being developed to improve the durability and functionality of military equipment and soldier gear. Embedded nano-sensors contribute to better battlefield awareness by continuously gathering and transmitting environmental and operational data.

(h) **Quantum Technologies:** Quantum advancements are set to revolutionise secure communication, navigation, and computing in military operations. Quantum computers can rapidly process complex calculations, making them useful in encryption and wargaming. Additionally, quantum sensors offer reliable navigation in environments where GPS signals are jammed or unavailable. **Figure 3** illustrates the various enablers of MDO.

Figure 3: Enablers of Multi-Domain Operation



Strategic Implications

Multi-Domain Operations (MDO) enhance India's strategic deterrence by enabling real-time, coordinated responses across land, air, sea, cyber, and space. They also bolster India's regional influence in the Indo-Pacific. Key strategic implications include:

(a) **Redefining Warfare Paradigms:** MDO marks a shift from traditional single/dual-domain warfare to integrated, multi-domain operations, requiring a rethinking of India's strategic doctrines to address unrestricted warfare.

(b) **Whole-of-Nation Integration:** Effective MDO demands synchronised use of all instruments of national power—military, diplomatic, economic, informational, and legal.

(c) **Enhanced Strategic Deterrence:** Operating across multiple domains complicate adversaries' planning and leverages India's asymmetrical advantages, especially in cyber and space.

(d) **Capability Development:** MDO drives the need for modular, cross-domain systems, influencing R&D, procurement, and force structure to ensure interoperability and agility.

(e) **Organisational Reforms:** It calls for restructuring of higher defence organisations, enabling better joint planning, command, and policy integration across services.

(f) **Cognitive Domain as a Strategic Frontier:** The cognitive battlespace, manipulating perceptions, spreading misinformation, and targeting decision-making is increasingly vital. Strategically, India must develop capabilities for influence operations, counter-narratives, and perception management on a national scale.

Tactical Implications

MDO enhances tactical flexibility by enabling seamless coordination across domains at the unit level. It allows ground forces to leverage air, cyber, and space assets for precision strikes, rapid manoeuvre, and

real-time intelligence. Tactical implications in the Indian context are enumerated as under:

(a) **Joint Tactical Manoeuvrability:** Tactical units must be capable of operating seamlessly across domains. Ground forces to direct air or naval fire; cyber units will support kinetic operations; and Special Forces leverage integrate space based assets for targeting or ISR.

(b) **Short-lived Tactical Superiority:** In contested domains, tactical advantages are transient. Commanders must exploit brief moments of domain dominance through synchronised, rapid, and decisive action.

(c) **Cyber and EW Integration at the Tactical Level:** Cyber and electronic warfare elements must be embedded within tactical formations to degrade enemy capabilities in real-time, protect own assets, and support manoeuvre.

(d) **Dynamic Command and Control (C2):** C2 systems must be agile, joint, and data-driven, with predictive tools and AI/ML-enabled decision support. Tactical leaders require real-time situational awareness across domains.

(e) **Operational Fires and Special Forces Synergy:** Employment of long range vectors, supported by cyber, space, and Special Forces, enables deep strikes and penetration. These synchronous operations support deep thrusts.

Table 1: SWOT Analysis of India's Preparedness for MDO

Strength	Weakness
1. **Institutional Reforms.** Establishment of the Chief of Defence Staff (CDS), Integrated Theatre Commands (ITCs), and Department of Military Affairs (DMA).	1. **Lack of MDO oriented Joint Doctrine.** Absence of a joint warfighting doctrine oriented towards MDO scenarios.

2. **Growing Technological Capabilities.** Advancements in indigenous space-based ISR, cyber infrastructure, and Electronic Warfare (EW) systems (e.g. Himashakti, Samyukta) to strengthen India's domain integration.	2. **Slow Technology Absorption.** Limited integration of AI, quantum tech, and advanced cyber tools in operational forces; combat cloud and sensor-fusion capabilities remain nascent.
3. **Operational Experience in Hybrid Warfare.** Decades of counterinsurgency, border skirmishes, and limited wars (e.g. Kargil, Galwan).	3. **Service-Centric Mindsets.** Inter-service rivalry and siloed modernisation approaches delay full spectrum integration and joint capability development.
4. **Defence Industry Base.** Growing collaboration with DRDO, ISRO, and private defence firms under initiatives like 'Make in India' is boosting self-reliance in key technologies.	4. **Inadequate Infrastructure for Space and Cyber Domains.** Persistent gaps in space situational awareness, cyber deterrence, and electromagnetic spectrum dominance.

Opportunities	Threats
1. **Emerging Technologies.** AI/ML, autonomous systems, quantum computing, and hypersonic weapon technologies have potential for Indian MDO development.	1. **Adversarial Advances.** China's rapid strides in AI, space, cyber, and EW, and Pakistan's asymmetric tactics, presents multi-domain threats.
2. **Strategic Partnerships.** Collaborations with the US, France, Israel, and Japan provide access to advanced technologies and joint exercises that enhance inter-operability.	2. **Cyber & EW Vulnerabilities.** Increasing dependence on digital networks creates exposure to state sponsored cyber attacks and information warfare.
3. **Private Sector Innovation.** Startups and tech companies offer potential to fast-track indigenous solutions in EW, cybersecurity, and ISR.	3. **Technological Asymmetry.** Delay in indigenous development widens the gap with technologically advanced adversaries, impacting strategic deterrence.

4. **Global MDO Trends.** India's MDO development can align with global doctrines, enabling interoperability in multilateral operations (e.g. QUAD, Indo-Pacific coalitions).	4. **Budgetary Constraints.** Competing national priorities impedes sustained investment in high-end technology and MDO infrastructure.

Comparison of India and China's MDO Capabilities

India and China are both progressing in Multi-Domain Operations (MDO), but at differing scales and strategic focus. China has achieved a more advanced level of integration through its Joint Operations Command System (JOCS) under the Central Military Commission, supported by structural reforms and real-time command-and-control capabilities. The People's Liberation Army (PLA) has centralised cyber, electronic, and psychological warfare under the Strategic Support Force (SSF), enabling seamless integration of non-kinetic domains. China's space independence, demonstrated by BeiDou and anti-satellite tests, and its widespread use of AI facilitated by civil-military fusion—enhance its cognitive warfare capabilities. India, while making progress, is still in the foundational stage. Initiatives like the creation of the CDS, DMA, and planned Integrated Theatre Commands are steps forward, but a unified MDO doctrine is still missing. Challenges persist in inter-service coordination and in scaling AI, cyber, and space technologies. Although India is developing indigenous solutions in AI and EW, it falls behind China in quantum technology, hypersonics, and combat cloud integration. Strategically, India focuses on regional defence and deterrence, while China's MDO is aimed at global influence and continuous peacetime competition. Thus, China's MDO posture is more centralised and technologically cohesive, while India remains in the phase of structural alignment and capability development.

Timelines for Implementation of MDO in India

The MDO implementation timelines provides a structured roadmap for India's transition into a fully integrated, technologically enabled, and strategically agile military force. Spanning from 2025 to 2035, the matrix outlines key phases viz. Foundation, Integration, and Dominance—each addressing critical areas such as doctrine development, organisational restructuring, technological modernisation, and international cooperation.

(a) **Phase I: Foundation (2025–2027)**

(i) **Objective:** Establish the doctrinal, structural, and technological base for MDO.

(ii) **Doctrine & Strategy:** Formulate a unified MDO doctrine integrating land, air, sea, space, cyber, and electromagnetic domains.

(iii) **Organisational Reform:** Operationalise Integrated Theatre Commands (Western, Northern, Maritime, Air Defence).

(iv) **Cyber & Space Readiness:** Operationalise Defence Cyber Agency and Defence Space Agency which was initiated in 2018–19.

(v) **AI & C2 Systems:** Begin fielding AI-enabled Decision Support Systems (DSS) for situational awareness and coordination.

(vi) **Training:** Introduce joint multi-domain warfare training across tri-service academies and simulation centres.

(vii) **MDO Policy Development:** Initiate drafting of a national MDO policy integrating inputs from MOD, DRDO, ISRO, NSCS.

(b) **Phase II: Integration (2028–2031)**

(i) **Objective:** Achieve functional integration of capabilities and mature institutional collaboration.

(ii) **Technological Upgrades:** Expand secure digital infrastructure (e.g. BharatNet, quantum-encrypted networks).

(iii) **Civil-Military Fusion:** Accelerate public private MDO partnerships under iDEX and DIO to develop indigenous AI, EW, and space technologies.

(iv) **Joint Operations and Excercises:** Conduct large-scale joint MDO exercises simulating hybrid threats across LAC and LoC.

(v) **Legal & Inter Ministerial Synergy:** Establish legal frameworks for space and cyber operations and enable robust inter agency coordination.

(vi) **Global Outreach:** Deepen strategic ties with QUAD, France, Israel, and the US for technology transfer and joint capability development (e.g. BECA, COMCASA)

(c) **Phase III: Dominance (2032–2035)**

(i) **Objective:** Operationalise full-spectrum, real-time MDO across all theaters.

(ii) **Combat Systems:** Deploy directed energy weapons, hypersonics, and quantum communication systems in critical theaters like Siachen, IOR etc.

(iii) **ISR Dominance:** Expand satellite based ISR capabilities for real-time, cross-domain intelligence sharing.

(iv) **Cognitive Warfare:** Institutionalise narrative management and psychological operations for cognitive domain dominance.

(v) **Civil-Military Fusion:** Institutionalise lateral entry of tech experts and enhance AI, robotics, and sensor-driven C2 networks.

(vi) **Multilateral Engagements:** Shape international norms for non-kinetic warfare domains and lead global MDO collaborations (RIMPAC, Malabar, BRICS).

Doctrinal and Organisational Changes

Formulating a Joint MDO Doctrine: India needs to establish a clearly defined, integrated doctrine for Multi-Domain Operations that covers all

domains viz. land, air, sea, cyber, space, and the electromagnetic spectrum. Current coordination among the armed forces is largely situational and lacks a formal, doctrinal foundation.

Structural Integration for Operational Synergy: Though India has initiated structural changes like Integrated Theatre Commands and specialised cyber and space units, the military still largely operates within traditional, service-specific frameworks. For MDO to be effective, these structures must evolve into truly joint operational commands capable of synchronised action across domains.

Modernising Command and Control Systems: Achieving multi-domain integration requires a digitised, responsive command-and-control (C2) system. Enhanced situational awareness, digital coordination between land and air forces, and real-time cross-domain decision-making tools, ideally supported by AI and secure networks, are essential to facilitate MDO.

Fostering Civil-Military Collaboration: Partnerships with academia, startups, and research organisations are *sin qua non* for evolution of MDO in the Indian context. A well-defined roadmap should identify technological focus areas like AI, cyber, space technology, quantum computing, secure communication, and robotics.

Building a Tech enabled, Multi-Domain Ready Force: To operationalise MDO, India's Armed Forces must develop a tech enabled, cross-domain capable force. Simultaneously, inducting experts in AI, cyber, space, and electronic warfare will bridge the gap between innovation and battlefield use cases, guiding the integration of emerging technologies into operations.

Policy Framework and International Cooperation

Establishing a Unified National MDO Policy Framework: This policy should align with the core principles of MDO i.e. jointness, integration, agility, and dominance across all operational domains. The framework

must incorporate inputs from the Ministry of Defence, National Security Council Secretariat (NSCS), DRDO, ISRO, and other national agencies.

Inter-Ministerial Coordination and Legal Infrastructure: An effective MDO policy needs coordination across key ministries to unify cyber, space, and information warfare efforts. Legal frameworks must adapt to define rules, attribution, and deterrence in non-traditional domains.

Strengthening Civil-Military Fusion and R&D Ecosystems: Initiatives like Innovations for Defence Excellence (iDEX) and Defence Innovation Organisation (DIO) should be expanded and aligned to MDO specific objectives. This will enhance indigenous development of technologies critical to MDO, such as AI enabled C2 Systems, robust networks, space based ISR, and EW.

International Cooperation and Strategic Partnerships: Global collaboration is essential to strengthen India's MDO capabilities. Strategic partnerships with countries like the US, France, Israel, Japan, and members of the QUAD offer avenues for joint development, technology transfer, interoperability exercises, and doctrinal alignment.

Participation in Multilateral Defence Platforms: India should actively engage in multilateral military platforms and exercises focused on multi-domain scenarios (e.g. RIMPAC, Malabar, and Cobra Gold). These forums not only enhance interoperability but also expose Indian forces to best practices in MDO execution and innovation.

Soft Power as a Strategic Enabler in MDO: Soft power serves as a vital complement to Multi-Domain Operations (MDO), especially in shaping perceptions and influencing the cognitive domain. Through diplomacy, culture, media, and strategic communication, India can strengthen deterrence and support its strategic goals. Participation in global platforms like the G20, Quad, and BRICS helps India build alliances, challenge and question hostile narratives, and promote responsible behaviour in cyber, space, and information domains.

Conclusion

Multi-Domain Operations (MDO) represent a decisive shift in India's military strategy, aimed at integrating capabilities across land, air, sea, space, cyber, and the electromagnetic spectrum. In an era marked by hybrid threats and technological disruptions, MDO empowers India to respond swiftly and effectively across all theatres of conflict. India's institutional reforms, doctrinal evolution, and adoption of cutting-edge technologies underscore its commitment to building a future-ready force. Strengthening jointness, enhancing inter-agency coordination, and leveraging international partnerships will be critical. A well-orchestrated MDO framework will enable India to secure its strategic interests and maintain superiority in a complex security environment.

> *India is moving ahead with the vision of a modern and self-reliant military that can respond effectively in all domains—land, air, sea, space, and cyber.*
>
> – Prime Minister Narendra Modi, Def Expo 2022

References

ABB/Anand. (2024, June 18). https://pib.gov.in/PressReleasePage.aspx?PRID=2026240. Retrieved April 2025, from https://pib.gov.in: https://pib.gov.in/PressReleasePage.aspx?PRID=2026240

Brar, L. G. (2024, February). Mosaic Warfare: Space as Enabler in the Indian Context. *Synergy,* 3(1), 192-205.

Chaithanya, A. S. (2024, July). Offensive and Defensive Cyber Operations in Multi Domain Battle space. *AIR POWER*, 19(3), 93-115. Retrieved from https://capsindia.org, https://capsindia.org/wp-content/uploads/2024/10/Abhinay-Shukla-and-VSV-Chaithanya.pdf?

Chaturvedi (Retd), M. G. (2025, April 13). https://sundayguardianlive.com/opinion/lessons-for-india-as-importance-grows-of-electronic-warfare-in-modern-conflicts. Retrieved April 2025, from https://sundayguardianlive.com: https://sundayguardianlive.com/opinion/lessons-for-india-as-importance-grows-of-electronic-warfare-in-modern-conflict

Collins, M. (2025, January). https://www.mirasafety.com/blogs/news/hypersonic-missile-update. Retrieved April 2025, from https://www.mirasafety.com: https://www.mirasafety.com/blogs/news/hypersonic-missile-update?

Cox, D. G. (2021, May). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2021/Cox-AI-MDO/. Retrieved April 2025, from https://www.armyupress.army.mil, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2021/Cox-AI-MDO/

Defence, P. I. (2020, February 20). Creation of New Department of Military Affairs. *Creation of New Department of Military Affairs*. New Delhi, India: Press Information Bureau, Government of India.

Delhi, P. (2022, February 4). https://pib.gov.in/PressReleasePage.aspx?PRID=1795536. Retrieved March 2025, from https://pib.gov.in, https://pib.gov.in/PressReleasePage.aspx?PRID=1795536

Delhi Defence Dialogue, 2. (2024, November 12-13). https://www.idsa.in/wp-content/uploads/2025/03/booklet-ddd.pdf. Retrieved April 2025, from idsa.in: https://www.idsa.in/wp-content/uploads/2025/03/booklet-ddd.pdf

Farley, J. D. (2019). "Defining the 'Domain' in Multi-Domain', 'Security Community'", *into Air & Space Power Conference 2019*, Germany.

Lt Gen (Dr) N. B. Singh, P. A. (2024, August). Multi Domain Operations: Creating Capability Overmatch. *Synergy,* 3(2), 80-93.

Mohiuddin, M. A. (2024, September 30). https://indiaai.gov.in/article/ai-driven-tools-in-the-indian-defense-sector. Retrieved April 2025, from https://indiaai.gov.in: https://indiaai.gov.in/article/ai-driven-tools-in-the-indian-defense-sector

New America editorial. (2020). *A Summary of Multi-Domain Operations*. Retrieved April 2024, https://www.newamerica.org, from https://www.newamerica.org/future-security/reports/army-and-multi-domain-operations-moving-beyond-airland-battle/a-summary-of-multi-domain-operations/

Sagar, P. R. (2024, September 10). https://www.indiatoday.in/india-today-insight/story/india-set-for-its-biggest-military-reform-as-integrated-theatre-commands-await-final-govt-nod-2597327-2024-09-10. Retrieved April 2025, from indiatoday.in, https://www.indiatoday.in/india-today-insight/story/india-set-for-its-biggest-military-reform-as-integrated-theatre-commands-await-final-govt-nod-2597327-2024-09-10?

Service, C. (2024, October 1). *Defense Primer: Army Multi-Domain Operations (MDO)*. Retrieved April 2025, https://crsreports.congress.gov: https://crsreports.congress.gov/

Singh, L. C. (2024, August). Technology Driven Multi Domain Operations (MDO) for Joint Warfighting. *Synergy,* 3(2), 94-109.

Singh (Retd), L. G. (2024, July 2). Competing Forces: Evaluating Military Capabilities of India and China. *Delhi Policy Group,* IX(15), 1-23.

Singh, A. (2021, November 20). *Multi Domains Operations and India (Part 1)*. Retrieved April 2025, from https://wavellroom.com, https://wavellroom.com/2021/11/10/multi-domain-operations-india-1/

Uppal, R. (2020, October 20). *Quantum Navigation is Emerging Technology for GPS-denied and Deep Space Environments*. Retrieved April 2025, from www.idstch.com, https://idstch.com/technology/quantum/quantum-navigation-emerging-technology-for-gps-denied-and-deep-space-environments/

Civil-Military Fusion: Necessity for Future Conflicts

Vivek Singh

"War is politics by other means"

– Clausewitz

Abstract

Civil-Military Fusion (CMF) has emerged as a defining strategic necessity for modern states confronting hybrid, non-linear and technology-driven conflicts. It aims to integrate civilian and military capabilities to enhance a nation's comprehensive power. India has demonstrated a considerable progress towards achievement of CMF in last decade which accrued concrete dividends during Operation Sindoor. India's journey towards Viksit Bharat 2047 demands that CMF must become a doctrinal and institutional reality. The fusion of governance, technology, academia, industry and the Armed Forces will transform India from a continental power into a comprehensive security provider and a global shaper of stability.

Colonel **Vivek Singh** was commissioned into the Rajputana Rifles Regiment in June 2002. He commanded his unit in Eastern Sector & Western Borders and has served in various Staff appointments at Brigade & Corps Headquarters and Directing Staff at Army War College, Mhow. Views expressed are personal.

Introduction

Civil-Military Fusion (CMF) has emerged as a defining strategic necessity for modern states confronting hybrid, non-linear and technology driven conflicts. It aims to integrate civilian and military capabilities to enhance a nation's comprehensive power. The primary goal is to close the gap between civilian & defence sectors to support military modernisation and overall economic growth of the country. It is focused on strengthening all instruments of national power to prevail in strategic competition in synchronisation with national interests.

Historical Voyage of CMF

Civil–Military synergy is deeply rooted in Indian statecraft. In ancient India, civil and military domains were intertwined as seen in Arthashastra, where Chanakya envisioned the strength of the state arising from the seamless alignment of governance, economy and defence. His principles of a strong treasury (kosha), effective logistics and multi-dimensional strategies (Sama, Dana, Danda, Bheda) reflect early concepts of CMF. This shows a strategic understanding that a nation's strength depends on the seamless alignment of all its components—both civil & military, to achieve state objectives. Ancient Indian statecraft also professed collusion of Shaastra (intellect) & Shastra (weaponry) which formed the basis of military education. Throughout ancient Indian history, the mobilisation of a kingdom's entire resources for warfare was a central tenet of statecraft, as elucidated in the Arthashastra.

Historically, empires that excelled at fusing civil & military capacities like Mauryan, Gupta and later colonial powers built resilient and expansive systems. The British East India Company's fusion of commercial and military might exemplify CMF's power in shaping geopolitical dominance. In the modern era, World War II catalysed the United States' CMF through coordinated mobilisation of science, industry and military production. In the 21st century, China has institutionalised CMF as a

core element of national rejuvenation, using it to propel innovation, dual-use technology and military-industrial modernisation.

Demystifying Civil-Military Fusion

Modern warfare extends far beyond kinetic battles. Political, economic, informational and technological domains have become integral parts of modern conflict. A whole of nation's approach is now indispensable. CMF transforms this approach into practice by fusing technology, governance, talent and national will into one strategic instrument. CMF has become increasingly relevant in contemporary conflicts wherein battles have permeated into the societal space, information spheres, cognitive domain and technology revolution necessitating transformation in military affairs. CMF is essentially the fusion of civilian & military resources and capabilities for optimising a nation's comprehensive national power. It is leveraging of close relationships between politicians, bureaucrats, defence sector, academia, private sector and the media cohesively to achieve national objective. Success for CMF entails dissolving the silos created amongst various verticals and establishing effective linkages with mutual trust. It is a transition from employment of 'talent from anywhere' to 'talent from everywhere'. The modern conflicts in various parts of the globe have reflected CMF as not only the force multiplier, but a pre-requisite to tackle future conflicts.

China has rolled out a prototypical model for CMF that stands them out from rest of the world. The term Civil-Military Fusion (CMF) or Military-Civil Fusion (MCF) depending on which agency takes the lead, first emerged in the late 1990s, when Hu Jintao, then Vice Chairman of the CCP's Central Military Commission, used the term to describe the coordination between civil and military domains. It was the concept applied primarily for converting military factories over to civilian production under the backdrop of the economic reform, which failed to bring innovative commercial technologies into the military sector.

The CMF efforts under Xi Jinping are more robust & have been more effectively executed. Certain areas of development in China's military-industrial complex definitely witnessed major benefits from the military-civil integration, particularly for shipbuilding, information technology and aerospace industry.

CMF is a concept of practical utility which is the key ingredient of modern statecraft as well as warcraft. It is the heart of overall national security framework. The Hon'ble Raksha Mantri, Sri Rajnath Singh, aptly noted that "traditional defence outlooks are no longer sufficient. The world today is moving beyond division of labour towards integration of purpose." CMF is thus, not just organisational integration, but is a strategic enabler that propels innovation, sustains talent and enhances technological self-reliance. For India, CMF is vital to achieving technological self-reliance, accelerating defence modernisation and aligning national instruments like diplomatic, information, military and economic towards achieving common security goals. Operation Sindoor has demonstrated the operational dividends of this fusion revealing how indigenous innovation, political-military synergy and multi-domain coordination can redefine India's strategic posture. Institutionalising CMF as a doctrinal and structural framework is, therefore, essential to prepare India for future challenges and realize the vision of *Viksit Bharat 2047*.

Display of CMF during Operation Sindoor

Operation Sindoor, launched in May 2025 following Pakistan's barbaric attack on civilians at Pahalgam, was a defining demonstration of CMF in action. Without crossing the Line of Control or International Boundary, India delivered calibrated, precise and multi-domain strikes that neutralised terrorist infrastructure. Beyond its military success, the operation showcased India's evolving national security architecture and the dividends of Atmanirbharta. Indigenous systems like Akash Air Defence, BrahMos missiles, ISR platforms, communication network

and loitering munitions did perform flawlessly, thereby, proving India's capacity for self-reliance and effective jointness in Tri-Service operations.

Operation Sindoor demonstrated new maturity in India's doctrine and evolving strategic posture. The execution of the operation displayed a considerable level of civil-military synergy—an important instrument for tackling modern conflicts. The operation exemplified seamless political direction, operational autonomy and inter-agency coordination. Real time data from ISRO satellites, surveillance drones developed under iDEX initiatives and coordinated cyber operations reflected integration across ministries, industry and academia. The harmony displayed amongst the Diplomacy, Information, Military and Economy (DIME)—the four pillars of national security, at all stages was unparalleled. It exhibited fusion of military precision, diplomatic agility, informational superiority and economic leverage. The operation was a testament of India's Atmanirbhar capability development and in-depth understanding of the transformative changes being pursued to deal with the disruptive changes in the technology-driven modern warfare.

Diplomatically, all-party parliamentary delegations reinforced India's unified national stance, while international outreach explained the legitimacy and restraint of India's response. Narrative warfare was managed with professionalism through joint briefings, verified visuals and proactive social media campaigns ensuring control over global perception. Operation Sindoor also highlighted non-kinetic instruments of national power like civil defence drills coordinated by the Ministry of Home Affairs, economic measures such as suspension of trade and the Indus Waters Treaty (IWT) and rapid mobilisation of internal agencies, all reflects a mature and fused approach to national security.

Way Forward for India

India has demonstrated a considerable progress towards achievement of CMF in last decade which accrued concrete dividends during Operation

Sindoor. It has made significant progress in embedding CMF principles through reforms such as the creation of the Chief of Defence Staff (CDS) and Department of Military Affairs (DMA), defence industrial corridors and the iDEX ecosystem. We, however, need to formulate a national CMF policy under the National Security Council Secretariat to synchronize all elements of national power. India's vision of '*Sashakt & Saksham Bharat*' by application of mantra of 'Jointness-Atmanirbharta-Innovativeness' (JAI) can be timely achieved by instituting doctrinal reforms at the Apex level and execution at the functional level. Some of the recommended institutional reforms and suggested roadmap is enumerated as under:-

Organisational Reforms

- **Establish a Comprehensive National Strategy**. Develop a top-down Politico-Military-Bureaucratic-Corporate fusion policy, that formalises a 'Whole of Nations' approach to be infused as doctrinal construct. This must incorporate civil-military fusion into long-term strategic defence planning to address hybrid and asymmetric threats including Grey Zone Warfare.
- **Improve Sharing Inputs on National Security**. Expand integration across civil agencies, state governments and National Security Council to ensure real-time, multi-source intelligence flow. Further reforms in the National Security Council and its advisory board with broader canvas of participation to ensure holistic involvement in advisory and planning.
- **Cross Pollination**. Ensure cross postings in departments involved in national policy making having a bearing on national security beyond DMA/MoD to facilitate mutual understanding of interests. Presence of military officers in Niti Aayog as advisors will go a long way in correct planning for projects related to national security. It will be a good step to establish Military Advisory Cells under Chief Secretaries for state-level security planning. Billeting of serving and retired

military officers as advisors in all important ministries is a necessity for improvement of ecosystem.

- **Create Integrated Theatre Commands**. There is a need to accelerate creation of Theatre Commands for multi-domain joint operations and unified logistics. Maritime Theatre Command should be the first one to come up to extend our reach into the Indo-Pacific domain which witnesses 70% of world trade transmission.

Boosting Defence Technology and Innovation

- **Public - Private Partnership**. Review the efficiency of the Defence Research and Development Organisation (DRDO) and push for a stronger public-private partnership (PPP) model. Incentivize DRDO and Defence Public Sector Undertakings (DPSUs) to collaborate with the private sector on design and technology development rather than relying solely on licensed production. Focus on building capability clusters for key sectors like space and emerging technologies such as Artificial Intelligence (AI), robotics, cyber and unmanned systems.
- **Procurement Reforms.** Reform policies and archaic procedures to mitigate bureaucratic hurdles. A dedicated Defence Procurement Board at various levels with members from varied strata i.e. user, technical experts and auditors who matter in the entire process could help speed up contracts and approvals. The archaic procedures and manuals need to be amended duly, with an aim at exploring technology for procurement, rather than time taking audits at each stage. The procurement cycle loops needs to be shortened to ensure matching pace with technological transformations.
- **Ease Access for the Private Sector**. Formulation of better ecosystem to promote investment by private players and Startups in defence sector will garner greater technological revolution, and thus, promote innovativeness and Atmanirbharta in the defence sector.

- **Incentivise Innovation**. Provide long-term funding commitments and incentivised procurement process for promising startups and MSMEs. Encourage innovation within the armed forces through initiatives which helps military personnel incubate their ideas with startups and academia. Focusing on domain specialisation and project based continuity will incentivise innovations further.
- **Data Sharing**. Reform policy directives to allow the military to share non-classified data with private firms and academic institutions with appropriate safeguards like Non-Disclosure Agreements.

Human Resource Development and Training

- **Promote Lateral Entry**. Encourage and institutionalise a 'revolving door' system that facilitates exchange of human resource between the military, civilian departments and private industry. This will allow military to tap into a wider pool of talent as also facilitate smooth transition of retired military personnel into civilian work force facilitating linkage for better mutual understanding.
- **Participation in Discussions**. All stakeholders—diplomats, bureaucrats, technocrats, space, cyber, academia and media should participate in various discussions/conclaves to ensure improved linkages. Regular wargaming of whole of nations approach with all stakeholders on board will develop better mutual understanding and ensure real time audit of the concept.
- **Cross Attachments**. A compulsory 1 to 3 months of cross attachment with military for all civil services & technocrats in the last year of their course based on 'call of duty concept' will go a long way in mutual understanding of the culture & military requirements. Similar cross attachment of military officers with civilian undertakings based on domain specialisation will be beneficial for understanding their strengths and challenges.

- **Participation in Courses**. Increasing civilian participation from bureaucracy, academia, technocrats and industry in various military courses will garner better mutual understanding. Similar reciprocal response from civil counterparts in their courses for military will establish better linkages.
- **Modernise Training Methods**. Collaborate with academia and private enterprises to introduce cutting-edge training methodologies including simulators, gamification and augmented/virtual reality packages.

Logistics Integration

- **Create Dual-Use Infrastructure**. Central and State Governments should build civil infrastructure like airports, ports, roads, warehouses, rail network & communication networks to military requirements, allowing dual civilian-military use. Projects like PM Gati Shakti, Bharat Mala & Sagar Mala should co-opt military requirements diligently, while planning and execution, to ensure its judicious utilisation by both.
- **Enhance Integrated Logistics**. Expand the number of Joint Logistics Nodes (JLNs) beyond inter-defence services to co-opt civil governments across the country to improve efficiency in resource utilization and interoperability.

Conclusion

Civil-Military Fusion is the heart of modern national security wherein innovation, integration and intent converge to secure the nation's future. It is essentially the fusion of civilian & military resources and capabilities for enhancing comprehensive national power. While India has entrenched numerous steps in its system towards institutionalising the framework by steering concepts like JAI (Jointness-Atmanirbharta-Innovativeness), but

a well laid out concrete path at the Apex level will facilitate its formal embedment into the system. India's journey towards *Viksit Bharat 2047* demands that CMF must convert into a doctrinal and institutional reality. The fusion of governance, technology, academia, industry and the Armed Forces will transform India from a continental power into a comprehensive security provider and a global shaper of stability. All the pillars of the government as well as private players need to work cohesively to ensure evolution of *Sashakt and Saksham Bharat*.

Skies Under Watch: Ethical and Legal Challenges of AI-Based Counter-Drone Systems in India and South Asia

Harmeet Singh and Anurag Jaiswal

Abstract

The rapid rise of drone technology has transformed the way we monitor people, transport goods, farm our lands, and even conduct warfare. However, the widespread use of drones also brings serious issues related to safety and personal privacy. In response to these emerging challenges, governments and private entities have begun deploying counter-drone systems, increasingly powered by artificial intelligence. While these AI-driven solutions offer faster and more autonomous threat detection and response, they also bring to the forefront complex ethical and legal dilemmas. This paper looks at these issues in India and across South

Colonel **Harmeet Singh** is currently pursuing a Ph.D. in Artificial Intelligence and Drone Warfare, focusing on the integration of advanced technologies into defence strategies. In the research, his academic pursuit complements his operational expertise, particularly in addressing modern conflict dynamics. Views expressed are personal.

Professor (Dr.) **Anurag Jaiswal** is a distinguished professor with extensive expertise in the Department of Defence Studies. The author conducted analysis of legal and ethical dimensions, and synthesized regional and international perspectives to provide policy-relevant insights into AI-based counter-drone systems. Views expressed are personal.

Asia, stressing the need for policies, rules, and ethical standards that can match the speed of technological progress. It calls for using AI in a way that is open, fair, and is in line with human rights.

Introduction

Across the skylines of South Asia, drones have moved from being a new idea to something essential. Initially used mainly for military purposes, unmanned aerial vehicles (UAVs) are now used for disaster response, delivering medical supplies, monitoring crops, and surveillance. In India, relaxation of rules around drones has led to a fast-growing domestic industry, expected to reach a value of over $1.8 billion by 2026. But with this growth comes a risk—misuses of drones for spying, smuggling, and targeted attacks has created a need for strong defence measures.

In response, systems powered by artificial intelligence have appeared, allowing for the real-time spotting, identifying, and stopping of unwanted drones. These systems can work on their own or with some human help, using machine learning, computer vision, and data analysis. However, with more automation comes a mix of legal confusion and ethical issues.

Can we rely on machines to make decisions that could change lives? And if an AI system gets it wrong, who should be held accountable? What rights do people have when being watched becomes routine almost every day?

This paper looks at these questions within the political and social setting of India and South Asia, areas with large populations, political tensions, and new digital rules. It explores the potential of AI-based counter-drone systems while also looking at the moral and legal rules needed to use them properly.

AI and Counter-Drone Systems

The advantage of AI in drone defence is its ability to handle complex situations at a large scale. Conventional methods of detecting drones

depend heavily on human judgment and direct observation—approaches that aren't always reliable or practical at scale. AI changes this. Using special computer programs feeded with data about drone behaviour, AI systems etc., can spot unusual activity, recognise threats, and decide on ways to deal with them in a fraction of second.

Counter-drone systems usually have four parts: detecting drones with tools like radar, radio waves, and sound sensors; identifying types of drones using AI; tracking them continuously; and stopping them through jamming, tricking them, or using force. AI significantly enhances identification and decision-making processes that once required the expertise of trained professionals.

In India, both the Ministry of Defence and the Ministry of Civil Aviation have started their own projects against drones, with agencies and companies like the Defence Research and Development Organisation (DRDO) and Bharat Electronics leading the way. Private companies across South Asia are also incorporating AI into their security systems, reflecting a growing regional trend towards intelligent threat management.[1] However, these systems are becoming more advanced than the legal and ethical rules available, creating a gap that this paper aims to fill.

Legal Challenges

Legal rules about airspace and new technologies are still developing in much of South Asia. In India, the Directorate General of Civil Aviation (DGCA) manages drone usage, but actions like jamming signals or using force against drones are often unclear in the law. A major challenge lies in determining as to who has the authority to take action. Since airspace is typically regulated by central governments, local authorities and private actors are often left uncertain about how to deal with unauthorised drones. In 2021, the Indian government introduced Drone Rules that categorises drones based on their weight and intended use—but these

rules fall short of providing clear guidance on how such drones can be intercepted or neutralised.[2]

Using force also brings serious concerns. According to Indian law and International Human Rights standards, any use of force must be necessary and not excessive. If an AI system incorrectly identifies a drone and causes an attack that harms people or property, it is hard to determine who is responsible—should it be the organisation using the system, the software company, or the person running the AI?

Privacy laws are also developing in India. The Digital Personal Data Protection Act was passed in 2023, however, it does not cover surveillance by counter-drone systems well.[3] These systems often collect extra data like photos or movements of people not involved. Without strong data policies, this could lead to serious violations of rights.

Figure 1: Balancing Legal Clarity with Technological Advancement

Globally, the legal system is also unclear. The Chicago Convention and ICAO guidelines cover airspace but does not address counter-drone tech.[4] In areas like Jammu & Kashmir or the India-Pakistan border, using autonomous counter-drone systems must follow International Humanitarian Law, especially the principles of distinguishing between combatants and civilians, limiting damage, and being cautious.

Ethical Challenges

The ethical challenges around AI-based counter-drone systems in South Asia are closely linked to the region's context of power, surveillance, and who is in charge. By design, these systems transfer greater control over surveillance and decision-making to opaque algorithms. This shift raises serious ethical concerns, particularly around transparency, accountability, and human oversight.

First, the issue of autonomy demands serious reflection. When a system is capable of independently deciding to stop a drone, it is, in effect, exercising authority. The ethical concern here goes beyond the system's reliability—it is about whether such critical decisions should ever be made without human involvement. In a region with trust issues in government, AI systems could make social and political problems worse.

Secondly, bias in AI algorithms is a big risk. AI models are trained on data that might reflect existing social inequalities. For instance, if surveillance data carries biases, AI systems may disproportionately flag certain communities or areas, reinforcing unfair targeting. Transparency is another major concern. Many AI models—especially those based on deep learning—operate as 'black boxes', with decision-making processes so complex that even their creators struggle to fully explain them. This lack of clarity becomes especially problematic in security contexts, where public accountability and legal oversight are essential.

More significantly, the growing use of AI in drone detection risks creating a culture of constant surveillance—one where individuals may

feel perpetually watched, raising concerns about privacy, civil liberties, and societal trust. In parts of South Asia where freedom of speech and assembly are already limited, such technologies could be misused to suppress dissent or monitor political events under the guise of drone control. Lastly, the dual use of AI technologies raises long-term ethical concerns. Tools built to defend against drones could be used for domestic monitoring, crowd control, or even political control. Without clear rules and supervision, the same systems that protect can also be used to control.

Figure 2: Ethical and Legal Challenges of Counter Drone Technology in India

Characteristic	India	International
Regulatory Framework	DGCA regulates UAVs, counter-drone interventions in gray zones	Chicago Convention and ICAO guidelines lack specific rules
Jurisdictional Issues	Central government controls airspace, unclear local authority	No clear rules on counter-drone technologies
Use of Force	Must meet necessity and proportionality tests	Must comply with International Humanitarian Law (IHL)
Privacy Laws	Digital Personal Data Protection Act offers limited protection	No specific mention in provided text
Liability	Complex; may rest with agency, developer, or operator	No specific mention in provided text

Regulatory Response

The rules covering AI-powered counter-drone systems in South Asia are not yet up to date with fast-moving technology. In India, the Drone Rules (2021) and the Digital Personal Data Protection Act (2023) are the main laws. However, existing laws offer little clarity on how autonomous AI systems should operate, how surveillance data is processed, or who should be held accountable for decisions made by machines without human input.

India's security and military agencies have created temporary rules for handling drones during high-risk events like Independence Day or large sports events. However, these rules are not official or part of the law. A lack of coordination between agencies further adds to the problem, resulting in inconsistent rules and practices across different regions. In countries neighbouring India, regulatory frameworks remain sparse, offering limited guidance on the use and governance of AI-powered drone systems. They mostly have rules for drones but not for counter-drone technology. In Pakistan, the military handles most counter-drone efforts without much public oversight, which can lead to unsafe monitoring and use of force without being accountable.

At the regional level, there is no agreement among South Asian countries on rules for drones or countering them. Since drone threats often cross borders—particularly in unstable or border-sensitive regions—the absence of cross-border collaboration weakens response efforts and heightens the risk of misunderstandings or conflict.

Global guidelines from groups like the IEEE and ISO provide some direction. Frameworks like the IEEE's Ethically Aligned Design and ISO/IEC standards on AI transparency and safety could offer valuable guidance in addressing these challenges.[5,6] However, without local adaptation and robust enforcement mechanisms, these guidelines remain largely ineffective in practice.

Recommendations

Tackling the ethical and legal issues of AI-based counter-drone systems in South Asia demands more than technical solutions—it calls for a broader, integrated approach. A strong commitment to transparency, accountability, and oversight must guide every stage of designing and deploying AI-driven counter-drone systems. At the same time, governments must act swiftly to establish clear national regulations that govern their use, ensuring these technologies are aligned with legal standards and public trust.

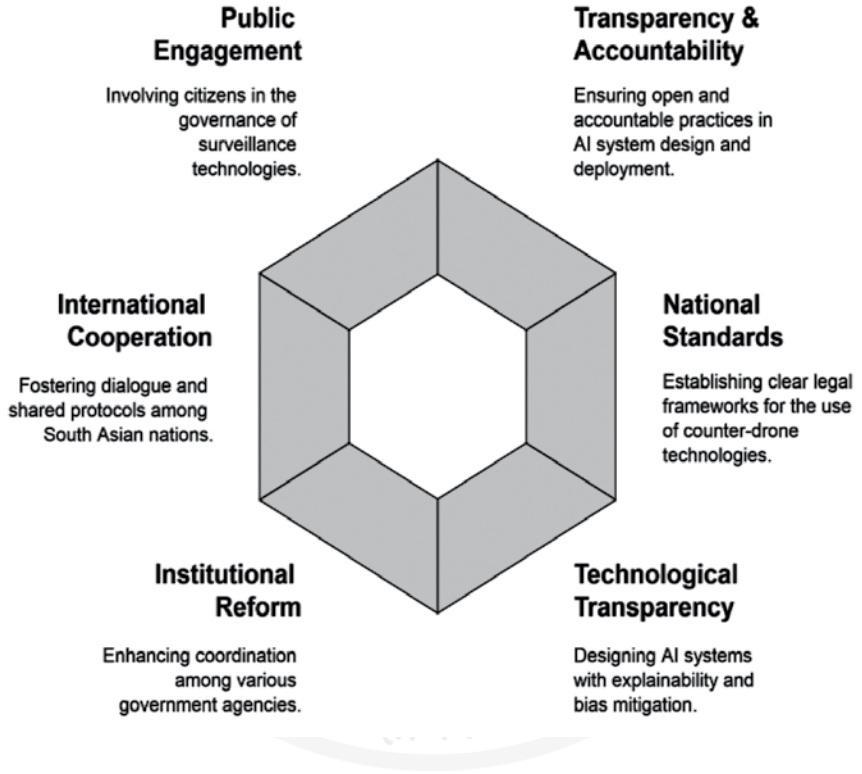
These rules should explain the legal reasons for taking action, require humans to approve any actions that involve force, and set strict limits on data collection and storage. Civil society must have the authority to scrutinize these systems and hold them accountable in cases of misuse or failure. On the technical front, AI systems should be designed with transparency and explainability at their core to ensure they can be understood and trusted. Developers should focus on making sure the AI is understandable and avoids prejudice. Publicly available reviews and tests should become the norm for AI systems that are used for security. The region also needs better organisational changes. Moreover, coordination between different agencies like defence, aviation, police, and data protection is essential.

In addition, creating a central body that oversees AI in security could help bring together standards and practices across different sectors. It is pertinent to note that working together internationally is also very important. South Asian countries need to speak across borders to create shared rules for identifying drones, assessing threats, and managing conflicts. With a history of mistrust and conflict in the region, working together on air space management could help build trust.

Lastly, involving the public is vital. The public has a right to understand how surveillance technologies operate in shared spaces, especially when these tools impact privacy and daily life. Systems for getting permission,

addressing complaints, and ensuring openness must be built with help from organisations that work with the public, so that technological progress does not harm democratic values.

Figure 3: Strengthening AI Governance in South Asia



Conclusion

As South Asia faces a growing number of both opportunities and risks in the sky, AI-based counter-drone systems are at a key point. They offer a strong defence against new aerial threats but can also be very dangerous if not properly controlled. Unclear laws, ethical issues, and weak rules threaten to damage public trust and human rights. This paper has explored both the promise and the pitfalls of these technologies,

calling for a balanced approach rooted in transparency, accountability, and regional collaboration. The future lies not in resisting innovation, but in managing it prudently—ensuring that security does not take away freedom, and that the benefits of AI are harmonised by our strong ethical assurance to use it fairly.

References

1. Ministry of Defence, 'DRDO develops anti-drone technology' (Press Information Bureau, 14 August 2021) https://pib.gov.in/PressReleasePage.aspx?PRID=1745851. Accessed on 21 July 2025.
2. Government of India, 'Drone Rules 2021' (Ministry of Civil Aviation, 25 August 2021) https://egazette.nic.in/. Accessed on 21 July 2025.
3. Digital Personal Data Protection Act 2023 (India).
4. International Civil Aviation Organization, 'Convention on International Civil Aviation' (Chicago Convention, 1944).
5. Institute of Electrical and Electronics Engineers (IEEE), 'Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems', First Edition (2019).
6. ISO/IEC JTC 1/SC 42, 'Artificial Intelligence—Overview of trustworthiness in AI' (ISO/IEC TR 24028: 2020).

Journal Articles

1. Sparrow R. Killer Robots. *Journal of Applied Philosophy*. 2007; 24(1): 62–77.
2. Taddeo M, Floridi L. The Ethics of Information Warfare. *International Journal of Ethics*. 2018; 28(4): 423–438.
3. Marchant G. Addressing Liability in Autonomous Systems. *Harvard Journal of Law & Technology*. 2019; 33(1): 132–167.
4. Crootof R. A Comparative Study of the Governance of Autonomous Weapons. *Yale Journal of International Law*. 2020; 45(1): 1–42.

Books/Monographs

1. Scharre P. *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company; 2018.
2. Boulanin V, Verbruggen M. *Mapping the Development of Autonomy in Weapon Systems*. SIPRI; 2017.
3. Eubanks V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press; 2018.

Chapters from Edited Books

1. Lin P. Why Ethics Matters for Autonomous Cars. In: Maurer M, Gerdes J, Lenz B, Winner H, editors. *Autonomous Driving*. Springer; 2016, pp. 69–85.

Conference Papers/Reports/Government & Institutional Publications

1. Arkin RC. Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/ Reactive Robot Architecture. *Tech Report GIT-GVU-07-11*. Georgia Institute of Technology; 2007.
2. Government of India. *Drone Rules 2021*. Ministry of Civil Aviation.
3. Ministry of Defence, India. *Defence AI Strategy Document*. 2023.
4. International Committee of the Red Cross (ICRC). *Autonomous Weapons and International Humanitarian Law*. 2021.
5. United Nations. *Group of Governmental Experts on Lethal Autonomous Weapons Systems*. CCW; 2021.
6. European Parliament. *Resolution on Autonomous Weapon Systems*. 2021.
7. Government of India. *Digital Personal Data Protection Act*. 2023.
8. US Department of Defense. *AI in Defense Applications: 2022 Roadmap*. 2022.
9. DRDO. *Anti-Drone Systems*. Defence Research and Development Organisation; 2022.
10. Gunning D. Explainable Artificial Intelligence (XAI). DARPA; 2017.
11. ICRC. Ethical and Legal Challenges of Military AI. 2021.
12. Sethi M. India's Drone Diplomacy and Regional Security. ORF Issue Brief. 2022.

AI in Countering Cyber Terrorism: Rethinking India's National Security Strategy

Sujeet Pillai, Julfikar and Kunal Koregaonkar

Abstract

Artificial Intelligence (AI) is redefining the parameters of national security and cyber conflict in the contemporary era. In India, where the pace of digital transformation frequently exceeds the rate of security adaptation, the convergence of AI and cyber terrorism poses complex and unprecedented challenges. This article situates its analysis within this evolving nexus, examining how AI is reshaping India's cyber-threat environment and that of its neighbouring states by simultaneously enhancing offensive and defensive capabilities. It critically reviews notable incidents, governmental and institutional policy responses,

Lieutenant Colonel **Sujeet Pillai** is an alumnus of NDA, MCTE (Mhow) and BITS Pilani. The Officer has been commissioned into the Corps of Signals, and is currently posted in Jabalpur. His areas of interest include Artificial Intelligence, Cyber Security, Emerging Technologies and Strategic Studies. Views expressed are personal.

Dr. **Julfikar** is a Professor of Political Science in SKD university with over 30 years of experience in the field. His area of expertise is Indian Political Thought and International Relations. Views expressed are personal.

Dr. **Kunal Kishore Korgaonkar** is an Assistant Professor in the Computer Science & Information Systems Department at BITS Pilani, Goa Campus, where he also leads the "Confluences of Computing" Lab, focusing on the intersection of science, technology, and society and the role of computing in driving socio-technological impact. Views expressed are personal.

and the strategic lacunae that persists within India's cybersecurity framework. In doing so, the study advances an Indian perspective on the legal, institutional, and cooperative mechanism required to ensure resilience in an AI-driven security landscape. Drawing upon official publications, peer-reviewed research, and open-source threat intelligence, the article ultimately proposes an integrated AI-enabled cyber-defence strategy to fortify national and regional security architectures.

Background

In recent years, India has emerged as one of the world's fastest-digitising regions, propelled by initiatives such as *Digital India*, *Aadhaar*, and the Unified Payments Interface (UPI). While these programmes have significantly advanced economic inclusion and technological innovation, they have simultaneously widened the national attack surface, exposing critical systems to increasingly sophisticated cyber threats. Cyber terrorism in India has evolved beyond conventional website defacements and propaganda to encompass large-scale data manipulation, ransomware operations, and AI-driven disinformation campaigns. Artificial Intelligence (AI)—a field of computer science concerned with replicating human cognitive functions such as perception, decision-making, and problem-solving, has become central to this transformation. Its ability to process vast datasets, identify hidden correlations, and predict outcomes has enhanced both offensive and defensive cyber capabilities, amplifying risks in an already volatile digital environment.

The concept of cyber terrorism—defined as the use of digital technologies to cause fear, disruption, or damage for ideological or political purposes—now extends far beyond traditional acts of digital sabotage. Terrorist and extremist organisations increasingly exploit the internet to disseminate propaganda, recruit followers, and coordinate operations, often through encrypted communication channels. The United Nations has acknowledged this duality of AI, noting its capacity to drive progress

while also posing significant ethical and security concerns, including threats to privacy, freedom of expression, and non-discrimination. This dual-use nature is especially visible online, where extremist groups deploy AI tools to amplify misinformation and manipulate public discourse. Platforms such as Facebook have reported removing tens of millions of extremist posts linked to groups like ISIS and Al-Qaeda, underscoring the scale at which AI-augmented digital radicalisation is occurring globally.

Academic discourse on cyber terrorism in India has broadened from a purely technical understanding to a multi-domain perspective that integrates political, psychological, and strategic dimensions. Early studies, such as those by Bhatnagar (2018) and Joshi (2023), characterised cyber attacks as symbolic disruptions rather than strategic operations. More recent scholarship, including Nayak (2022) and CENJOWS (2024), highlights the shift towards hybrid warfare, wherein AI-powered propaganda, social-media algorithms, and encrypted platforms are employed to influence cognition and erode public trust. Policy analyses by the Data Security Council of India (2023) and Niti Aayog (2018) call for the convergence of AI governance and cybersecurity policy through capacity building, legal reform, and international cooperation. Collectively, this body of research marks a paradigm shift from reactive cybersecurity to proactive, intelligence-driven resilience—where technological innovation, legal safeguards, and strategic foresight together underpin national preparedness against AI-enabled cyber terrorism

The Evolving Threat Landscape

> *"Cyber terrorism is no longer purely a technical threat—it is an algorithmic, psychological, and strategic phenomenon requiring AI-enabled countermeasures".*

Cyber terrorism refers to the deliberate exploitation of digital technologies, networks, and information systems to instil fear, disrupt

essential services, or threaten national security for ideological, political, or religious motives. In India, it has become a critical component of both internal and external security challenges. The country has faced repeated attempts to compromise government databases, defence communications, and research networks—many traced to state-sponsored or extremist actors operating from hostile neighbouring states. Incidents such as the 2018 Cosmos Bank malware heist and the 2020 cyber intrusion targeting Mumbai's power grid exemplify the growing vulnerabilities within critical infrastructure. Terrorist organisations have also weaponised social media platforms to disseminate propaganda, recruit operatives, and conduct psychological warfare, while disinformation campaigns have incited social unrest and communal tension. Consequently, cyber terrorism presents a multidimensional threat to India's sovereignty, economic stability, and societal cohesion, necessitating an integrated national cyber-defence strategy.

Artificial Intelligence (AI) has intensified these challenges by transforming the nature and scale of cyber operations. AI now facilitates the automation of reconnaissance, generation of deepfakes, and creation of adaptive malware. Extremist and terrorist groups increasingly exploit AI for propaganda dissemination, recruitment, financial facilitation, and online community management. In the Indian context, hybrid threats that combine cyber-attacks with coordinated information operations have emerged as a particularly acute concern. AI-powered bots and deepfakes are being deployed to manipulate perceptions, erode trust in public institutions, and destabilise societies, particularly during politically sensitive periods. Moreover, the use of AI-enabled drones for kinetic attacks demonstrates the blurring boundaries between cyberspace and the physical realm, underscoring the convergence of technological and traditional security domains.

The evolution of cyber terrorism in India reflects the erosion of boundaries between cyber warfare, information operations, and

psychological influence. Groups such as China-linked RedEcho and Pakistan-aligned APT36 (Transparent Tribe) epitomise this convergence. RedEcho has been documented as penetrating India's power and port sectors through modular backdoors such as ShadowPad, likely to establish strategic access for contingency operations. APT36, meanwhile, has conducted persistent espionage against government, defence, academic, and diplomatic targets using multi-platform payloads including CapraRAT, ElizaRAT, and the Poseidon implant. Both illustrate the weaponisation of cyberspace for intelligence gathering and potential disruption of national infrastructure. Despite institutional advances through CERT-In, NCIIPC, and the Defence Cyber Agency, India's cyber-intelligence ecosystem continues to face constraints in real-time data fusion, predictive analytics, and inter-agency coordination. Addressing AI-enhanced cyber terrorism and espionage will therefore require a unified, intelligence-led framework that integrates machine learning, indigenous data resources, and international collaboration to achieve a resilient and anticipatory national cyber-defence posture.

Cyber Attack Statistics in India

In the last decade (2015-2025), India's cyber threat landscape witnessed a pronounced escalation marked by a surge in phishing attacks, cybercrime incidents, data breaches, and large-scale cybersecurity compromises. The rapid digitalisation of governance, finance, healthcare, and critical infrastructure has expanded the nation's attack surface, exposing systemic vulnerabilities to both state-sponsored and criminal actors. The technology sector remains a prime target, accounting for nearly one-third of all phishing incidents, with India registering over seventy-nine million phishing attempts in 2023—ranking third globally after the United States and the United Kingdom. Cybercrime cases rose by over thirty per cent during the same period, revealing both the growing sophistication of cyber adversaries and improved domestic reporting mechanisms. At the same

time, India ranked fifth globally for data breaches, with approximately 5.3 million compromised accounts, underscoring the challenges in enforcing encryption, access control, and data protection standards envisaged under the Digital Personal Data Protection Act (2023). National reports submitted to the Indian Computer Emergency Response Team (CERT-In) indicates a rise in cybersecurity incidents—from 1.03 million in 2022 to 2.27 million in 2024—an alarming reflection of the widening threat spectrum.

India continues to face a diverse array of cyber threats emanating from both foreign and domestic sources, encompassing espionage, financial fraud, critical-infrastructure disruption, and ideological radicalisation. Persistent intrusion attempts have targeted government, defence, and research networks, often attributed to China-linked groups such as DragonOK and RedEcho and Pakistan-based actors like APT36 (Transparent Tribe). These campaigns primarily seek strategic intelligence and operational disruption through techniques such as credential harvesting, modular backdoors, and malware implants. Incidents such as the Cosmos Bank malware heist (2018) and the Mumbai power-grid intrusion (2020) exemplify the disruptive potential of cyber warfare. Concurrently, extremist organisations have exploited social media to disseminate propaganda, recruit supporters, and coordinate operations, while disinformation and fake-news campaigns have become potent tools for psychological manipulation, communal polarisation, and electoral interference. Such hybrid tactics blur the distinction between cyber terrorism, espionage, and information warfare, thereby challenging traditional notions of state security and governance.

The intersection of Artificial Intelligence (AI) and cybersecurity has further transformed India's digital threat environment. AI now functions both—as an enabler of malicious operations and as a novel attack surface requiring defensive innovation. National advisories and open-source threat intelligence reveal the growing use of automation and machine

learning to conduct reconnaissance, craft persuasive phishing content, and bypass detection systems. High-impact intrusions, including the DTrack malware at Kudankulam and the AIIMS ransomware incident, exemplify the exploitation of weak network segmentation, supply-chain vulnerabilities, and human factors—amplified by AI-driven social engineering. Recognising this, CERT-In advisories between 2023 and 2025 have highlighted emergent risks such as prompt-injection, model data leakage, and synthetic deepfakes used for impersonation and fraud. While direct forensic attribution of AI-authored attacks remains limited, the cumulative evidence demonstrates that AI technologies are accelerating the scale, speed, and sophistication of cyber operations. Strengthening India's resilience will therefore require an AI-aware cybersecurity architecture incorporating predictive threat intelligence, model integrity assurance, and inter-agency coordination—supported by robust public awareness and international cooperation to safeguard national security, digital sovereignty, and societal trust. A summary of some major incidents is tabulated below.

Sr No	Incident	Year	Analysis	Remarks
1	Kudankulam Nuclear Plant (KKNPP) malware (Dtrack)	2019	Malware (Dtrack) found in administrative systems; linked by researchers to Lazarus variants; CERT-In detection reported September 2019	High-value infrastructure intrusion; not an explicit AI attack but illustrative of advanced targeted intrusion capabilities
2	Mumbai grid outage	12 October 2020	Large outage with preliminary malware findings reported by some sources, but official committee found cascade/ equipment failure	Forensic ambiguity; demonstrates high impact and investigative/ attribution challenges

3	RedEcho / PRC-linked intrusions against Indian power and ports (Campaign C0043)	2021–2022	MITRE documents a sequence of intrusions targeting Indian electric utilities and logistics firms (RedEcho, TAG38)	Advanced persistent activity and pre-positioning of access
4	All India Institute of Medical Sciences (AIIMS) ransomware incident	23 November 2022	Large healthcare ransomware event encrypting ~1.3 TB of data; services disrupted; documented in CERT-In/media/ parliamentary replies and analysed in CERT-In ransomware reporting	Ransomware is increasingly combined with automation and targeted social-engineering; some later reporting discusses AI-augmented phishing generative tools at the ecosystem level
5	Nationwide rise in ransomware and phishing	2022–2024	CERT-In's Ransomware Report and annual incident statistics show a marked increase (e.g. 51% rise in H1-2022 vs 2021; CERT-In reported >1m incidents in 2022)	These reports also emphasise evolving tactics (supply-chain, RDP compromise, targeted phishing)
6	CERT-In advisory on AI language-model risks (CIAD-2023-0015)	2023	CERT-In explicitly warned developers/ users of risks when interacting with AI LLMs (misuse, impersonation, data leakage, impersonation domains)	This is a clear, government-level acknowledgement of AI-related cyber risk vectors

7	CERT-In/ Government publications and advisories on AI-driven threats (including prompt-injection guidance, and 2024/25 ransomware trend updates)	2024–2025	CERT-In issued a 2025 advisory on prompt injection and model jailbreak techniques (CIAD-2025-0013), signalling official recognition that attackers are exploiting AI systems themselves as an attack surface.	CERT-In and allied reports (2024 Ransomware Report) noted the rising presence of automated/ adaptive attacks across sectors

Cyber Terrorism Landscape and Threat Actors Targeting India (2015–2025)

Explicit evidence of Artificial Intelligence (AI) deployment in publicly disclosed cyber intrusions within India remains limited. Most high-impact incidents, including ransomware attacks, supply-chain compromises, and targeted espionage campaigns, continue to be attributed to conventional adversarial tactics, techniques, and procedures such as phishing, remote access trojans (RATs), and backdoor exploitation rather than confirmed AI-driven toolkits. Nevertheless, both CERT-In and industry reports increasingly acknowledge that AI techniques are being used to scale and refine cyber operations. These include automated spear-phishing, generative deepfake impersonation, and model-jailbreaking or prompt-injection attacks that enable adversaries to bypass security protocols with greater precision and speed. Recognising this emerging threat, CERT-In has institutionalised concerns about AI systems as potential attack surfaces. Its advisories issued in 2023 and 2025 explicitly focus on the vulnerabilities of AI language models, including risks of model-poisoning, data leakage, and output manipulation. These publications reflect a notable policy evolution: a recognition by Indian authorities

that AI must be regarded not only as a defensive enabler but also as a domain requiring active protection, governance, and regulatory oversight.

Empirical evidence from CERT-In and MITRE ATT&CK further illustrates the evolving complexity of India's cyber threat landscape. CERT-In's Ransomware Report (2022) documented a fifty-one per cent rise in ransomware incidents in the first half of 2022 compared with the same period in 2021, particularly affecting the information technology, healthcare, and financial sectors. Complementary advisories, including CIAD-2023-0015 and CIAD-2025-0013, warned of AI-related risks, specifically misuse of language models, impersonation attacks, and prompt-injection exploits targeting the models themselves. Meanwhile, MITRE's 'Campaign C0043' detailed nation-scale intrusions between 2021 and 2022 against Indian energy and logistics infrastructure, attributed to RedEcho and TAG-38, which highlight the automation and scalability of adversarial campaigns. High-impact operational incidents—such as the 2019 Kudankulam DTrack intrusion and the 2022 AIIMS ransomware attack—underscore the tangible consequences of these developments for India's healthcare and energy sectors. Collectively, these findings affirm that while direct forensic proof of AI-authored attacks remains rare, the convergence of automation, machine learning, and advanced tooling is accelerating the weaponisation of cyberspace against India's critical assets. The cyber terrorism ecosystem operating against India has expanded significantly over the last decade, comprising both state-linked Advanced Persistent Threats (APTs) and ideologically driven hacktivist groups. Open-source intelligence, CERT-In reports, and global threat repositories such as the MITRE ATT&CK database provide robust attribution evidence for several persistent actors that have systematically targeted India's defence, diplomatic, and critical-infrastructure sectors. These operations typically combine espionage,

disinformation, and network sabotage, revealing a convergence between cyber-terrorism and information warfare.

Rank	Group Name	Type/ Affiliation	Motivation/ Region	Notable Tactics, Techniques and Procedures (TTPs)	Evidence Level/ Source
1	APT 36 (Transparent Tribe)	Nation-linked APT (Pakistan-aligned)	Political-strategic espionage vs India	Spear-phishing using weaponised documents; Crimson RAT; credential theft; targeting defence, diplomatic and education sectors; recent use of malicious LNK files for Windows and BOSS Linux	High—MITRE G0134; Sentinel One; CERT-In (2023)
2	Side Copy	Pakistan-linked APT/ subset of APT 36	Espionage and information operations	Phishing lures mimicking Indian govt entities; ReverseRAT and AllaKore RAT deployment; multi-stage C2 channels	High — MITRE G1008; KPMG CTIP Report (2023)

3	RedEcho/ TAG-38	PRC-linked APT	Strategic pre-positioning in India's power and port sectors	Modular backdoors (Shadow Pad); targeting operational technology (OT) networks for contingency access	High—Recorded Future Insikt Group (2023); MITRE C0043
4	Indian Cyber Force	Domestic hacktivist collective	Pro-India ideological hacktivism	Defacements and DDoS campaigns against foreign domains; symbolic retaliation after border incidents	Medium—Media reports; Wikipedia 2024
5	Cyber Volk	Hybrid Ransomware-as-a-Service (RaaS)/ Hacktivist group	Alleged India-based pro-Russia alignment	Combines political messaging with ransomware operations; targets public and corporate assets	Medium—Public technical analyses (2024)
6	Trojan 1337	Indian hacktivist group	Ideological hacktivism	Symbolic website defacements on national anniversaries and events	medium—Media and open-source tracking

7	No Name 057(16)	International hacktivist collective (Pro-Russian)	Ideological/ geopolitical DDoS campaigns	High-volume DDoS attacks on regional targets linked to pro-Western positions; some operations spilled over to Indian digital services	Medium — Radware Threat Advisory (2024)

Among the principal cyber adversaries targeting India, APT36 (Transparent Tribe) and SideCopy stand out as the most persistent and technically sophisticated, conducting long-term espionage operations with confirmed attribution across multiple independent studies. RedEcho's activities, though not overtly terrorist in nature, demonstrate the strategic convergence of state-sponsored cyber intrusion and potential cyber-terror outcomes through the pre-positioning of access within critical infrastructure networks. In contrast, hacktivist collectives such as the Indian Cyber Force and Trojan 1337 engage in low-intensity, symbolic operations—primarily website defacements and distributed denial-of-service attacks—intended to amplify propaganda visibility rather than achieve strategic disruption. The emergence of hybrid entities such as CyberVolk and NoName057(16) further blurs the boundaries between cybercrime, ideology, and state influence, complicating attribution and response. The proliferation of generative AI tools and automated reconnaissance systems has substantially expanded these actors' operational capabilities, enabling scalable disinformation, deepfake, and spear-phishing campaigns. Although direct forensic attribution of AI-authored malware or phishing in Indian incidents remains limited, the accelerating integration of AI into offensive tradecraft underscores the need for India's counter-terrorism and cybersecurity frameworks to evolve

towards AI-aware threat intelligence, automated anomaly detection, and enhanced inter-agency coordination capable of pre-empting both cognitive and infrastructural attacks.

The integration of Artificial Intelligence (AI) into national security frameworks present profound ethical, operational, and diplomatic challenges for India and the broader South Asian region. Attribution in cyberspace remains a persistent difficulty, complicating deterrence and accountability. Consequently, the development of a multi-layered strategy that combines intelligence sharing, resilience building, and international cooperation has become imperative. AI embodies a dual character—it functions both as a catalyst for the evolution of sophisticated cyber-terrorism and as an indispensable tool for defensive innovation. India, as the region's largest digital economy, faces disproportionate exposure to AI-driven threats that exploit vulnerabilities across its rapidly expanding digital infrastructure.

AI and generative-AI technologies have revolutionised the scale and precision of social-engineering attacks. Cyber adversaries now employ AI to design highly personalised phishing campaigns that imitate legitimate communications with remarkable authenticity. The emergence of deepfake technology has further intensified this threat, enabling criminals to fabricate audio and video impersonations of authority figures—such as corporate executives or government officials—to deceive victims into executing fraudulent transactions. By scraping publicly available data from social-media platforms and corporate networks, AI algorithms craft targeted, context-specific messages aimed at high-value individuals or institutions. In parallel, extremist organisations have begun deploying AI-powered chatbots that simulate human interaction to engage, mentor, and radicalise susceptible individuals online, thereby industrialising processes of recruitment and ideological indoctrination.

The automation enabled by AI has significantly accelerated the speed, scale, and complexity of malicious cyber operations, often outpacing

traditional defensive mechanisms. Automated malware and ransomware use AI to conduct reconnaissance, exploit vulnerabilities, and dynamically adapt to evade detection. India has witnessed an increase in such AI-assisted attacks, including high-profile incidents against the All India Institute of Medical Sciences (AIIMS) and the Mumbai power grid. AI also plays a pivotal role in sophisticated supply-chain intrusions, wherein attackers compromise third-party software providers to infiltrate multiple downstream targets simultaneously. Moreover, adversarial AI poses a subtler but equally dangerous threat by corrupting training data or manipulating machine-learning models to produce misleading outputs, thereby eroding the reliability of AI-based security systems. These developments underline the necessity for India to strengthen its AI governance and defensive architecture to counter rapidly evolving cyber threats.

Publicly available reporting over the past two years indicates that militant organisations worldwide—including several Pakistan-linked groups—have begun exploiting AI-enabled tools to automate propaganda, enhance recruitment, and generate synthetic media. Although, there is limited verifiable evidence that groups such as Lashkar-e-Taiba (LeT) or Hizbul-e-Mujahideen (HM) possess bespoke AI capabilities, the trajectory is clear: generative models are being leveraged to produce multilingual extremist content, fabricate persuasive deepfakes, and deploy chatbot-style interfaces that lower the technical barriers to radicalisation. Regional analyses highlight that entities such as Islamic State Khorasan Province (ISKP) and Pakistan-based propagandists have experimented with automated recruitment and content-optimisation techniques across platforms like Telegram, X, and WhatsApp. Law enforcement agencies and Social Media companies have responded with takedowns and content moderation measures; however, the accelerating convergence of AI and extremist communication strategies threatens to make influence operations faster, more adaptive, and increasingly difficult to trace.

Strategic Gaps in India's Cyber Defence

India's rapid digital transformation, expanding critical infrastructure, and deep integration of digital services across public and private sectors have significantly increased its exposure to cyber threats. Despite a series of policy initiatives and institutional mechanisms, several strategic lacunae continue to undermine national cyber resilience. Foremost among these is a severe deficit in human capital. The shortage of qualified cybersecurity professionals remains a structural vulnerability—as of mid-2023, nearly 40,000 positions in cybersecurity were vacant, with almost a third unfilled due to skill shortages. The World Economic Forum estimates an overall gap of approximately 800,000 professionals when measured against current demand. This deficit extends beyond numbers to a lack of expertise in cloud security, threat intelligence, penetration testing, incident response, and AI-driven defensive systems. Simultaneously, India's critical infrastructure—particularly operational technology (OT) systems in energy, water, transport, and utilities—remains highly exposed. Numerous installations continue to operate with weak authentication protocols and default credentials, ranking India among the most vulnerable nations for insecure OT/ICS devices. Such weaknesses heighten the risk of cascading failures that could disrupt essential services or inflict physical harm.

Equally concerning is the inadequacy of incident detection, forensic response, and overall readiness for sophisticated cyber intrusions. While frameworks such as CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC) provide essential oversight, national capacity for real-time threat detection and rapid remediation remains limited. Academic studies on India's cyber warfare readiness note persistent deficiencies in situational awareness and cross-sectoral coordination. Surveys further reveal that around forty per cent of corporate cybersecurity teams are understaffed, leading to delayed breach detection and prolonged recovery periods.

Fragmentation within governance and regulatory systems compounds these problems. Jurisdictional overlaps between agencies, inconsistent enforcement of sectoral norms, and ambiguous legal frameworks for emerging technologies—such as AI, cloud computing, and the Internet of Things—continue to hinder coherent national response. Weak cross-border cooperation on evidence sharing and attribution further constrains India's ability to deter or prosecute cyber adversaries operating from foreign jurisdictions.

A broader weakness lies in the relatively low level of cyber hygiene among citizens, small and medium enterprises (SMEs), and under-resourced public bodies. Many organisations lack even basic security measures such as timely patching, robust password policies, and multi-factor authentication. This creates exploitable entry points for threat actors who use these entities as conduits for larger-scale attacks. Reports by CloudSEK and other security firms have documented instances of default credentials being retained in critical public systems, including municipal water supply networks and government email servers. Without sustained public-awareness programmes, capacity-building initiatives, and accessible support mechanisms for SMEs, these systemic weaknesses will continue to undermine broader national resilience.

Despite these vulnerabilities, India is making progress in integrating Artificial Intelligence (AI) into its cyber-defence and counter-terrorism strategies. AI is increasingly employed to automate threat analysis, detect anomalies, and identify phishing or disinformation campaigns. The Indian Computer Emergency Response Team (CERT-In) has issued multiple advisories addressing AI-related threats such as deepfakes and prompt-injection, while public-awareness initiatives—including Cyber Jagrookta Diwas and the National Cyber Security Awareness Month—aim to improve societal understanding of digital risks. Legislative and institutional measures, notably the Information Technology Act, the Bhartiya Nyaya Sanhita (BNS), and the Digital Personal Data

Protection Act (2023), have strengthened the legal framework for cyber governance. Internationally, India's engagement with the United Nations Counter-Terrorism Committee's initiatives on cybersecurity and new technologies underscores its commitment to multilateral cooperation. Within the South Asian and Indo-Pacific contexts, India has emerged as a pivotal actor in regional cyber stability—leading within BRICS, contributing to operations such as Sindoor, and demonstrating growing influence in global digital governance. Nonetheless, its predominance in regional malware and ransomware statistics highlights both its strategic importance and continued vulnerability in an increasingly AI-driven cyber domain.

Recommendations

Strengthening the Policy and Legal Architecture

India's cybersecurity architecture has evolved significantly over the past decade; however, the accelerating integration of Artificial Intelligence (AI) into both offensive and defensive cyber operations necessitates a fundamental recalibration of its policy and legal frameworks. Existing statutes, notably the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, provide the foundation for cyber governance but remain inadequate for addressing the emerging risks posed by AI-enabled systems. These frameworks continue to emphasise reactive incident management—focusing on phishing, malware, and data protection—rather than the anticipatory governance required to mitigate algorithmic manipulation, model poisoning, and cross-border attribution challenges. Revising the National Cyber Security Policy (2013) to explicitly incorporate AI-related risks is therefore essential. The inclusion of clear definitions of AI accountability, algorithmic transparency, and automated decision-making responsibilities would help bridge regulatory ambiguity and enhance institutional coherence.

Furthermore, specialised legislation on AI ethics, transparency, and safety—aligned with global benchmarks such as the EU's Artificial Intelligence Act—would create legal certainty for public and private entities deploying AI in cybersecurity contexts.

Establishing an AI-Enabled Cyber Defence Architecture

The rapid digital transformation of the Indian economy demands a comprehensive, AI-driven cyber-defence architecture capable of countering adaptive malware, deepfakes, and automated phishing. The allocation of ₹782 crore in the Union Budget 2025–2026 for cybersecurity projects reflects the Government's recognition of this priority. However, financial investment must be matched by a clear operational blueprint. Such an architecture should integrate AI-powered threat detection, predictive analytics, and automated incident-response protocols to ensure rapid containment and recovery. Machine-learning models can be trained to identify behavioural anomalies in network traffic, thereby supplementing traditional signature-based defences that remain insufficient against polymorphic threats. Public–private collaboration will be indispensable to this effort. Partnerships between the Defence Cyber Agency, CERT-In, the private technology sector, and academic institutions can foster indigenous research and development of AI-based security tools adapted to India's unique digital environment. The creation of an AI-Cyber Fusion Centre—modelled on global best practice—could centralise analysis, enhance early-warning systems, and promote cross-agency intelligence integration.

Reforming Legal Definitions and Regulatory Frameworks

Legal reform must accompany technological modernisation. The dynamic nature of AI and cyber operations has blurred the boundaries between criminal activity, espionage, and hybrid warfare, making clear legal demarcations critical. Revisions to the Information Technology

Act and related statutes should establish explicit provisions governing AI accountability in threat detection and automated response. Data-protection legislation must be strengthened to ensure that AI systems processing sensitive or personal information comply with privacy and security obligations equivalent to those under the General Data Protection Regulation (GDPR). Moreover, new norms are required for regulating cross-border data flows to balance national-security imperatives with global interoperability. The establishment of an AI and Cyber Law Commission—tasked with reviewing technological developments and recommending periodic legislative updates—could institutionalise responsiveness and ensure that India's legal ecosystem keeps pace with evolving threats.

Enhancing Capacity and Skill Development

Human capital remains one of India's most pressing cybersecurity constraints. Estimates by the World Economic Forum suggests a shortage of approximately 800,000 skilled cybersecurity professionals—a gap that severely impedes national preparedness. Bridging this deficit requires systemic investment in education and professional training. Curricula at secondary and tertiary levels should integrate modules on AI, machine learning, and cybersecurity ethics, thereby cultivating foundational literacy across disciplines. Specialised certification programmes—administered through institutions such as the National Institute of Electronics and Information Technology (NIELIT) and the Future Crime Research Foundation (FCRF)—can provide targeted upskilling in areas such as cloud security, threat intelligence, and incident response. Continuous professional-development frameworks, supported by government funding and industry partnerships, will help sustain a skilled workforce capable of operating advanced AI-enabled defence systems. Public awareness campaigns, including Cyber Jagrookta Diwas and the National Cyber Security Awareness Month, should be expanded

to encompass AI-related risks, ensuring that citizens, SMEs, and local administrations adopt safe digital practices that reduce the national attack surface.

Fostering Regional and International Cooperation

Given the transnational nature of cyber threats, unilateral action is insufficient. Regional cooperation must therefore form a central pillar of India's cybersecurity strategy. The establishment of a South Asian Cyber Resilience Initiative (SACRI) would provide a formal platform for harmonising cybersecurity standards, sharing threat intelligence, and conducting joint training exercises among member states. SACRI could function in coordination with the United Nations Counter-Terrorism Committee (CTC) and the United Nations Interregional Crime and Justice Research Institute (UNICRI) to enhance regional law-enforcement capacities and facilitate evidence exchange for cross-border cyber incidents. India's leadership within BRICS and its growing profile in global cyber diplomacy, positions it well to champion an inclusive framework promoting collective resilience. A parallel proposal—the creation of an AI–Cybersecurity Council for South Asia—could address the dual imperatives of security and ethical AI governance, encouraging transparency in algorithmic use and shared norms on responsible deployment. Such multilateral mechanisms would reinforce trust, enable interoperability, and reduce duplication of efforts across the region.

Promoting Ethical AI Use and Algorithmic Transparency

As AI becomes integral to cybersecurity operations, ensuring its ethical and transparent deployment is imperative. Bias, opacity, and lack of accountability in AI systems can erode public trust and produce unintended harm. Initiatives such as the India CASA dataset, developed by the Centre for Responsible AI at IIT Madras, represents critical steps towards identifying and mitigating bias in language models within the

Indian context. Building upon this foundation, the Government should establish national ethical guidelines for AI in cybersecurity, delineating principles of fairness, explainability, and human oversight. Algorithmic transparency must be institutionalised through mandatory audit mechanisms that allow independent evaluation of AI decision-making processes. Furthermore, bias-mitigation techniques—ranging from diverse training datasets to continual monitoring—should be embedded into the design phase of AI systems. Ethical governance frameworks will not only uphold constitutional values but also enhance India's credibility as a responsible digital power in global technology governance forums.

Leveraging Predictive Analytics for Counter-Terrorism

AI's analytical capacity can be harnessed to transition counter-terrorism from a reactive to a predictive paradigm. Predictive-analytics models, trained on large volumes of anonymised behavioural and communication data, can identify emerging trends and forecast potential threats without infringing on individual privacy. These systems should prioritise aggregated statistical patterns rather than the surveillance of specific persons to mitigate ethical concerns. When appropriately safeguarded, predictive analytics can provide law-enforcement and intelligence agencies with valuable situational awareness—allowing the prioritisation of resources, detection of anomalies in terrorist networks, and early warnings of radicalisation pathways. Machine-learning algorithms can process vast datasets encompassing financial transactions, travel records, and online discourse to reveal correlations indicative of preparatory activity. In the cyber domain, such models can detect abnormal network traffic or bot-driven propaganda bursts, enabling pre-emptive disruption of terrorist communication channels. Nevertheless, safeguards against algorithmic bias and overreach must remain integral, ensuring that predictive technologies complement, rather than replace, human judgement and due process.

Countering Radicalisation, Disinformation, and Extremist Narratives

The online ecosystem has become a critical battleground for ideological influence, necessitating innovative uses of AI to identify, counter, and neutralise extremist propaganda. Natural-language-processing (NLP) tools can detect linguistic markers of radicalisation within digital communities, flagging vulnerable individuals for intervention by social workers and law-enforcement authorities. Programmes similar to *Moonshot's Redirect Method*, which uses targeted advertising to direct individuals seeking extremist content towards de-radicalising materials, could be adapted for the Indian and South-Asian context. These approaches must be accompanied by ethical safeguards that protect privacy and freedom of expression while enabling timely prevention. AI can also enhance digital forensics—automated analysis of audio-visual material from surveillance cameras, drones, and online platforms can expedite the identification of suspects and the verification of extremist content. Moreover, combating mis- and disinformation, propagated by terrorist entities, requires AI-assisted detection of synthetic media and bot networks. By integrating machine-learning systems into information-verification workflows, government agencies and media organisations can curtail the viral spread of falsehoods that undermine social cohesion. Collectively, these measures will support a holistic, AI-enabled approach to counter-terrorism that combines technology, ethics, and inter-agency collaboration to safeguard India's national security in the digital age.

Conclusion

Artificial Intelligence (AI) has emerged as both—a shield and a sword in the contemporary cyber domain. For India, it represents not only a transformative tool for strengthening national cybersecurity but also a source of new vulnerabilities that adversaries can exploit. As the nation

continues its rapid digital expansion, the integration of AI into defensive systems has become imperative. AI-driven technologies enhance real-time threat detection, automate incident responses, and support predictive analysis to anticipate attacks from both state and non-state actors. Through advanced machine-learning models and behavioural analytics, India can identify malicious patterns, neutralise phishing campaigns, and prevent ransomware intrusions before they escalate. Furthermore, AI-assisted cyber forensics can accelerate the attribution of attacks, improving the country's ability to respond to hostile operations and enforce digital deterrence. By embedding AI into national security architectures—such as those managed by CERT-In, the National Technical Research Organisation (NTRO), and the Defence Cyber Agency—India can transform its cybersecurity posture from reactive containment to proactive defence.

In the broader geopolitical context, the effective application of AI in cybersecurity has far-reaching implications for regional and global stability. Across the world, AI technologies are being leveraged to counter terrorism, disrupt transnational criminal networks, and detect extremist propaganda disseminated through digital platforms. For India, whose strategic environment is shaped by persistent threats from both neighbouring states and transnational terrorist groups, AI offers an asymmetric advantage. It enables the monitoring of hostile cyber infrastructure, the identification of AI-generated disinformation, and the protection of critical national assets from sophisticated digital incursions. As India's global influence continues to grow, its capacity to deploy AI for defensive purposes will play a pivotal role in shaping the norms of responsible state behaviour in cyberspace. A comprehensive AI-enabled defence framework—anchored in ethical governance, international cooperation, and technological innovation—will not only safeguard India's digital sovereignty but also contribute to securing the global cyber commons against the evolving threats of the twenty-first century.

References

Bhatnagar, R. (2018). Cyber Terrorism and National Security, New Delhi: Pentagon Press.

Centre for Joint Warfare Studies (CENJOWS). (2024). Strengthening National Cybersecurity of India with the Use of Artificial Intelligence, New Delhi: CENJOWS.

Data Security Council of India (DSCI). (2023). India Cybersecurity Domestic Market Report 2023, New Delhi: DSCI.

FireEye Threat Intelligence. (2023). APT36: Persistent Threat in South Asia. Milpitas, CA: FireEye Inc.

Government of India, Press Information Bureau. (2025). Curbing Cyber Frauds in Digital India, New Delhi: PIB.

Joshi, A. (2023). Artificial intelligence and the new cyber threat paradigm. Journal of Defence Studies, 17(3), 45–67.

Nayak, V. (2022). Hybrid threats and cyber terrorism in South Asia. Indian Journal of Political Science, 83(2), 134–149.

NITI Aayog. (2018). National Strategy for Artificial Intelligence, New Delhi: Government of India.

OECD. (2023). AI and Cybersecurity: Policy Challenges. Paris: OECD Publishing.

Recorded Future Insikt Group. (2023). RedEcho: Targeting India's Power Infrastructure. Somerville, MA: Recorded Future. United Nations Office on Drugs and Crime (UNODC). (2022). Global Report on Cybercrime and Terrorism. CN Rath (2023) NXTGEN Publications 2023. Role of Artificial Intelligence in Defence Sector.

The Corps of Signals: Digital Combat Arm of the Indian Army

S.R.R. Aiyengar

Abstract

The Corps of Signals, established in 1911, has transformed from a telegraph-based communication arm into the Digital Combat Arm of the Indian Army. Its evolution mirrors the Army's transition from analog communication to a fully network-enabled, multi-domain force. Through successive technological eras—ranging from line communication and VHF/HF radio to fibre-optic grids, satellite networks, and secure digital architectures—the Corps has built the backbone of India's information-driven warfighting capability.

Today, the Corps leads the Indian Army's digital transformation through Tactical Communication Systems, the Defence Communication Network, Battlefield Surveillance Systems, and sovereign platforms such as ASCON, AWAN, A-SIGMA, and the Network for Spectrum (NFS). During Operation Sindoor, it demonstrated the operational maturity of unified C4ISR and the DG Signals–DGIS partnership,

Lieutenant General **S.R.R. Aiyengar**, PVSM, AVSM,VSM (Retd), was commissioned into the Corps of Signals of the Indian Army. He graduated from the National Defence Academy, Pune and later Indian Military Academy, Dehradun. The Officer has had the privilege of commanding the Armed Forces, and three premier Training Institutions namely MCTE, DSSC and NDC. Views expressed are personal.

validating India's concept of information superiority in a contested electromagnetic environment.

As warfare expands into cyber, space, and the electromagnetic spectrum, the Corps of Signals operates at the intersection of communication, cyber defence, and information warfare. It collaborates with tri-service cyber and space agencies, integrates electronic warfare functions, and ensures interoperability in preparation for Integrated Theatre Commands. With emerging capabilities in Artificial Intelligence, Quantum Communication, autonomous networks, and satellite resilience, the Corps is shaping the Army's future Joint All-Domain Operations architecture.

Standing as India's digital sword and shield, the Corps of Signals enables commanders to see, decide, and act faster than the adversary. It has become the central nervous system of the Indian military—empowering combat power across domains and defining India's path to dominance in the information age.

Introduction

The Indian Army's Corps of Signals, founded in 1911, has evolved from being a telegraph detachment to being the central nervous system of India's land warfare capability. In an era defined by information dominance, cyber resilience, and network-centric warfare, the Corps of Signals functions as the digital combat arm of the Indian Army. Its role has expanded beyond providing secure voice and data communication to enabling battlefield transparency, electromagnetic spectrum operations, and command information infrastructure that links the tactical, operational, and strategic echelons of warfare. The digitisation of the battlefield, through, Tactical, Operarational and Strategic Networks, Secure Mobile Networks, Air Defence Networks, Tactical Communication Systems (TCS), Battlefield Surveillance Systems (BSS), integration of Akashteer with Integrated Air Command and Control System (IACCCS), AFNET (Air Force Network)

and Indian Navy interlinkages, has elevated the Corps' significance to that of a combat multiplier.

As India transitions toward Integrated Theatre Commands and Digital Warfare Doctrine, the Corps of Signals embodies the Army's transformation into a network-centric force capable of operating in hybrid, multi-domain environments. The character of warfare in the 21st century has undergone a radical transformation. Modern conflicts are no longer restricted to land, sea, and air—they now extend into the cyber, space, information, and electromagnetic domains, where data and communication superiority often determine victory. In this evolving battlespace, the Corps of Signals has emerged as the digital combat arm of the Indian Army — a force that not only connects troops and commanders but also empowers operations through information dominance, cyber resilience, and electromagnetic control. The Corps today stands at the intersection of technology and tactics, embodying the essence of multi-domain warfare where communication itself is a weapon.

Evolution of the Corps of Signals: From Analog to Digital

Origins and Analog Foundations (1911–1970s)

The Corps of Signals, established in 1911, began as the communication arm of the British Indian Army. Its early decades were marked by wired telegraphy, field telephones, and line-laying detachments that ensured reliable voice and Morse communications during operations.

World War II saw expansion in wireless radio sets and rudimentary frequency management. Communication systems were manual, circuit-based, and analog, dependent on physical connectivity and human relay.

Training at the School of Signals (later MCTE, Mhow) focused on line communication, switchboard operations, and radio discipline. During this period, Signals was primarily seen as a combat support arm, ensuring battlefield connectivity among combat formations.

The Transition Phase: Advent of Electronics and VHF (1970s–1990s)

The 1970s ushered in Electronic Warfare (EW) and transistorised communication. The Corps adapted to new forms of HF/VHF radio, line multiplexing, and microwave communication.

Key milestones:

- ASCON (Army Static Switched Communication Network) initiated in the 1980s to provide a secure, backbone communication grid across the country. Became the foundational network for later digital systems—Army Wide Area Network (AWAN) and Army Secure Indigenous Messaging Application (A-SIGMA)
- Introduction of electronic exchanges, frequency-hopping radios, and satellite communication (SATCOM).
- Establishment of Signal Regiments at the Corps and Division levels, responsible for secure and continuous communication.
- Formation of Signals Intelligence elements to intercept and counter adversarial communication.

This phase also saw the shift from voice-centric to data-capable systems, though analog modulation still dominated.

The Digital Dawn: Networking the Battlefield (1990s–2010s)

With the advent of digital signal processing, microprocessors, and fibre optics, the Corps of Signals entered the network era:

- Digital switching systems replaced analog exchanges, enabling higher bandwidth and error-free transmission.
- **AWAN.** Launched in early 2000s, it was implemented in phases across Commands. Built over ASCON's static backbone, it integrates Network Management System (NMS), encryption and

multi-layer security. Designed for real-time data, video, and voice communication and supports applications, portals, and decision-support systems.

- Integration with civil telecom infrastructure, use of satellite links, and encryption technologies improved resilience, security and interoperability.

Signals began to emerge as a core enabler of Network-Centric Warfare (NCW)—linking sensors, shooters, and decision-makers in real time.

The Era of Convergence: Towards Information Dominance (2010s–Present)

The 2010s marked the onset of convergence of communications, cyber, and electronic warfare.

- Deployment of AFNET (Air Force Network), NAVNET, and Defence Communication Network (DCN) showcased tri-service digitisation. What's the relevance of AFNET and NAVNET? It's the advent of Army One and Army Data Network which is more relevant and the integration of the tri-services Network in some form.
- The Corps of Signals spearheaded integration with Defence Cyber Agency, Information Warfare, and Space Command initiatives.
- **A-SIGMA.** Launched in 2021. A home-grown application for secure messaging as a replacement of AWAN. It replaced all foreign-origin messaging applications for internal Army use. AWAN and ASCON, together creating a sovereign Digital ecosystem—it embodies the Army's information dominance and cyber resilience goals.
- Introduction of Software Defined Radios (SDRs), MANETs, and AI-enabled network management tools. SDRs and MANET are yet to be fielded in full.
- Training at MCTE, Mhow evolved to include cybersecurity, artificial intelligence, quantum communications, and cloud networking.

- Battlefield Surveillance System (BSS), **C**ommand Information and Decision Support System (CIDSS), and TCS (Tactical Communication System) projects represent India's move toward multi-domain operations (MDO) readiness. CIDSS and TCS are yet to come in fully.
- The Indian Army Sovereign Cloud to enable hosting of applications and ensure data centricity.
- Advent of SAMBHAV—mobile secure communications using public telecom infrastructure—a force multiplier.

From Enabler to Combat Arm: The Digital Combat Force (2020s–Future)

In the informationised and intelligentised battlefield, the Corps of Signals is no longer just a facilitator—it is a combat arm in its own right.

- It creates, secures, and dominates the electromagnetic spectrum (EMS), directly influencing battlefield outcomes.
- Future Signal operations will rely on AI-driven network orchestration, quantum encryption, and autonomous communication nodes.
- The integration of cyber-electronic warfare (CEW) capabilities would further signify the Corps' transformation into the Digital Combat Arm of the Indian Army.

Strategic Synthesis

The evolution of the Corps of Signals reflects India's broader journey from industrial to digital-age warfare. From laying copper lines in rugged terrain to establishing satellite-linked, AI-secured, multi-domain networks, the Corps has demonstrated unmatched adaptability and vision. In the coming decades, the Signals arm will form the backbone of India's digital sovereignty, ensuring that the nation's information space remains secure, resilient, and decisive in peace and war alike.

The initiatives briefly mentioned in the above paragraphs, collectively advance the Army towards:

- Information superiority in the battlespace.
- Atmanirbhar Bharat in defence ICT systems.
- Preparation for multi-domain and cognitive operations.

Digital Transformation and Network-Centric Warfare

The 21st century brought a doctrinal transformation within the Indian military—towards network-centric warfare, emphasising information dominance. The Corps of Signals became the architect of this digital transformation, spearheading projects that unified communications, sensors, and weapons into a seamless grid.

The Tactical Communication System (TCS) represents this transformation's centre piece. Developed indigenously with Bharat Electronics Limited (BEL) and the Defence Research and Development Organisation (DRDO), TCS replaces legacy radio networks with software-defined, IP-based, secure systems capable of supporting voice, video, and data across tactical formations. Its design ensures connectivity from Corps HQ to forward troops, providing battlefield transparency and near-real-time decision-making.

The Corps of Signals is the principal enabler and guardian of the Battlefield Surveillance System (BSS). Its doctrinal role extends far beyond providing communication—it ensures the survivability, security, and synchronization of every sensor and decision-support loop within the network-centric battlespace.

In Operation Sindoor, the Corps proved that modern signal units are no longer mere "line troops" but combat information warriors who defend the electromagnetic spectrum and cyberspace alike. Their operational excellence validated India's move towards Net-Centric, Multi-Domain, and Cyber Electro-Magnetic Activities (CEMA)-enabled

operations, setting the doctrinal foundation for future Integrated Battle Management Systems (IBMS).

The project 'Network for Spectrum (NFS)' resulted in a state of art IP network pan India, which is now fully functional and formed the backbone for Op Sindoor.

Operation Sindoor was India's largest field deployment of a digitally integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) grid under the Directorate General of Information Systems. Its goal was to achieve information superiority through a joint, network-enabled force, enabling real-time situational awareness and accelerated decision-making across tactical, operational, and strategic levels.

Cyber, Space, and Electronic Warfare Integration

In the digital battlespace, communication and cyber operations are interdependent. The Corps of Signals collaborates closely with the Defence Cyber Agency and Defence Space Agency to secure the Army's information environment. Signal formations manage encrypted intranets, key public infrastructure systems, and cyber intrusion detection architectures that protect critical communication nodes.

Parallelly, the Corps works with the Defence Electronics Research Laboratory to field advanced electronic warfare systems. These capabilities allow commanders to detect, jam, and exploit enemy communications while ensuring the survivability of friendly networks. Integration of cyber and electronic warfare functions position the Corps of Signals at the centre of India's emerging information warfare framework.

The Corps of Signals as the Nerve Centre of Multi-Domain Warfare

One of the tenets of MDO is 'Convergence'. Convergence is defined as the rapid and continuous integration of capabilities in all domains,

the electromagnetic spectrum, and the information environment that optimises effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative. The tenet maintains that via 'cross-domain synergy, layered options, and mission command', the armed forces stymie the adversary in aspects that are only feasible in MDO and not in single-domain alternatives. The commanders are required to build mechanisms and processes that assist in the management with an 'increased span of control' of a 'diverse collection of capabilities' while knitting them together for a better harmonisation matrix.

With the fusion of kinetic and non-kinetic warfare, the Corps of Signals has evolved from a support arm into a strategic combat enabler. As Artificial Intelligence (AI), Electronic Warfare (EW), Quantum Communication, and Space-based systems redefine the battlefield, the mastery of the electromagnetic spectrum has become as vital as control of territory. The Corps ensures that India's commanders can operate seamlessly in this contested domain—transmitting, securing, and exploiting data faster than the adversary.

As stated in the Joint Doctrine of the Indian Armed Forces (2017), "*Information is a force multiplier, and control over the information domain will be critical to future conflicts*".

This doctrinal vision encapsulates the Corps' evolving mission: to transform communication superiority into combat power, making it the nervous system of the Indian military.

Cyber Defence: Expanding into the Digital Battlespace

In the digital age, cyberspace is both a weapon and a battlefield, and the Corps of Signals is at the forefront of India's cyber defence architecture. Working in tandem with the Defence Cyber Agency (DCyA) and National Cyber Coordination Centre (NCCC), the Corps operates Network

Operations and Security Centres (NOSCs) that monitor, defend, and secure tri-service communication networks.

It employs AI-powered intrusion detection systems, machine learning-based anomaly prediction, and automated threat response tools to safeguard military data from espionage, sabotage, and misinformation. The Corps also supports offensive cyber operations, integrating electronic deception and digital countermeasures to neutralise enemy networks.

> "*Future conflicts will be multi-domain and non-contact in nature, demanding dominance across cyber, space, and information domains*".

Reflecting the above extract from the Indian Army Doctrine (2018), the Corps exemplifies this philosophy by treating cyberspace not as a support function, but as a combat front where it actively fights for information superiority and digital deterrence.

Dominance in the Air Littoral and Electromagnetic Battlespace

The rise of the air littoral battlespace—the dynamic zone between land and air dominated by UAVs, sensors, and precision munitions—has further expanded the Corps' combat role. In this environment, communication, electronic warfare, and kinetic operations are inseparable. The Corps of Signals ensures sensor fusion, electronic protection, and data-driven targeting, linking drones, artillery, radars, and command posts through real-time digital grids.

By synchronising intelligence, surveillance, and firepower, the Corps enables India to "see first, decide faster, and strike effectively". It is no longer merely ensuring connectivity—it is enabling multi-domain operational dominance.

Role in Integrated Theatre Commands

The rationale for Integrated Theatre Commands stems from the evolving nature of warfare, which increasingly demands 'jointness, interoperability, and multi-domain integration' to respond swiftly and decisively to complex threats. The model seeks to overcome the siloed functioning of the three services, wherein each operates under separate command structures. Multiple elements of combat, combat support and combat service support, directed at a common objective, are placed under a single commander who ensures that the objective is understood through his intent and mission orders. In this evolving notion of unity of command, unity of effort is achieved by an overarching "intent and purpose". At theatre level, to control all combat, combat support and combat service support forces, single commander—a C-in-C or joint Force Commander (JFC)—is needed in order to ensure unity of effort.

The creation of Integrated Theatre Commands marks a historic shift from service-specific operational doctrines to joint, multi-domain warfighting. It embodies India's commitment to transforming its armed forces into a technologically advanced, agile, and unified fighting force—fully capable of addressing the challenges of the 21st century's hybrid and information-centric warfare.

As India moves toward establishing Integrated Theatre Commands, the Corps of Signals assumes a pivotal role in linking tri-service communication systems into a single Defence Communication Network (DCN). The DCN provides encrypted, high-capacity links across land, air, and maritime forces, enabling joint situational awareness and synchronised command.

The Corps' experience in managing multi-domain networks uniquely positions it to integrate theatre-level communication, ensuring interoperability and data fusion across domains. In essence, it will form the digital skeleton of India's future joint force structure.

Global Comparison: US Cybercom, PLA SSF, and India's Corps of Signals

While traditionally considered a support service, the "signals" component in modern militaries is increasingly viewed as the backbone of information warfare. A comparative examination of China's Restructured Strategic Support Force (SSF) and the United States' Cyber Command (USCYBERCOM) provides valuable insights into how different powers have reorganised their signals and information warfare elements into higher operational and strategic roles.

The US Cyber Command (USCYBERCOM), established in 2010, focuses on offensive and defensive cyber operations, guided by the principle of "Defend Forward". It integrates with the National Security Agency (NSA) to conduct pre-emptive cyber operations globally. The Signal's function is embedded within broader cyber operations, with the NSA providing signals intelligence and network security. Communications and signals expertise are not confined to a support role but serves as the foundation for offensive cyber actions and network defence.

Meanwhile, China's Restructured Strategic Support Force (SSF), in April 2024, signals a shift: future wars seen as battles for information dominance as much as for territory. China is elevating information, cyber, and space operations as co-equal pillars of military power—an indicator of how Beijing envisions the next war. Reorganised into three entities—**Aerospace Force (ASF), Cyberspace Force (CSF) and Information Support Force (ISF**), it indicates improved warfighting effectiveness in space, cyber and informationised warfare.

India's Corps of Signals, though older, is following a similar path of integration through collaboration with the Defence Cyber Agency (DCyA), Defence Space Agency (DSA), and Defence Intelligence Agency (DIA). With indigenous projects like TCS, DCN, and Quantum Communication, it is building a foundation for a future Information

Warfare Command that mirrors the strategic depth of the US and Chinese models—but rooted in India's own doctrine of "Information and Spectrum Superiority".

Future Vision: AI, Quantum, and Beyond

The future of the Corps of Signals lies in harnessing Artificial Intelligence (AI), Quantum Communication, and 5G-enabled tactical networks to create an adaptive, autonomous digital battlespace. DRDO-led projects like Project Sanchar Netra and the Defence AI Council (DAIC) are developing AI-driven decision support systems, predictive cyber defence, and autonomous spectrum management. AI will allow real-time network optimisation and cyber attack prediction, while machine learning algorithms will help allocate bandwidth dynamically and detect anomalies instantly.

India's progress in Quantum Key Distribution (QKD), demonstrated jointly by DRDO and IIT Delhi, marks a leap towards unbreakable encryption and quantum-resilient communication systems. The Corps aims to integrate these technologies with Low Earth Orbit (LEO) satellites and edge computing nodes, ensuring secure connectivity even in denied or disrupted environments.

The path forward involves:

- **AI and Automation**: Leveraging machine learning for network resilience, cyber threat detection, and automated signal planning.
- **Quantum Communication**: Exploring quantum key distribution for unhackable encryption.
- **Satellite Resilience**: Deploying indigenous small-satellite constellations for assured communication during high-intensity conflicts.
- **Human Capital Development**: Continuous upskilling of personnel through cyber and AI training modules at MCTE and tri-service academies.

The Corps of Signals thus stands ready to lead India's transformation into an AI-empowered, quantum-secure digital defence force.

Synchronisation between DG Signals and DG Information Systems (DGIS) during Operation Sindoor

During Operation Sindoor, the synchronisation between DG Signals and DG Information Systems reached its most mature operational form to date. Together, they achieved continuous communication, secure data flow, and rapid information fusion in a contested cyber-electromagnetic environment—transforming the operational art of command into a genuinely network-enabled warfare model. Synchronisation has proven that command agility in high-tech warfare depends less on weapon platforms and more on information infrastructure unity. The operation reaffirmed India's emerging concept of Information Superiority achieved through a unified C4ISR framework. It demonstrated that the DG Signals–DGIS partnership functions as the central pillar enabling effective Multi-Domain Operations.

As the Army prepares for increasingly complex joint operations, it is imperative to recognise the interdependent nature of modern warfare. Modern warfare is inherently joint and interdependent, with victory hinging on the seamless integration of combat, combat support, and logistics functions. No single arm, however potent, can secure success in isolation. The Corps of Signals, while rightly described as the 'Digital Combat Arm' of the Indian Army, derives its strength from its capacity to enable, accelerate, and synchronise the fighting potential of all arms and services. Its networks, systems, and digital architectures create the vital information fabric that empowers commanders to see, decide, and act faster than the adversary. In this sense, the Corps does not merely support operations—it transforms the very tempo and coherence of combat power across domains, ensuring that the Army fights as one integrated digital force.

Conclusion

The Corps of Signals has evolved from managing message lines to commanding the information grid of the Indian Army. Its legacy systems laid the foundation for a secure, indigenous communication architecture. Its modern programs, including TCS and DCN, embody India's vision of network-centric warfare.

As warfare becomes increasingly defined by data and decision speed, the Corps stands at the intersection of communication, cyber operations, and command intelligence.

As articulated in the Joint Doctrine of the Indian Armed Forces (2017):

> "*The battle of the future will be fought as much in the electromagnetic spectrum and cyberspace as on land, sea, and air*".

In this context, the Corps of Signals is no longer a mere communication provider—it is the digital command arm of India's warfighting machine, the brain and nervous system connecting every sensor, shooter, and decision-maker. Through innovations in AI, Quantum Communication, Cyber Defence, and Spectrum Control, it ensures that India's Armed Forces remain connected, informed, and dominant in every domain of battle. Just as USCYBERCOM and China's SSF embody their nations' pursuit of digital supremacy, the Corps of Signals stands as India's digital sword and shield, safeguarding the nation's sovereignty across the expanding frontiers of information warfare. It is, indeed, the Digital Combat Arm of the Indian Army—the force that will define victory in the wars of the information age.

The Corps of Signals has transformed from being a communication support arm to becoming the digital command spine of the Indian Armed Forces. Its indigenous initiatives—from NFS and TCS to Quantum and AI programs—are converging to enable a Joint All-Domain Operations

architecture, ensuring that India remains competitive in the emerging AI-driven, information-centric battlefield. In fulfilling its motto, Teevra Chaukas—Swift and Secure—the Corps of Signals continues to ensure that the Indian Army remains connected, informed, and dominant in the digital battlespace.

References

Bharat Electronics Limited (BEL). Tactical Communication System Overview. Bengaluru, 2022.

CENJOWS. Network-Centric Warfare and the Indian Armed Forces. New Delhi, 2021.

Defence Research and Development Organisation (DRDO). Annual Report: Communication and Cyber Systems. New Delhi, 2023.

Indian Army. Land Warfare Doctrine. Army Headquarters, New Delhi, 2018.

India's Joint Doctrine for Multi-Domain Operations (MDO) released by Raksha Mantri, Shri Rajnath Singh on 27 August 2025.

India's Joint Doctrine for Cyberspace Operations. 2024.

Institute for Defence Studies and Analyses (IDSA). Information Warfare and India's Strategic Posture. New Delhi, 2023.

Integrated Defence Staff. Joint Doctrine of the Indian Armed Forces. Ministry of Defence, New Delhi, 2017 and 2023.

MCTE, Mhow. Signals Corps Journal – Digital Army Special Issue. 2022.

Ministry of Defence. Annual Report 2023–24. Government of India, New Delhi, 2024.

Press Information Bureau. Digital Transformation of the Indian Armed Forces. MoD Release, 2024.

Concept of Non-Contact Warfare

R C Srikanth and Prashant Agarwal

Abstract

The concept of Non-Contact Warfare has assumed immense salience in the past few decades. Identified as a crucial outcome of the first Gulf War and documented by Russian General Vladimir Slipchenko, the hypothesis of non-contact warfare predicts weaponising each and every aspect of national comprehensive national power and utilizing it in an unobtrusive, unstructured yet thoughtfully decisive manner to achieve decisive results against adversaries—state or non-state without or with minimal use of force. The article explores the aforesaid notion in its theoretical construct and what it would take to orchestrate a campaign in non-contact domain. It scans various approaches underlining the construct and examines their impact on conduct of operations.

Concept of Non-Contact Warfare

The conventional/contact method of prosecution of war per se has been associated with the destruction of adversarial military capabilities

Lieutenant General **RC Srikanth**, AVSM, VSM is an alumnus of Officers Training Academy (OTA), Chennai. The Officer is a graduate of Long Gunnery Staff Course, Defence Services Staff College, Higher Command Course and the National Defence College. Currently, he is heading the Army Air Defence College as its Commandant, and is pursuing his PhD. Views expressed are personal.

Dr **Prashant Agarwal**, is Professor at the Department of Defence and Strategic Studies, University of Allahabad. Views expressed are personal.

with an undesirable impact on the economies of countries as well as the region. The achievement of grand political objective (territorial, moral, psychological etc.) while sustaining the least degradation was the *raison-d-etre* of joining a war. Though the prosecution of conventional war may attract luster from the traditionalists but the question that needs to be addressed is—Are there any better ways of achieving the same by controlling the collateral damage as well as providing better management of the end state in the 21st Century? Is a war without contact feasible, possible and more importantly winnable? For Vladimir Slipchenko, the harbinger of non-contact war was the limited use of cruise missiles in the Falkland War and he surmised its essence as "the necessity in Russia for completely different armed forces. If today our armed forces function in three distinct mediums, air, sea and land, what we need is two functional branches: strategic attack and strategic defense forces. No tank armies will roll across the Russian border. The future war will involve non-contact precision strikes against the state and military control systems, communications, and economy. Preparing for such a conflict would demand a reorganization of Russian defense industries, research and development capabilities, and the recasting of Russia's Armed Forces to fight and win Non-Contact Wars."[1, 2]

The exponential growth of information in the 20th and 21st century and its permeation in every aspect of human life (civil and military) has altered the nature, method and modes of accessing information. Additionally, even larger quantum of information lies in the 'Dark Web' ready to be exploited against an organisation or a precise individual. This threat lurks in the minds of all and consequently has created serious challenges in social, political, economic and cultural spheres and established novel facets to existing paradigm of military threats. They have also unveiled lucrative vulnerabilities and opportunities which when targeted may achieve capitulation of nation/society without 'firing a shot'.

War in the 21st century is more likely to see nations focusing on exploiting a composite mix of national power within a theatre of operations, which may itself be redefined, to achieve victory without resort to arms. No component of a nation or society will be left out of the war with some being simultaneously targeted at the moral, conceptual, psychological as well as at the military plane. War by Non-Contact means may become the predominant strategy for prosecuting military operations. Nations who have the ability, will leverage their superior capabilities across domains in multi-domain application of force to create conditions to subjugate other nations without or with minimum physical battlefield contact.

Contact Warfare

Though there is no term as 'Contact Warfare' prevalent in military glossary technically, but it needs to be elaborated to add clarity to the concept of 'Non-Contact Warfare'. In military-tactical terms, 'Contact' is understood to convey physical proximity to an objective, enemy or location, it being further qualified as 'Contact by visual means, by radio or by fire'. 'Contact' could also be relative viz. close, proximate, distant or out of contact. In terms of warfare, the term Contact Warfare could be related to prosecuting war through conventional/traditional methodology where the focus is to close in with the enemy and destroy him by physical violent action and capture the objective. This is largely in the land domain. These objectives could include capturing territory, destroying enemy war waging potential, taking a large number of prisoners of war or getting into a superior posture at post conflict bargaining negotiations. The objectives being such, the war is fought in definable dimensions viz. land, sea and air with primacy of land-air or air-land concept of operations. Victory and defeat in such a war is defined in terms of how much has the adversary been forced to accede to Victor's diktats consequent to his defeat on the battlefield. The traditional wars of the past have been characterised

by their orderliness with armies millions strong, continuous positional frontlines and one belligerent's immense numerical superiority over the other playing the decisive role.[3] Prosecuting Contact Warfare could imply the following:

- **Definite declaration of War** by at least one of the belligerents and clear battle indicators of adversaries going to war.
- **Massive mobilisation, movement and posturing** of formally organised regularly equipped and trained armed forces.[4]
- **The defeat or physical destruction of rival military capability** remains crucial to accomplishing the planned end state which may entail bringing the rival armed forces to battle and then destroying them by attrition or manoeuvre.
- **Duration of operations** may be constrained by multifarious factors such as international pressures, economy etc.
- The war generally conforms to the **Laws of Armed Conflict** and other international conventions.
- The **zone of combat** generally remains confined to designated military theatre of operations rarely escalating beyond into civilian/ populated areas with **clear delineation of the combat and non-combat zones.**
- **Victory** is defined in terms of tangible destruction/degradation of enemy war waging potential, territorial gains, prisoners captured etc.
- The **realisation of total, complete and comprehensive political objective** is critical for the successful culmination of war in purely contact perspective.

Non-Contact Warfare

The Gulf War of 1991, Global War of Terror (GWOT) post '9/11', recent Crimean conquest by Russia in 2014, the ongoing Russia— Ukraine War (2022), The Israel—Hamas conflict (2024) and most recent Israel—Iran

conflagration (2025) witnessed considerable variance to aforementioned contours of conventional conflict, wherein huge application of non-contact capabilities were potently applied to generate effects that resulted in achievement of the political objective without major commitment of ground troops in combat operations. The 1991 Gulf war was fought between the Allied Forces led by USA and Iraqi Army amidst a wide technological asymmetry, the GWOT is being prosecuted against an amorphous enemy (Al-Qaeda, Taliban etc.) which avoided attritional contact with conventional armed forces while Russia exploited its superior multi-dimensional capability to wrest Crimea through engineered political dissent supported by discreet military capacities. The ongoing conflicts in Europe and West Asia as highlighted above continue to observe application of multi-dimensional capabilities synergized with net centricity and whole of nation approach.

In the Gulf War, the Allied Forces equipped with state-of-art weapon systems, technologies and armed with an international mandate took on the Iraqi army that was still steeped in 'outdated inflexible positional standoff strategy'[5]. The Iraqi tactics of holding ground proved no match to the new technologies and methods of warfare employed by the United States and its allies leading to Iraqi capitulation. The 'Gulf War' was a practical demonstration of the truth that technological superiority in weapons could cancel the enemy's numerical advantage[6] and can cause strategic defeat at minimal or no cost. It probably was the first occasion that an army of half a million strong was turned over without being able to fight due to application of Non-Contact capabilities across spectrum. The key peculiarity of the Gulf War, that noticeably emerged, was the disproportionate 'Non-Contact Component' of war (Kinetic and Non-Kinetic) that involved strikes by Tomahawk Cruise Missile, use of Beyond Visual Range Missiles, Electronic Jamming of Iraqi Command and Control Stations, targeting of critical civil and military infrastructure, intense Information Operations, use of unmanned and

space based assets to gain information superiority over the Iraqi Armed Forces, thus creating overarching conditions for demoralisation of Iraqi Armed Forces and civilian population as well as its early capitulation[7]. The exploitation of hitherto for unchartered territories altered the scope and manner of conventional warfare as unseen weapons could bring to bear extensive destruction on not only military targets but non-military targets with precision to create 'paralysis' in the chain of political leadership and military command as well as demoralise armed forces and general populace. The Gulf war demonstrated very eloquently that it may be feasible to make enemy reach culmination point without physically getting into contact with him by exploiting competitive advantages within and outside the battlefield by concurrent Multi-Domain application of force.

The prosecution of the GWOT on the Pan Islamic terror outfits led by 'Al-Qaeda' exposed a differing interpretation. The war against the terror outfit has been raging on without frontiers in trans-continental domain. It is characterised by the enemy (Al-Qaeda) morphing itself with each defeat and transiting postures where opportunity presents itself. It is difficult to define and still more difficult to defeat in the usual way we define 'Victory'. Though the proscribed organisation may be defeated in physical domain but in cognitive domain its influence has not yet petered out, thus the 'Will' aspect continues to germinate in forms and manners at differing locations and in different formats. Newer and better methodologies or combinations of methodologies need to be thought of to achieve victory in the asymmetric domain characterised by Al-Qaeda or other global/regional terror outfits. The franchising of ideologies of extremism, radicalism, religious intolerance, caricaturing of enemy and call for Muslims across to answer the call for Jihad are manifestations that have accessed the vitals of multiple nation states without puncturing significant military capabilities and emphasise salience of non-contact capacities in pursuing their motives.

Slipchenko's Theory of Non-Contact Warfare

The theory of 'Non-Contact Warfare' took roots based upon the study of 'Gulf War' of 1991 and the impact of new generation weapons on the conventional armed forces. As evidenced in Gulf War, the cumulative technological capability was now inventing the potential for select few nations of inflicting irretrievable damage on an enemy state without getting into physical contact. War could be fought concurrently in multiple domains—physical (signifying the contact battlefield), virtual (signified by space, cyber, informational), economic, trade, resource, ecology, perceptual, cognitive, moral and other domains. The 'shock' of operations, in the virtual sphere, in conjunct with physical, economic and moral domains etc. was assessed to be generating concurrent, cascading and debilitating impact on the outcomes in the contact sphere, thus facilitating speedy capitulation. The decisive relevance of physical domain in warfare was receding and virtual/perceptual domain was gaining prominence. Victory in the virtual/perceptual realm facilitated or fast-forwarded triumph in the physical arena with ever reducing need for equivalent physical contact. Consequently, the criticality of dominating virtual sphere of influence has gained currency and means of spawning decisive effects in virtual domain are being sought to attain decisive victories in future conflicts. Victory in virtual sphere is now equally if not more critical to sustain and modulate national 'Will'.

The term 'No Contact Warfare' was first used by late Major General Vladimir Slipchenko in the aftermath of Gulf War of 1991. The sixth generation warfare was explained as involving the capacity to conduct distant, no-contact operations. The informatisation of conventional warfare and the development of precise targeting capacities made prosecution of conventional war an "Invitation to Disaster". He further recommended that the nations must evolve capabilities and means to mass effects through depth of enemy to fight 'Systems versus Systems Warfare.[8] He drew extensively from Marshal Ogarkov's "Revolution

in Military Affairs" and saw "Desert Storm" as the first indication of appearance of such capabilities[9]. Slipchenko believed that sixth generation warfare would replace fifth generation warfare (thermonuclear warfare) prompting him to suggest "No-Contact Warfare" as the optimal form for sixth generation warfare. In terms of deliverables, the 'Slipchenko Hypothesis' underscored the following:

- **'Informatisation'** would be the key factor in any future war and the side that masters it the best will win the conflict.
- **'Informatisation' may define the new paradigm** beyond the Nuclear Deterrence (Information Deterrence)[10].
- It is feasible to **generate decisive effects** on an enemy by suitably modulating the comprehensive national power against an opponent beyond contact domain.
- There would be a need to undertake an overhaul of existing military doctrines and organisation to absorb the tenets of 'Sixth Generation Warfare' that do not rely only on Contact Warfare.

Gerasimov Doctrine.[11, 12] Valery Vasilyevich Gerasimov is credited with articulating the "Gerasimov doctrine" in an article published in *Voenno-promyshlennyi kur'er*, the Military-Industrial Courier on 27 April 2013. This doctrine relates to Russian Military thought on combining military, technological, information, diplomatic, economic, cultural and other tactics. The doctrine acceded to the thought process of Slipchenko and understood that distinct and defined conditions of Peace and War can no longer be defined. Further, wars in future may be no longer explicitly declared (Grey Zone), implying that state and non-state actors would be in constant state of 'war' below the traditional known sense of war and once joined it would be nearly impossible for participants to predict and control their direction. General Gerasimov further articulated that, a perfectly thriving state can be transformed into a theatre of war, made a target of external intervention and forced into disarray,

catastrophe and severe internal dissensions and civil war by executing non-contact operations. The extent of fatalities and destruction, the terrible societal and cultural impact, debilitating financial disruption and divisive political costs effected operations would be analogous to the implications and outcome of any Contact War. He contended that the very "rules of war" have distorted and the function of nonmilitary means in attaining political and grand strategic goals have matured, and, in many cases, they have gone beyond the supremacy of might of weapons in their efficacy. The emphasis of force application therefore, he contended, must be modulated to include use of political, economic, informational, humanitarian, and other non-military measures and applied in coordination with the protest potential of the population in the target country[13]—a precursor to current thought of 'Military-Civil Fusion' or 'Whole of Nation Approach'. The aforementioned capabilities, when required, could be augmented or supplemented by cloaked application of kinetic capabilities in appropriate mix. He also alluded to the intervention under the ruse employing troops/forces under the guise of peacekeeping and crisis regulation primarily for the achievement of terminal success in the conflict (Crimean Operations). The strategic heft seems to be shifting as under[14]:

- Morphing from direct destruction to direct influence.
- Inner decay of opponent preferable to its direct annihilation.
- Exploitation of culture as a new weapon of war.
- Use of specially organised forces for specific tasks.
- Information, psychological and war of perceptions.
- From a superficial and compartmented war to total war—including the enemy's internal side and base—everything is a legitimate target only the dimension of capability application against the target changes.
- From war in the physical environment to a war in the human consciousness and in cyberspace.

- From war in a defined period of time to a state of permanent war as the natural condition in national life.

Defining Non-Contact Warfare

The Non-Contact Warfare is differently interpreted—differing thoughts on defining the concept are:

- The king, Ministers, Territory, Fortifications, Treasury, Army and Allies constitute the seven components' elements or limbs of state. These elements are inter-related and interdependent, so much so that if any of them is out of order the whole system breaks down. Hence, careful attempts should be directed towards all round development of the elements collectively[15]. This also implied that these elements could be targeted to make the state capitulate internally.
- The concept of Total Dimensional Warfare was brought out by USA in 1993 and it was visualised that it should possess the special characteristics of "total depth, total height, total frontage, total time, total frequency, and multiple methods" bringing out a clear coherence amongst all elements of combat and non-combat military operations. Surprisingly, this thought was discarded by successor US think tanks as challenging the primacy of combat forces and hence was not pursued further[16]. Hybrid warfare evolved as a term subsequently to encapsulate certain essentials of Total Dimensional Warfare. In essence, hybrid warfare involved a state or state-like actor's use of all available diplomatic, informational, military and economic means to effect warfare against an adversary[17].
- Lt Gen (Retd) Davinder Kumar, PVSM,VSM** defined Non-Contact Warfare "as the type of warfare which involves application of all national capabilities in an integrated manner while ensuring minimum physical contact of own forces, to conduct distant operations to achieve a quick decisive victory by disrupting, denial and destroying the enemy's war waging potential and his command and control

systems through remote delivery of destructive kinetic energy and soft power by relentless information operation".[18] Though, the definition comprehensively covers operational aspects of Non-Contact Warfare something akin to what happened in Gulf War and may be relevant to a Joint Force environment within a theatre of operation, it does not lend itself adequately to grand strategic or geo-strategic elucidation. The emphasis on destruction of enemy War Waging potential tends to circumscribe the ambit of application of the national capabilities, whereas the scope as highlighted by Gerasimov Doctrine, is all encompassing with war waging potential just an element in the larger target matrix of adversary. Further, the application of national power through remote delivery of kinetic energy and soft power through information operations does reverberate certain critical doctrinal precepts of the extent of Non-Contact Warfare, but is short of assimilating its full extent. Non-Contact Warfare as a doctrine of operations and warfare is relevant throughout the entire continuum of conflict spectrum (Total Peace to Total War) and beyond and hence transcends the boundaries of Peace, Proxy War, Crisis, Limited War and Total War.

- Brigadier Vivek Verma in his book *Non-Contact Warfare—An Appraisal of China's Military Capabilities* defined the concept as the form of warfare in which states seeks to employ all elements of national and non-state groups attempt to leverage their influence across multiple domains to target adversary's population, sovereignty, governance, structures and economy through non-military or military non-kinetic and kinetic means to intimidate, paralyse or denude its politico-military response capabilities and enable winning without fighting or fight with minimum use of physical contact of own forces.[19]
- Non-Contact Warfare, in the elementary sense, represents an astute orchestration / choreographing of steering Military—Civil Operations

across a time continuum against adversaries. It is driven by national interests, wholly effects based, devoid of emotions and concentrated, thus enabling modulated application of national/coalition competences or abilities to construct incremental opportunities/ exploit weaknesses of states/non-states/organisations for extending influence, seeking favourable outcomes, amending 'Will' of adversary or partner through Smart Military-Civil Operations. Thus, an inclusive definition of Non-Contact Warfare should reflect the above paradigm. Non-Contact Warfare could defined as the intention to mark and elicit predictable responses from an array of inter-related objectives of an opponent (state or non-state) or coalition of adversaries transcending their entire national/organisation architecture viz. polity, leadership, population, infrastructure, society, culture, economy, psychology etc. by coherent application of assortment of all or precise assets/capabilities of a nation/coalition to seduce, persuade, prompt, coerce, modulate, subordinate, subjugate, or defeat the opponent(s)/adversary(s) into compliance, compellence or submission without resort to the necessity for force or physically entering into combat with it or with minimum physical contact. The effects conceptualised to be achieved by non-contact warfare tend to be incremental, gradual, cumulative, concurrent and dynamic and may occur during periods of peace, crisis, proxy war or war. Non-Contact Warfare thus implies a doctrine of conducting warfare that enables a nation or coalition of nation to target and incapacitate core capabilities of its adversary (perceived CoGs) without physical contact or with minimal physical contact with them in the battlefield or outside of it. The objective is not to enter into conflict, rather to force enemy into a disadvantageous position by imaginative application of national power and leverages over time. The conduct of non-contact warfare, in its truest sense demands patience, continuity, perseverance

and wisdom to coalesce the national/coalition capability towards the desired end state.

Conclusion

The Non-Contact Warfare is a comprehensive concept that enables a nation or non-state to weaponise each of its capabilities for further progress of its national interests. It migrates from the conventional understanding of effects in physical domain to an all-encompassing action to achieve domination and impact 'Will' of the target nation or non-state actor through sustained and generational application of capabilities across domains and dimensions.

References

1. Vladimir Slipchenko and Makhmut Gareev.*Future War*, Vladimir Slipchenko and Makhmut Gareev, Budushchayavoyna. Moscow: Polit.ru OGI.
2. https://medium.com/center-for-strategic-and-international-studies/lt-gen-h-r-mcmaster-harbingers-of-future-war-implications-for-the-army-full-transcript-92457635905e, address by Lt Gen H R Mcmaster Harbingers of Future War: Implications for the Army at Centre for Strategic and International Studies on 4 May 2016, accessed on 11 July 2024.
3. http://www.eastviewpress.com/Files ISSUE_No.4_2013.pdf, accessed on 19 October 2024. The Nature and Content of New Generation War by Col S G Chenikov and Lt S A Bogadanov, Military Thought, p. 15.
4. Nontraditional Warfare Twenty First Century Threats and Responses by William R Schilling, p. xv.
5. Ibid., n. 3.
6. Ibid.
7. Ibid.
8. Russian Sixth Generation Warfare and Recent Developments—Publication: Eurasia Daily Monitor, Volume: 9, Issue: 17, January 25, 2012, by Jacob W. Kipp.
9. Ibid.
10. The Revolution in Military Affairs—Weapons of the 21st century by Chang Mengxiong, in Part IV of China's View of Future War (Revised Edition), Edited by Michael Pillsbury, 1997 (National Defence University/Institute for National Strategic Studies).
11. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war, accessed on 9 March 2024.

12. https://www.thecipherbrief.com/article/gerasimov-doctrine, accessed on 8 July 2024.
13. https://www.files.ethz.ch/isn/189389/2015C09_kle.pdf, accessed on 31 October 2024.
14. Peter Mattsson's DSPC lecture in Riga "The Russian Armed Forces Adapted to New Operational Concepts in a Multipolar World?" Accessed on 20 August 2024.
15. The Nitisara by Kamandaki, Edited By Raja Rajendra Lala Mitra, published by The Asiatic Society 3rd Reprint 2023, Chapter V, p. 67.
16. World Military Almanac, 1997, pp. 291-294, also quoted in the book 'Unrestricted Warfare' by Col Qiao Liang and Col Wang Xiangsui, Natraj Publisher, p. 85.
17. US Army Special Operations Command—Counter-Unconventional Warfare White Paper, 26 September 2014, www.infor.publicintelleigence.net/USASOC-Counter UnconventionalWarfare.pdf, accessed on 4 October 2024.
18. As highlighted by Lt Gen Davinder Kumar, PVSM, VSM**, in his talk on Threats in the field of Non-Contact Warfare delivered at the 16th Tactics and Doctrine Seminar held at Army War College on 20 March 2017.
19. Brigadier Verma Vivek, Non-Contact Warfare—An Appraisal of China's Military Capabilities, published by United Services Institution of India, New Delhi, 2021, Chapter 1, p. 42.

Autonomous Systems and Artificial Intelligence: A Non-Traditional Threat to Humanitarian Security

Uday Pratap Singh and Mayank Saraswat

Abstract

Artificial intelligence (AI) and autonomous systems are developing out of pace, and it is a two-edged sword—both contributing to the active technological development and presenting a new and serious threat to the humanitarian security. This research paper examines the application of AI and autonomous technologies in the military surveillance and information fields, which jeopardizes international peace, ethics, and civil liberties. These systems are being designed to perform their functions with reduced human control making it difficult to hold governments accountable in warfare, simplifying government surveillance and making information warfare by use of disinformation techniques and manipulation. The emergence of autonomous weapons systems

Dr. **Uday Pratap Singh** is an Assistant Professor in the Department of Defence and Strategic Studies at Iswar Saran Degree College, University of Allahabad, Prayagraj. Dr. Singh is a keen researcher specialising in International Strategic Relations and National Security. Views expressed are personal.

Mayank Saraswat is a Senior Research Fellow at the Department of Defence and Strategic Studies, Iswar Saran Degree College, University of Allahabad, Prayagraj and specialises in contemporary security and strategic affairs. His research focuses on military reforms, regional security, and non-traditional security challenges. Views expressed are personal.

(AWS) with the capability to independently make lethal decisions is highly controversial with cognitive ethical and legal issues against the international humanitarian law because it jeopardizes our existing rules of war and principles of civilian protection. This has resulted in the use of invasive surveillance and data analysis technologies; AI-powered surveillance and analysis technologies have been used in the name of system security and cybercrime against privacy and civil liberties in democratic nations. Algorithms propaganda and deepfakes and the creation of cognitive manipulation threaten to destabilise the democratic process and social unity. This paper discusses how existing laws and codes of ethics are inadequate in coping up with these innovative issues and how they desperately need a widescale international regulation. The proposed strategy is community based and engages more than two stakeholders comprising regulation, transparency, citizen education and ethical creativity. It is essential to pursue an all-encompassing approach to constraint risks associated with artificial intelligence and autonomous systems being proactive and inclusive to protect the values of humanitarianism as the technological process rapidly runs forward.

Introduction

Humanitarian security, one of the most important components of the international law of human rights and humanitarian law, has traditionally referred to protection of people against war, persecution, poverty and other sources of harmful effects, which assault their dignity and survival. However, in the last two decades, humanitarian security has expanded to include new and non-traditional security threats, the most notable of which has been in new technologies. Among them, autonomous technology and artificial intelligence (AI) are the most competent and two-sided: they can transform the world in a positive way, improving human well-being and efficiency, yet, they also bring significant and not quite comprehended threats to international security and human rights.

The spread of AI systems into information, surveillance, and military is an extreme change to the exercise of power and war. War and governance are no longer confined to human-platformed space, but now more than ever before, autonomous decision systems are able to operate autonomously, make decisions based on experience and scale faster than ever before. These technologies can evade conventional restrictions on state and corporate authority, subverting the ethical principles of humanitarian law and accountability regimes, starting with swarms of drones and facial recognition technologies and deepfake disinformation and social manipulation codes.

The application of autonomous systems circumvents accountability to the people, as it is either secret or not mandated by the people. The technologies are used to entrench political power and suppress dissent to the authoritarian governments. Their use is possible even in the democratic environment and can be included in over-policing, systemic discrimination, or unnecessary violence of untransparent algorithms and unaccountability. In addition, the pace of AI development is expected to exceed the regulation, creating an administrative loophole and endangering civilian populations. The technological issues do not end with the question of use of the technologies but with the design, purpose and value system of the technologies. The use of algorithmic decision-making, as an example, can reproduce and recycle the biases that exists in society, and autonomous systems of weapons undermine the nature of the human choice regarding life-and-death decisions. The danger of these innovations is that they standardize a reduced role of human judgment in the area where ethical consideration and humanitarian principles can be applied.

The concept of International Humanitarian Law (IHL) did not consider an artificial intelligence, and its format is not able to consider the presence of algorithmic actors in a war. There is still legal uncertainty in the area of liability against harm caused by independent actors and

this complicates the ability to redress harm to the victims as well as it eases impunity. These difficulties are blown out of proportion in conflict zones and failed states whereby the rule of law is weak and there are incomplete or absent system of checks and balances. In this article, the range of such unconventional threats will be defined with the focus on how the autonomous systems and AI can undermine the principles and implementation of the humanitarian norms. It is going to address their effects on war, spying on civilians, controlling the mind, and governing ethically. It is in such analysis that the paper seeks to elevate to the front burner the direct and indirect humanitarian consequences of autonomous technologies, which requires the humanity to look ahead and take multi-disciplinary action to regulate autonomous technologies and a renewed commitment to uphold human dignity in the context of technological disruption.

The Emergence of Autonomous Systems

The development of autonomous systems and AI (Artificial Intelligence) is one of the most essential technological developments in the 21st century. These systems, which were once reserved for the realms of science fiction, now rule over every aspect of society—ranging from individual computer users and robotic vehicles to army drones and decision support systems. Machine autonomy is not a completely new concept. Historical attempts to construct machines with autonomous capabilities began with the invention of the autopilot system in the 1920s, which enables aircraft to maintain consistent flight courses without constant human supervision. However, the addition of AI has significantly expanded the potential of these systems.[1]

Their rapid evolution and integration into vital infrastructure and planned sectors have enabled them to move from simple tools to instruments with insightful diplomatic, social, and human results. The ability of artificial intelligence systems to mimic otherwise retroactive

human cognitive methods, such as studying, reasoning, and decision-making, is a key element in this advanced adaptation. These systems utilise massive data sets and sophisticated algorithms to analyse form, adapt to new data, and develop autonomous systems that operate without human supervision. As automation continues to exist longer and longer in production and planning, the preamble of machine learning and nervous alliances has allowed a new degree of autonomy, capable not only of carrying out a project but also of moving from one environment to another in real time.

The expanding increase in computerised control and information dissemination is one of the major drivers of this transition. Self-supporting frameworks gain access to a continuous flow of objective knowledge as the global Internet connectivity expands and the Internet of Things (IoT) grows. The current real-time input cringle improves its accuracy, performance, and autonomy. For instance, robotic vehicles are capable of promptly detecting congestion and adjusting their navigation plans on the fly. At the same time, autonomous drones are capable of pinpointing and tracking targets without the need for human input. The regimes and industrial actors invest considerable effort in studying and developing AI, recognising that their power can be applied not only in academic writing to enhance fiscal productivity but also in adjusting the balance of control in national security. China, the US, and the Continental coalition have all undertaken calculated efforts to dominate the AI invention, regularly setting the pace for superiority in military and international requirements.[2] This aggressive landscape has enabled a surge in dual-use technologies—AI applications that help both civil and military objectives. All the goods in that dual-use trajectory are independent surveillance systems, predictive police algorithms, and Unmanned Combat Aerial Vehicles (UCAVs). Still, the current increase has no effect in a vacuum. Self-supporting artificial intelligence systems raise significant concerns about accountability, management, and safety, in addition to their

advanced capabilities. The 'black box' environment of some AI models, in particular deep learning structures, is a key subject. Their inner logic and decision procedures are often opaque to their creators, making it difficult to imagine otherwise explaining their behaviour.[3] That opaqueness, when used in contexts where humans live, such as war, health care, and condemnable righteousness, becomes particularly hazardous.

Moreover, conventional management and moral structures are becoming increasingly autonomous AI structures. Some regulations and conventions concerning war, secrecy, and human freedom were planned before intelligent devices could be achieved. As a consequence, yonder could be a legitimate and virtuous vacuum that encompasses the deployment of artificial intelligence in delicate areas. For instance, who is in charge of the assumption that a self-supporting weapon falsely identifies and extinguishes a civilian target? The programmer, the commander, or perhaps even the algorithm itself? These problems remain largely unsolved. The autonomy arrangements also have a broad monetary and social influence. Artificial learning-based automation threatens to displace large parts of the global workforce, especially in manufacturing, transport, and buyer support. This disturbance may further exacerbate existing inequalities and produce recent forms of social volatility, especially in provinces that are already defenceless. At the same time, concerns about digital colonialism and advanced monopoly are raised by the concentration of AI skills by few powerful corporations and governments. However, these problems, the pace following self-supporting measures and automated reasoning, are unbroken. Various entities exploited the temptations of effectiveness, cost-effectiveness, and critical advantage to take AI remedies that were not subject to satisfactory supervision, as well as ethical aspects. During few international initiatives and considering the tank's name as a further cautious and human-centric strategy, such efforts are still nascent and distant. However, the international society must initiate strong governance arrangements that can keep pace with the rapid

adaptation of artificial intelligence tools. Consequently, the development of autonomous structures and artificial intelligence constitutes a crucial split second in the history of humans, guaranteeing immense assistance but also requiring unprecedented challenges. It is essential to critically analyse how these systems are improved, deployed, and managed in sectors such as the defence mechanism, the enforcement of human rights, and the protection of human rights. The unfettered growth of artificial intelligence would not lead to empowerment but to the elimination of prerogatives, the aggravation of inequalities, and the weakening of human security.

Artificial Intelligence and Autonomous Systems in Warfare

Autonomous Weapon Systems (AWS), such as drone driving, loitering weapons, AI-guided missiles, and robotic land vehicles, are developing and threatening humanity's security. Unlike conventional weapons, AWS can provide precise engagement, target identification, and target prioritization—all capable of autonomous operation.[4] Their integration into the modern military arsenal reveals a complex mixture of ethical, permissible, and human-centred dilemmas, namely responsibility, bigotry, and proportionality under International Humanitarian Law (IHL).[5] The removal of human perception from serious life and death verdicts, together with AWS, is one of the primary terrors. Traditional rules of engagement rely on human fighters' ability to ethically deduce, discretion, and empathy, which AI frameworks inherently lack. This lack of human conscience increases the risk of an indiscriminate or unbalanced attack, particularly on a densely populated environment or an environment with a narrow intellect. A misplaced target due to differential errors or other adversarial statistical manipulation may result in significant civilian casualties and sustained damage. Furthermore, the use of automated reasoning in defence decision-making entails a risk of rapid escalation of disputes. Autonomous systems operating at high speed

can respond to understand dangers that do not have a let-up interval for human diplomacy. This can lead to unintended escalation, accidental war, or misattribution of an attack in a tense global context.[6]

Furthermore, the spread of AWS techniques across state and non-state actors increases the world's uncertainty, as rogue governments or terrorist groups are likely to acquire and deploy such systems, with little concern about valid or ethical guidelines. Lack of clear trustworthiness in the event of misuse or failure is another critical aspect. Assuming an autonomous weapon accidentally kills a population, establishing liability is a matter of debate: should responsibility lie with the developer, the manufacturer, or the commander, or should it be the statement that authorises it?[7] This ambiguity jeopardises the fundamental standards of IHL, which are built upon the theory of human liability for misdemeanour. In practice, it may also hinder fairness and compensation for victims of wrongful attacks.

Although, there is a growing need for governance and international consensus on the regulation of AWS, several states are promoting a pre-emptive ban on all autonomous weapons, similar to the current treaties on chemical and biological weapons. Others argue that such structures may be used ethically and competently, provided they are properly monitored. However, the pace of the development of artificial intelligence and the significant advantage offered by AWS continue to drive their expansion. The arms race in self-armed vehicles is expected to accelerate without clear conventions and treaties. For defence surveillance, pre-emptive targeting, logistics organisation, and psychological operations, artificial intelligence is continuously being employed. Such abilities may be exploited to regulate societies, suppress dissension, and disrupt society in a non-kinetic way. Similar to AI, war was not only about the extermination of the body but also about control, coercion, and laterality. A multidisciplinary technique is needed to overcome these obstacles. Legitimate standards must be updated to reflect the world of AI-enabled war, including clear definitions

of AWS and a stringent supervision mechanism. The irreplaceable character of human management and moral obligation must be highlighted in the standards of morality. Digital precautions should be mandatory, such as failsafe, audited account history, and human-in-the-loop architecture. In particular, to prevent the standardisation of self-reliant brutality and to continue human standards governing combat behaviour, global dialogue and cooperation are of paramount importance.

Surveillance and Privacy Erosion

Introduction of AI innovations into surveillance arrangements has transformed the atmosphere of privacy and courteous autonomy—marking a significant shift in the symmetries between the pronouncement authority and individual immunities. Together, authoritarian and democratic governments are increasingly using artificial intelligence tools such as facial recognition, pace analysis, biometric identification, police planning, and interpersonal marking systems.[8] These systems, which regularly take place under the banner of national security or societal safety, pose significant challenges for human-centred security by facilitating intrusive, uninterrupted surveillance on civilian populations. Artificial intelligence surveillance has become a cornerstone of electronic dictatorship in authoritarian countries. To monitor virtual actions, track material movement, and prevent dissent, governments employ sophisticated artificial intelligence techniques. For instance, China's communitarian loan structure and its widespread use of facial identification innovations in localities enjoy Xinjiang's pull of transnational disapprobation for enabling mass surveillance and oppression of cultural minorities.[9] Such practices are violating the right to confidentiality, but they also create an atmosphere of fear, coercion, and bias.

Automated reasoning surveillance can lead to the marginalisation of vulnerable neighbourhood areas even in a democratic society.[10] Predictive

police methods, based on biased old criminal data, are usually directed at disproportionately targeted low-income areas and cultural minorities.[11]

In the contemporary scenario, certain actions reinforces inequalities that may lead to distortion of society's confidence. Furthermore, many artificial intelligence surveillance systems are being used without acceptable transparency and supervision, which society approves of, leading to panics about democratic accountability. Freedom of expression and association is also affected by the increase in omnipresent surveillance. Know that activities of individuals, movement, or communication can lead to self-censorship and reduced local involvement.

Confidential companies also play a key role in the development and use of surveillance AI. Technical school organisations frequently cooperate with the government, equipment suppliers, and networks for mass data collection and evaluation. The aforementioned innovations are exported to the government with defective human rights data and thus facilitate abuse. Furthermore, the commercialisation of surveillance raises legitimate questions concerning net income and human rights aspects, particularly when systems are subject to opaque terms and strict restrictions on end users.

Furthermore, cyber vulnerability occurs in case the large volumes of unique information are gathered and processed through automated reasoning systems. Violation of statistics, the access of unauthorised access, and the misuse of sensitive data may lead to severe consequences such as personal theft, reputational burden, material threat. A report identified 84 percent of AI tools as having been hacked with user credentials and infrastructure vulnerabilities, which are heightened by aggregating vast amounts of data.[12] This information may be used to attack targeted groups or against another individual which may worsen human conflict.

The erosion of confidentiality requires effective legal and moral frameworks. Administrations need to define boundaries on monitoring, anchorage, proportionality and human rights respect. In order to reinforce

the strict visibility and accountability requirements with independent audited accounts, public disclosure, and recourse, automated reasoning systems used on surveillance should exist. Notably, there should be strict regulations on the clustering, storage, sharing, and use of the data around, and there should be strong protection against such misuse. A key role in performing surveillance methods and recommending a rights-based approach to technology administration is held by a courteous community and world corporations. Global cooperation is essential for harmonising privacy standards, limiting exports of inhibitory tools, and promoting computer privileges. The transnational neighbourhood can ensure that technological progress does not come close to sacrificing essential freedom only through organised action.

Manipulation and Information Warfare

Artificial intelligence has transformed the nature of information warfare dramatically—introducing new tools and techniques that are capable of influencing public opinion, discrediting institutions, and initiating violence. Some of the most concerning tendencies include AI-generated disinformation, deepfakes, algorithmic boosting, and microtargeting. These technologies enable state and non-state actors to structure the cognitive space of populations in ways unimaginable before, making the battlefield not one of geography but of psychology. One of the most powerful information warfare weapons today is disinformation generated by AI. It can create highly realistic text, audio, and video content in bulk, and it is difficult for individuals to discern what is true and what is false. Such tools are utilised to produce credible stories that are for ideological, political, or strategic reasons. Social media platforms, in particular, are fertile terrain for the dissemination of such content since algorithms prefer engagement to fact and amplify sensational or polarising content. A 2018 study conducted by MIT found that fake news stories on Twitter were 70% more likely to be retweeted than true stories.[13]

The danger of deepfakes—extremely realistic synthetic videos created on the basis of deep learning, is a peculiar threat. They are able to make up evidence, pose as high personalities, or fabricate activities, which were never entered into. This invalidates the credibility of honest media and they can be applied to invalidate adversaries, release fake news or excuse violence. A successful deepfake in a conflict zone or at an election period will trigger riots, discourage voters, or even hamper political processes.[14]

It also eliminates the need to guess during psychological campaigning with the help of AI, which enables microtargeting to target specific audiences. The artificial intelligence-enhanced microtargeting widens social and political divisions by creating individual content images or videos that resonate with a particular group of values, fears, or prejudices.[15] AI can find the suitable individuals based on what they do on the internet and construct messages that will appeal to their phobias, prejudices, and interests. The targeted messages can affect the electoral behaviour, split societies, and even radicalise people. The Cambridge Analytica scandal showed how these methods were being exploited to control the democratisation process and the general opinion. Such AI-related strategies have devastating humanitarian implications. Ethnic violence, mass hysteria, and subversion of health and safety programs have been allied with the use of disinformation campaigns. Indicatively, during the COVID-19 pandemic, AI-generated fake news on vaccination caused vaccine hesitancy and preventable mortality. Estimates show that anti-vaccine tweets resulted in 750,000 avoidable refusals to vaccinations in the US alone which led to at least 29,000 cases and 430 deaths between Feb-Aug 2021.[16] To increase the hostility, manufactured information makes it harder to provide humanitarian aid because of the distortion of facts on the ground.[17] Since citizens do not know what to believe and what not to believe, social cohesion is destroyed, conspiracy theories are popular, and a reasonable debate is almost impossible. Lost trust does not only undermine the stability of the government of the home

country but also undermines international collaboration in dealing with international crisis.

Fighting information warfare of AI kind demands a number of strategies. Technology companies should take responsibility for the design and effect of the algorithms. Sites should have very powerful content verification mechanisms, increase the level of transparency in content moderation, and provide the user with tools to report and identify fake news. Governments need to implement laws that deal with trickery on the internet and safeguard the freedom of speech. It is also important to increase media literacy and critical thinking. Teaching individuals to consider and authenticate information before publishing can potentially restrict the extent of manipulative content. Fact-checking organisations, independent media, and schools all have roles that they can fulfill in supporting information resilience. On a global scale, diplomatic means are necessary to establish norms and deterrents against state-sponsored information warfare. Since chemical and biological weapons are universally banned, there must be a universal consensus on AI use in the information space that is acceptable. Regarding this, the Framework Convention on AI (Council of Europe), signed by over 50 countries in September 2024, establishes binding commitments based on human rights, democracy, and the rule of law to govern AI systems.[18]

Ethical and Legal Challenges

The current legal and ethical frameworks for artificial intelligence (AI) and autonomous systems are unable to keep up with the rapid technological development and their dual uses in civilian and military situations. The absence of detailed, implementable rules and regulations has left a void through which the unchecked development and use of potentially destructive technologies is possible. This section identifies the central ethical and legal issues presented by AI and autonomous systems in humanitarian security. One of the core ethical issues is the

mission of life-or-death choices to machines. Autonomous Weapon Systems (AWS), which can choose and attack targets independently without human supervision, threaten basic concepts of human dignity and moral accountability. The application of machines to take such crucial decisions disintegrates the ethical necessity of human judgment, which is necessary in war to segregate combatants from non-combatants and balance the proportionality of use of force. Most ethicists consider that giving lethal force to machines dehumanises war and undermines the moral accountability framework inherent in International Humanitarian Law (IHL).

The AI-based surveillance systems also have ample space even in the current statute, and it will present immense ethical and legal consequences. These systems can process and analyse large reservoirs of data to monitor civilian populations often without their knowledge or oversight. There is the violation of personal privacy, privacy of expression and association and this is contrary to the laid human rights standards. In any democracy, predictive policing and gazing at the population with AI may reinforce racial profiling and institutional prejudice.

Further, there is an ethical issue with algorithmic bias. The impartiality of AI technology is based on the data it is trained on. Distorted data may have unfair consequences, such as in law enforcement, work, and social services. This has also been complemented by non-existence of transparency to AI models (so-called black box models), which neither allows explaining how decisions are reached, nor does it provide the ability to redress or appeal in the case of harms. The third significant issue is AI asymmetries in the world. The technological sovereignty is not evenly distributed with the dominance of the AI landscape by the rich countries and large corporations. A significant number of developing countries lack the resources and political systems to ensure that their people are not exposed to the predatory and malicious uses of AI. This inequality

is ethically and morally problematic, as technological advancement is becoming another source of geopolitical power.

This will need a solid moral and legal system to fight it. It is being called internationally to have a binding lethal autonomous weapons treaty that would have actual human control of all weapon systems. Both the Campaign to Stop Killer Robots and the many machineries of the UN have emphasised the need to take preventive actions against the spread of the AWS, as it is ineffective to regulate it once it has spread. There is also a need for strong legal defence against invasive AI surveillance, transparency, and accountability of algorithms. The principal international documents, such as AI Act of the EU and OECD AI Principles, serve as the platforms to use AI in a moral manner. In 2019, OECD member and partner countries had a set of AI Principles, which provide a set of five ideals when it comes to ensuring ethical development and production of AI systems and applications, thus bringing benefits in the form of human-centered ideals, fairness, and robustness, security, and safety.[19] These are general rules that are embraced to assist governments and commerce institutions to connect AI innovation and moral issues.

The EU AI Act, introduced in 2024, was the first comprehensive system of laws to control the use of artificial intelligence in the world. The Act defines four categories of risk to AI systems viz. unacceptable, high, limited, and minimal risk.[20] It is prohibited to use AI systems that are determined to pose intolerable risks, including social ranker and biometric surveillance in the streets. High risk AI systems, especially those that are used in critical sectors such as healthcare and law enforcement, are subject to strict standards regarding the quality of data, transparency, human control, and safety. To ensure that AI does not violate the fundamental rights and the principles of democracy within and without the EU, the Act focuses heavily on human-centred approach. The two frameworks should be considered as the key resources of countries and organisations that are trying to adopt AI in a responsible manner morally and socially.

These technologies should be informed by an ethical code of AI standards and development. These are human rights respect, fairness, transparency, accountability and inclusiveness. It is now time that the tech communities, lawmakers, civil society organisations and international institutions come together and entrench these principles in both codes of law and institutional procedures. Besides this, third-party regulatory bodies and ethics committees ought to be introduced to monitor the utilisation of AI, especially in the critical fields such as security and defence. Lastly, the integration of AI technology and autonomous systems into society necessitates a change in the existing ethical and legal frameworks—as these markets and technologies evolve, the regulatory framework governs them to evolve as well. The challenges against humanitarian security can only get worse without such kind of proactive, coordinated efforts to safeguard human dignity and strengthen legal systems.

Humanitarian Implications

Combination of the advent of artificial intelligence (AI) and autonomous systems with modern society, and, more specifically, military and security activities has far-reaching and drastic humanitarian impacts. These technologies poses threats to the civilian population, ethical mores, and international stability. The unexpected consequences and tactical misuse of AI mechanisms will probably intensify the sufferings of humanity, the decrease of humanitarianism operations and the weakening of human rights and the IHL. The increased risk to civilian lives during armed conflict is, perhaps, the most urgent humanitarian problem. Autonomous Weapon Systems (AWS) that are capable of working without the participation of a human being may not necessarily know the distinction between fighters and civilians. This indiscriminate character may cause extravagant devastation in congested cities or in bad topography. Without proper human control, this type of systems may also violate IHL principles

of distinction, proportionality, and precaution. Also, machine learning can fail or act unpredictably in fluid fight situations, putting more people in danger of unintended casualties.

The other notable impact is conflict with humanitarian operation in conflict zones. To deliver aid and protect the affected people, humanitarian organisations depend on accurate information, secure communications and free movements. Surveillance and cyber activities using AI can impede these activities. Information warfare and AI-enabled cyber operations are becoming increasingly common to undermine humanitarian efforts, thus warning aid providers of their ability to coordinate, communicate, and protect their data and information.[21] State and non-state actors are increasingly employing AI to monitor the activities of aid agencies, disrupt logistics via cyberattacks, or to undermine the activities of humanitarian organisations and activities by discrediting them. Not only does this put the aid workers at risk, but also kills the trust between the foreign relief actors and the locals.

Surveillance systems with AI also pose a great threat to privacy and freedom of expression, especially in totalitarian regimes. These technologies enable mass data collection, identification of faces and the determination of behaviour that enables pervasive surveillance. Such surveillance can be used to check and oppress political opposition, religious minorities or refugees. As an illustration, a leaked document shows that the government of North Korea uses Chinese biometric technologies and facial recognition in businesses and schools to track individuals, suppress dissent and limit their freedom.[22] In occupied territories or refugee camps, where humanitarian needs are urgent, monitoring may further alienate the already vulnerable populations. AI systems also increases number of inequalities in the world and strengthens digital colonialism. Since, the majority of AI breakthroughs are created by some technologically developed nations and individual corporations, and systems are therefore sold or implemented in other parts of the world, hence marginalised

communities, that have low digital literacy or government abilities, are highly susceptible to the harms brought by these systems. This digital divide not only widens the inequalities that already exist, but also makes the autonomy of marginalised communities.

The application of AI in humanitarian situations may raise ethical issues of neutrality, impartiality, and consent. Biometric identification technologies and predictive analytics, that are regularly used in managing refugees or handing out aid, may violate the privacy of individuals accidentally or might even stigmatise the recipient. In the absence of regulation, such technologies may entrench discriminatory trends that are harmful or may be bent towards security interests. As an illustration, information acquired on behalf of aid provision, can be shared by counter-intelligence agencies, thus jeopardising the security of refugees and asylum seekers. Another humanitarian impact of unregulated AI implementation is trust in institutions. In the event in which people are victims of the harm or mistreatment caused by the AI systems in discriminating decisions, unfair surveillance, or autonomous cruelty, they may lose their trust in government, humanitarian organisations, and international bodies. The unmediated loss of trust may bewilder peace-making efforts, increase social divides and frustrate long term peace making. It is on this basis that the issue of humanitarian interests must be prioritised in the regulation of AI and autonomous systems. A collective duty of developers, policymakers and humanitarian communities should be to design technologies, that are being respectful of human dignity, transparent and rights protective. Risk analysis, social consultations, and moral effects should be regulated before deployment in special settings.

Mitigation Strategies

Considering the complex risks of autonomous systems and artificial intelligence (AI) to humanitarian security, it is critical to have a proactive

and holistic approach to mitigation. To tackle the issues, it will be necessary to have joint efforts by governments, international bodies, civil society, institutions of higher learning and the business world. Mitigation should be oriented towards the legal regulation, ethical design, transparency, capacity building and international cooperation.

Setting up Strong International Norms and Legal System

One of the most important strategies is the creation and implementation of legally binding international treaties and agreements that govern the development and use of AWS and surveillance AI. Especially in the field of autonomy in warfare, updates are required because the ambiguity in the IHL, with regards to AI, is currently present. One of the new normalcies that ought to be entrenched by international institutions such as the United Nations (UN) and the International Committee of the Red Cross (ICRC) is the notion of meaningful human control over the weapon systems. Another measure that can be taken for halting indiscriminate violence and safeguarding human dignity, is the outlawing of or tight regulation of wholly autonomous lethal weapons.

Enhancing Ethical AI Design and Development

Ethical factors must be included in the development of AI and autonomous technologies at the initial stage. Developers and businesses need to adhere to the human-centred design principles that prioritizes safety, equity, accountability, and transparency. When they are used in the context of security and humanitarian situations, they should be assessed for potential damages to the system by third-party audit and ethical review boards. Algorithms must be constructed in a clear line of responsibility, reduce bias, and human rights should be observed. Ethical deployment guidelines are available in such standards as the OECD AI Principles and the AI Act of the EU.

Assuring Transparency and Accountability

To establish trust and prevent abuse, there must be transparency in the operation of AI systems. Review and legal recourse require explainability, or human comprehension and challenge of AI decisions. Governments and other organisations utilising AI should publicize the purpose, scope, and impact of the technology, particularly in the field of military, policing, and surveillance.

Enhancing International Collaboration and Institutional Potential

The global regulation of AI needs international cooperation. National platforms should also be established to promote exchange of best practices, communication and international understanding. The benefits and downsides of the novel technologies can be mitigated with the assistance of collaborative research works, especially those that focuses on AI to achieve humanitarian goals. The Global South should be strengthened, equitable access to AI advancements must be ensured, and the communities must be safeguarded against abusive AI use. International development organisations may be of great help by offering regulatory support and technical assistance in increasing capacity.

Developing Digital Literacy and Citizen Participation

The key to avoiding manipulation and information warfare is to educate the population about the possible harm that artificial intelligence may cause. The educational systems should incorporate technological skills and critical thinking would allow individuals to detect and resist false content, deepfakes and algorithmic bias. Media outlets, civil society institutions, and academic institutions will have to collaborate to disseminate proper information and promote digital resilience. The informed citizens are an important defence line against manipulative psychology and the degradation of the language of democracy.

Increasing Data Protection and Privacy Gates

Strong laws on data protection and confidentiality are essential because of the amount of data that AI systems operate with. Governments should implement clear legislation governing the collection, storage, and utilisation of information particularly in sensitive humanitarian contexts. Policies of data must focus on authorisation, anonymity, and restriction of purpose. The security of the data gathered in the course of humanitarian actions should also be ensured with the help of international protocols that prevent biometric information misuse. The privacy-by-design principles must be implemented in AI systems.

Ethical Humanitarian Innovation Support

Humanitarian organisations should develop internal policies and ethical standards when adopting AI methods in their activities. They were to be made up of risk-benefit analyses, community consultations, and anti-misuse. The use of AI by NGOs and international agencies will build trust among the affected populations. Crisis response technologies, delivery and tracking technologies, and refugee tracking technologies should be reviewed and ethically monitored on a regular basis in order to prevent unintended consequences or mission creep.

Research on AI and Humanitarian Security

The collaboration between AI, autonomy, and humanitarian law is an area that requires the support of academic institutions and think tanks. There is a need to conduct additional empirical studies on the practical implications of autonomous systems in crisis and conflict situations. This research can shape policy, ethical design and early warning signs of AI abuse. Devoted funding and partnerships of governments, NGOs, and academic institutions can hasten this knowledge base.

Conclusion

The increasing growth of autonomous systems and artificial intelligence have opened a very radical but very ambiguous new period of humanitarian security. The most recent developments have created machines that are extremely competent and in certain tasks, outperform human beings. But just under these technical refinements is an intelligence which is still so narrow, brittle and vulnerable. The existing AI systems lack general-purpose reasoning and is not reliable for transferring knowledge across contexts. They are still left to human judgment as to when they are to be applied, how far their restrictions are to be interpreted and where the dangers and disadvantages outnumber the advantages. Their use in the absence of such management puts the principles of humanitarian protection at risk.

In all spheres, the fundamental weaknesses of modern AI, such as unpredictability, lack of explainability, undependable verification, and bias prone data represents structural threats. The systems that are trained using faulty objectives or on erroneous data may develop unwanted behaviours that multiply threats to civilians, humanitarian interventions, and weak communities. As such systems move out of the controlled laboratory setting to the unstable real-world settings, the pressure of providing safe and responsible behaviour increases dramatically. This difficulty is particularly acute in a military context, where there are high levels of operational stakes, rapid adaptation, and deception, which makes it hard to test and validate. The results of failure in these situations are not hypothetical—when life-threatening systems get dysfunctional, the damage that it causes can be irreparable and devastating. Simultaneously, AI, when used non-militarily, surveillance, disinformation, algorithmic profiling, and data exploitation are transforming humanitarian security to the detriment of privacy, human dignity, and democratic institutions. When implemented with insufficient protection, these systems become even more acute social injustice, disproportionately impacting vulnerable

groups, and disrupting humanitarian efforts, which require trust, impartiality, and transparency. Therefore, the risk of self-directed and AI-driven technologies is not limited to the battlefield. It has spilled over into the political, economic and social life of societies, where decision-making is more and more concentrated in the hands of opaque algorithmic processes by the strong states and corporations.

This developing environment requires a fundamental redefining of humanitarian security—one that goes beyond the traditional and includes non-traditional risks posed by machines as independent actors. The management of AI cannot be considered only as a technical issue—it is legal, ethical and political by nature.

The autonomous systems need a multi-layered response to mitigate the risks. Effective ethical methods, explicit lawful requirements, and enforceable technical principles have to be the basis of responsible governance. These actions should be accompanied by the real international collaboration that incorporates the humanitarian value system into the centre of technological progress. The design, implementation and monitoring of AI systems should be guided by human welfare, international law and the need to uphold fundamental rights.

More importantly, the discussion of the policy issue should not be narrowed down to whether AI will keep progressing or not. Autonomous Systems might be able to increase the efficiency of humanitarian logistics and minimise human susceptibility to harm, but they are equally likely to become the source of oppression, propagate violence, and increase inequality. The course they take will be determined by current choices. This scene is a climactic point. The international system needs to come up with governance structures that are indicative of collective responsibility and commitment to humanitarian security. In this way, states and institutions will be able to make sure that autonomous systems and artificial intelligence are developed as a tool that strengthens human dignity instead of undermining it. It cannot be left to chance that the

balance between innovation and the values that human beings hold at heart should be safeguarded by an action on policy that is principled, inclusive, and futuristic.

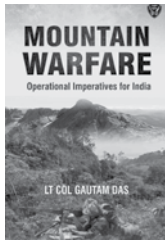
References

1. Goud S., Kaul H., Chinnegowda H. S., The Rise of AI and Autonomous Systems: Transforming Industries and Navigating Ethical Challenges, IJRASET, Journal for Research in Applied Science and Engineering Technology. December 06, 2024. https://www.ijraset.com/research-paper/transforming-industries-and-navigating-ethical-challenges
2. Horowitz M., Kania E.B., Allen G.C., and Scharre P., Strategic Competition in an Era of Artificial Intelligence, CNAS, July 25, 2018. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence
3. Op. Cit. https://www.ijraset.com/research-paper/transforming-industries-and-navigating-ethical-challenges
4. Lt Gen (Dr) Panwar R.S., AI in Military Operations, Concepts and Doctrines, Transformation, FUTURE WARS, October 29, 2024. https://futurewars.rspanwar.net/defining-autonomous-weapon-systems-a-scenario-based-analysis-part-i
5. Santos E.A., Autonomous Weapons and International Law, Diplomacy and Law. https://www.diplomacyandlaw.com/post/autonomous-weapons-and-international-law
6. Proceed with Caution: Artificial Intelligence in Weapon Systems, From Chapter 3 ("Escalation and an AI arms race"), under "Stuck on the escalator?", UK House of Lords, December 01, 2023. https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/1607.htm
7. Minhas A., The Legal Framework Governing Artificial Intelligence in Warfare: Challenges and Opportunities, Record of Law, University of Greenwich, April 18, 2025. https://recordoflaw.in/the-legal-framework-governing-artificial-intelligence-in-warfare-challenges-and-opportunities/
8. Eneman M., Ljungberg J., Rolandsson B., The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities, DOI Foundation, Volume 27, Issue 2, May 1, 2022. https://doi.org/10.3233/IP-21153
9. Qiang X., The Road to Digital Unfreedom: President Xi's Surveillance State, Journal of Democracy, January 2019. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/
10. Brayne S., Big Data Surveillance: The Case of Policing, National Library of Medicine, August 29, 2016. https://pmc.ncbi.nlm.nih.gov/articles/PMC10846878/
11. Shared Statement: 'Predictive Policing' Systems Rely on Biased Data, Exacerbate Disparities, Brennan Center for Justice, August 31, 2016. https://www.brennancenter.org/our-work/analysis-opinion/shared-statement-predictive-policing-systems-rely-biased-data-exacerbate

12. Analysis of AI tools: 84% breached, 51% facing credential theft, Cybernews Team, May 8, 2025. https://cybernews.com/security/ai-tools-data-breaches-workplace-security-risks
13. Muirhead R., Deepfakes and Disinformation: The Dark Side of Generative AI. https://www.richardmuirhead.pro/blog/deepfakes-and-disinformation-the-dark-side-of-generative-ai
14. Ibid. https://www.richardmuirhead.pro/blog/deepfakes-and-disinformation-the-dark-side-of-generative-ai
15. Political microtargeting deepens social divides – and AI is making it easier, Universiteit van Amsterdam, July 2, 2025. https://www.uva.nl/shared-content/uva/en/news/news/2025/07/political-microtargeting-deepens-social-divides---and-ai-is-making-it-easier.html
16. Bollenbacher J., Menczer F., John Bryden J., Effects of Antivaccine Tweets on COVID-19 Vaccinations, Cases, and Deaths, arxiv, June 13, 2024. https://arxiv.org/abs/2406.09142
17. Katz E., Liar's war: Protecting civilians from disinformation during armed conflict, International Review of the Red Cross, December 2021. https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914
18. Framework Convention on Artificial Intelligence, Wikipedia. https://en.wikipedia.org/wiki/Framework_Convention_on_Artificial_Intelligence
19. OECD AI Principles overview. https://oecd.ai/en/ai-principles
20. European approach to artificial intelligence. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
21. The rise of artificial intelligence requires a human-centred approach in conflict zones, The International Committee of the Red Cross, July 24, 2023. https://www.icrc.org/en/document/rise-artificial-intelligence-requires-human-centred-approach-conflict-zones
22. North Korea deploys Chinese surveillance technology to workplaces, The Times, April 17, 2024. https://www.thetimes.com/world/article/north-korea-deploys-chinese-surveillance-technology-to-workplaces-wzvjqbrhw

Book Reviews

Mountain Warfare: Operational Imperatives for India
By Lt Col Gautam Das



Publisher: Sabre & Quill (2025), Price 1299/-,
Hardcover, pp. 247, ISBN: 978-8119509430

Review by RC Patial

Why did I pick this book '*Mountain Warfare: Operational Imperatives for India*'? For an infantry soldier from the Gorkhas and a mountaineer who has served the length of the Himalayas, from the West to East, the title was catching to be picked up and go back into the memory lane and see what the author, Lt Col Gautam Das—a soldier and mountaineer himself had to share on Mountain Warfare with the reader. The reputed author has authored over ten books and has generally written around the Himalayas and our immediate adversaries of today and the future focused on our strategy around Himalayas, "Mountain Warfare the wars of our future".

I have spent much of my life in the shadow of these mountains, serving, trekking, climbing, and sometimes simply sitting still in their silence. From the icy passes of Ladakh to the peaks of the Karakoram Ranges leading onto the highest battlefield of the world viz. the Siachen Glacier, to the mist cloaked ridges of Arunachal, and across the sacred terrain up to Kailash–Manasarovar in Tibet, I have seen the Himalayas

Colonel **RC Patial**, SM, FRGS, PhD is a retired Infantry Officer of 11 GR. He possesses unique experience of serving in active CI Ops across the country and in Sri Lanka. Has served with the NSCS as a Senior Defence Specialist and in NTRO as OSINT Chief Editor. Currently, he is the Principal of Amity Indian Military College, Manesar. Views expressed are personal.

in all their moods: majestic and merciless at times. I have had the opportunity of being appointed as the Red Land Commander (PLA) for the Tawang Sector in Arunachal and twice in Rajouri sector (Pak) and in these wargames the Blue Land was convinced to have a Rethink on their Op Plans!

Lt Col Gautam Das's *Mountain Warfare* is not just another military treatise; it is a timely intervention in India's strategic conversation. While technology and networked warfare dominate contemporary discourse, the author repeatedly returns the reader to an immutable reality: geography and human endurance still shape outcomes in the high Himalaya. His mix of picked up soldierly narratives, doctrinal discussions and operational lessons forces civil-military planners and citizens alike to confront the limits of mountain operations with a rethink. In doing so, the book bridges the lived world of the infantryman who breathes thin air on a ridge, and the abstract, data-driven world of strategy-makers of the AC offices and the viewers in their drawing rooms.

'*Mountain Warfare: Operational Imperatives for India'* is divided into Six Chapters. I quite liked the brief prologue and the preamble to the book. The author has largely quoted the ground soldiers of various operations as part of the post-independence history in minutest detail providing near real narratives of facts not known to many earlier. I was not aware of the details of the 1971 war fought in Partapur Sector, as much has not been written about it. It does focus on the vagaries of High-Altitude Mountain Warfare and how Maj Rinchin overcame the battle of logistics and health issues being a local. Lt Col Asthana's narration on the Kargil War where he was the officiating CO and 2IC of 2/11 GR is informative, sharing his experiences and lessons learnt. Poor planning and preparation are to be seen of cross attaching Battalions, Companies and even up to Platoons! The Indian Army has failed to give due importance to the Kohima and Imphal battles of the WWII whereas the British Army considers these two battles as the most important

battles fought post 18th century. Battles fought in Europe unfairly stole the limelight.

In High Altitude Mountain Warfare, nature often proves to be a deadlier adversary than the enemy itself. The extreme cold, unpredictable weather, avalanches, and treacherous terrain take a heavier toll on soldiers than the bullets or shells. Thin air and low oxygen levels cause fatigue, altitude sickness, and reduced combat efficiency, while isolation and logistical challenges make survival and evacuation even harder. In such conditions, it is not the clash of arms but the relentless hostility of the environment that claims the greatest number of lives. The 1971 war, in the Kargil sector, and the Partapur sub-sector, prove the reality that nature is a deadlier adversary while fighting in mountains especially in winters.

In this modern High Altitude Mountain Warfare, specific to India, in the future will have multi-domains, so we need to leverage with the emerging technologies and keep innovating and counter innovating. A whole of nation approach is required to protect our Himalayan territorial integrity and critical assets and unleash punitive action on the adversary, if the situation so demands, through the modern High-Altitude Warfare.

The book's main limitation is its uneven distribution of coverage. High-altitude warfare only gains sustained, chapter-length treatment from Chapter 4 onwards; readers seeking an exhaustive operational manual might find earlier chapters more of historical narratives in the words of soldiers who fought those battles or of some earlier authors mostly well known to the students of military history. The treatment of historical lineage could also have been richer for instance, a fuller acknowledgment of the pioneering Himalayan campaigning of General Zorawar Singh and its doctrinal implications would have strengthened the Mountain Warfare connect between past and present. Wish the soul of Himalayan soldiering, General Zorawar Singh, a Dogra General who

led his Dogra warriors in peak winters of December 1841 across the frozen passes into Tibet, reaching as far as the sacred shores of Kailash–Manasarovar, had been given the due credit for laying the foundation for India's modern understanding of mountain warfare where geography, logistics, and endurance determine victory more than the strength of numbers. Finally, the critique of policy decisions for example of Agniveer recruitment is bold but could have been more analytically supported and contested.

For policymakers and officers' recommendations are to invest in specialised mountain logistics and medical evacuation capabilities; prioritise acclimatisation and local recruitment where appropriate; codify mountain-specific doctrine and synchronise multi-domain assets like drones, cyber with AI with the immutable constraints of altitude and terrain. For the national security community, he argues persuasively for a "whole-of-nation" posture that integrates civilian infrastructure and indigenous innovation into a resilient offensive capable posture. Hope few Bhairav Battalions or call them Hanuman or Himalayan Battalions are suitably organised to fulfil the role to carry out limited offensives operations if need arises.

The book is an offering from someone who has walked the ridgelines. He believes that even in the age of drones and of the precision guided munitions (PGMs) the spirit of the Himalayan soldier will remain our truest defence. Our future mountain warfare must be yet tougher and adapt to the emerging technologies as India cannot afford to lose any pass or peak of our sacred Himalayas—the crown of Bharat Mata.

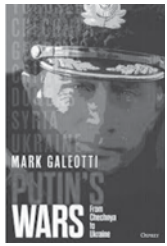
The coming battles, if they are to be fought, will require a new kind of warrior: one who can combine the intuition of the climber with the precision of the coder, the endurance of the soldier with the imagination of the innovator. It reminds us that even as we field drones, long-range precision systems, the Himalaya will test human resolve, endurance and improvisation. Serving officers and students of military history and those

concerned about India's Himalayan defence are advised to read this book—'Mountain Warfare: Operational Imperatives for India'.

"The Himalayas will test our every future generation, and they have to prove themselves worthy to hold them—The only Himalayas which India cannot afford to lose".

Jai Hind - Jai Bharat

Putin's Wars: From Chechnya to Ukraine
By Mark Galeotti



Publisher: Osprey Publishing (2022), Price 699/-,
Paperback, pp. 320, ISBN: 9781472847553

Review by Anusua Ganguly

Mark Galeotti's *Putin's Wars: From Chechnya to Ukraine* offers a compelling and detailed account on how Putin's Russia has consistently employed special operations units, military force and state security agencies like the Federal Security Service (FSB) to maintain the nations position in global affairs. An internationally acclaimed expert on Russian security affairs, and recipient of the Fletcher School's best book award on US – Russian relations for this scholarly account, Galeotti argues that Putin's military engagements are not isolated episodes but parts of a coherent strategic pattern. By placing events in chronology, Mark traces Russia's transformation from the military chaos and institutional crisis of the 1990s to the outbreak of Ukraine conflict in 2022. This approach makes the book essential not only for understanding Russia's recent wars but also for grasping debates around hybrid conflict and the future of European security.

The book is divided into five parts, that present these events in chronology and are thematically layered, serving as a lens into the Kremlin's political system, military reforms and strategic culture. Illustrating the border disputes, communal violence and economic

Anusua Ganguly is Research Assistant at the Centre for Land Warfare Studies (CLAWS), New Delhi and focuses on Russia and Central Asia. Views expressed are personal.

freefall that was faced by Post-Soviet Eurasia, Part One of the book discusses the chaos and crisis on the 1990s, and the legacy of state collapse. Part Two, focuses on the transition of power from Yeltsin to Putin, and the latter's rise and militarised statecraft. As the author indicates war to be a tool to rebuild the state, project power, and create a national myth, Part Three, highlights how Putin's Wars from Chechnya to Ukraine become a defining feature of Putin's tenure. Part Four, focuses on the details of Russian military modernisation. At the end, Part Five, discusses the new forms of warfare being employed by Moscow during various conflicts.

Historical and Conceptual Foundations

In the initial chapters of the book, Galeotti establishes the longue durée trajectory of the Russian warfare, tracing how successive conflicts dating back from the Mongol invasions to the Second World War, have produced a national mythology in which unity ensures survival and disunity will result in catastrophe. This historical grounding illuminates the post-Soviet military collapse of the 1990s, marked by institutional weakness, corruption and the violent dysfunction of dedovshchina (or 'grandfatherism'). Thus, in Mark's account, the First Chechen War (1994–1996) emerges as a symbol of Russia's degraded military capacity and the erosion of state cohesion.

Within this setting, Galeotti presents Putin as the figure who is determined to reverse this decline and rebuild the armed forces. The Second Chechen War (1999–2009) hence becomes the testbed through which the new Russian leader consolidates his authority. The conflict's brutality combined with Putin's resolute posture, allowed him to project an image of decisive leadership and restore the state's domestic legitimacy. For Galeotti, this period forms the basis of Putin's conviction that force, even when used ruthlessly, can reassert Russia's regional dominance and deter external interference. In all, while as Putin seemed offended when

the West questioned his methods, he also believed that the West's lack of will, would be Russia's strategic advantage.

Military Reform and Operational Transformation

The intermediate chapters of the book provide an in-depth analysis of the transformation of the Russian military following the Russo-Georgian War of 2008. Although, Russia prevailed quickly, the "underwhelming performance of the military" exposed serious deficiencies in logistics, planning and interoperability. These significant shortcomings enabled Defence Minister Anatoly Serdyukov to implement the most radical reforms, aimed at professionalisation and structural rationalisation, which were subsequently institutionalised under Sergei Shoigu. The creation of the "New Look Army," Galeotti argues, allowed Russia to wage the types of limited, high-tempo, and hybrid operations that became characteristic of the following decade.

Three campaigns exemplify this evolution:

- **Crimea (2014):** Executed with a high degree of operational precision, the annexation of the Crimean Peninsula relied on deniable Special Forces ("little green men"), informational control, and coercive diplomacy. Set against this scenario, the Kremlin gained a massive popularity boost, so much so that Putin's personal approval ratings, Galeotti suggests, "went up from 60 per cent to over 80 per cent."
- **Donbas (2014-continuing):** On this part of the border, what began as a fragmented secessionist movement soon evolved into a theatre for experimentation with Battalion Tactical Groups (BTGs) and long-range fires. Moscow's interventions, particularly the "Northern Wind" operation, prevented Kiev's victory and entrenched a frozen conflict that served the political aims of the former.
- **Syria (2015-continuing):** The Syrian intervention provided a controlled environment in which Russia tested new weapons

and refined command-and-control systems, notably through the National Defence Management Centre (NTsUO: *Natsionalny Tsentr Upravleniya Oboronoi*). Additionally, it secured Moscow a central diplomatic role in Middle Eastern geopolitics and demonstrated its ability to project power beyond the post-Soviet space.

Political Warfare, Hybrid Means, and the Role of Non-State Proxies

A critical contribution of *Putin's Wars* lies in its conceptualisation of Russian "political warfare". Galeotti defines this as the use of all national instruments short of overt war, which includes disinformation, cyberattacks, economic coercion and covert political manipulation with an aim to achieve strategic ends. This approach reflects the Kremlin's structural insecurities and its belief that the West seeks to marginalise it. For Galeotti, the hybrid toolkit is not ancillary but central to Russia's strategy, enabling Moscow to blur the boundaries of conflict and exploit democratic vulnerabilities.

Private military companies, such as the Wagner Group, feature prominently in Galeotti's analysis. The Group's use has offered the Kremlin plausible deniability while avoiding the domestic political costs associated with military casualties ("Cargo 200s"). However, Galeotti points out the tensions between regular forces and Wagner's non-state proxy operatives, bringing to fore incidents such as the 2018 Khasham battle, which revealed both the potential and the perils of semi-deniable warfare.

The 2022 Ukraine Conflict: Structural Failures and Strategic Miscalculation

With the conception of Putin's Wars coinciding with the beginning of the ongoing Russia–Ukraine war in 2022, in the concluding section Galeotti addresses "Russia's full-scale invasion of Ukraine". Russia's anticipation

that there will be a rapid collapse of Ukrainian resistance and a minimal response from the West, he states, were miscalculations rooted in authoritarian information asymmetries and strategic hubris. According to this analysis, the Ukrainian conflict exposed structural challenges within the Russian military system, including the effects of centralised decision-making, logistical and organisational strains and entrenched bureaucratic practices.

While the war between Russia and Ukraine has evolved beyond the book's publication, Galeotti's framework remains strikingly prescient. Ukrainian military official, Colonel Mykyta Zhuiko, affirms in his review of the book the accuracy of Galeotti's assessment of Russian logistical problem. The book's discussion of Russia's difficulty in establishing air superiority, the significant attrition among certain elite units, and incidents such as the loss of the *Moskva* further seem to have highlighted the operational challenges the Russian military encountered during the campaign.

Evaluation and Limitations

As a true historian would write, Galeotti's *Putin's Wars* is distinguished by its clarity, analytical depth, and accessibility. He weaves together historical narrative, institutional analysis, and strategic theory in a manner that will appeal to both specialists and general readers. His approach towards the decision-making dynamics and hybrid warfare practices offers a particularly valuable framework for understanding the Russian state's behaviour in its post-Soviet neighbourhood.

However, the book does have certain minor limitations. The coverage of earlier conflicts, especially the later stages of the Second Chechen War seem comparatively brief, creating an imbalance relative to the detailed treatment of post-2014 events. Furthermore, while the granular discussion of unit structures and security agencies are very informative for

military experts and specialist, at times it may appear overly technical to the non-expert readers.

Conclusion

Despite its minor limitations, *Putin's Wars* serves as an essential contribution to the study of contemporary Russian strategy and warfare. Galeotti's theory that all nations are, to some extent, shaped by wars, and more so in the case of Russia, located at the crossroads of Europe and Asia, with no natural borders, turns out to be true. He suggests that Russia's public rhetoric is often performative and that its practices are embedded in long-standing political logics that hold significant implications for policymakers and scholars alike. The book convincingly argues that Putin's attempt to forge a "Eurasian Sparta" has instead precipitated a strategic overreach reminiscent of Tsar Nicholas II, leaving the Russian state and society with enduring and profound costs.

Galeotti's work thus provides not only a detailed history of Putin's military ventures but also a sobering reflection on the dangers of personalised authoritarian decision-making. Therefore, even though parts of the book might be exhaustive to non-expert readers, *Putin's Wars* is indispensable reading for scholars of international security, military affairs, and Russian politics.

Notes for Contributors

General

The CLAWS Journal welcomes professional articles on warfare and conflict, national security and strategic issues, especially those related to the art and science of land warfare including sub-conventional conflict in the Indian context. Articles may be submitted by serving and retired members of the armed forces as well as civilians in India and abroad. Articles on aerospace and maritime issues and those on foreign policy and international relations having a bearing on land warfare are also welcome. The Journal particularly encourages articles from younger members of the armed forces.

Manuscripts: Contributors should submit their manuscripts (main articles, commentaries, review articles and book reviews) by e-mail, with one hard copy being sent separately by post. All material must be original, unpublished and should not have been submitted for publication elsewhere. Main articles must have a length of 3,000 to 6,000 words. Commentaries and review articles must not exceed 1,500 to 2000 words.

Book Reviews: Book reviews must contain the name of the author, the title of the book reviewed, particulars of the publisher, place and date of publication, number of pages and price. Authors who wish to have their book considered for review should ask their publisher to send a copy to the Editor, CLAWS Journal.

Submission: Since manuscripts will be sent out anonymously for peer review, the authors should omit their identity from the manuscript. The author's name, rank, unit/institutional affiliation, e-mail ID, postal address and telephone number should be submitted on a separate cover page. Each article must be accompanied by an abstract of about 250 to 300 words. A four to five line (or 75 words) biographical note describing the author should accompany the manuscript. Manuscripts should be typed in double space, including endnotes and references, with 1.5 inch (3.0 cm) margins, on one side of A4 size paper.

Acceptance and Revision: Intimation regarding suitability of the article for publication will be given within 30 days of its receipt in normal cases. Articles not accepted for publication will not be returned. The Editorial team reserves the right to edit articles for better clarity and to ensure that the style conforms to the style of the CLAWS Journal. However, views expressed by an author will not be altered. Authors should be prepared to revise their manuscript based on the suggestions made by the reviewers and the editorial team.

Honorarium: A suitable honorarium will be paid for articles accepted for publication. The CLAWS Journal may also commission articles from time to time.

Mandatory Certificates

- Retired armed forces officers and civilian authors should submit a certificate of originality, clearly stating that the article is original and unpublished and has not been submitted for consideration elsewhere.
- Serving members of the armed forces must submit the necessary clearance certificates in terms of the relevant rules and regulations pertaining to their respective Services.
- Serving army officers must submit three certificates.
  - ❖ First, a certificate of originality, clearly stating that the article is original and unpublished and has not been submitted for consideration elsewhere.
  - ❖ Second, a certificate from the author stating that s/he has not used any official information or material obtained in an official capacity while writing the article submitted.
  - ❖ Third, a certificate from her/his Superior Officer stating that there is no objection to the publication of the article.
  - ❖ The format of the latter two certificates is given in Para 21 (a) and (b) of SAO 3/S/2001/MI.
- Responsibility for obtaining Army HQ DGMI (MI-11) clearance in respect of articles pertaining to subjects specified in Paras 13 and 14 of SAO 3/S/2001/MI, will be that of the officer herself/himself.

Style of the Journal

Clarity: Articles should be written in a clear and lucid style. Sentences should be kept short. The use of too many adjectives should be avoided. The most complex ideas can be expressed in simple language. Paragraphs should also be short.

Use of Pronouns: Articles should be written in third person. Writing in first person should be avoided completely—unless the author is over 65 years old!

Spelling: Use British, not American spellings. Thus, use "humour," not "humor," and "programme," not "program." Where alternative forms exist, choose "-ise" instead of "-ize" or "-isation" instead of "-ization" spellings. Thus, use "modernise," "stabilise", "modernisation," "stabilisation," etc.

Quotations: Quotations must be placed in double quotation marks, reserving single quotation marks for a quote within a quote. Long quotes (i.e., four lines or more) should be indented, without quote marks, to set them apart from the text.

Abbreviations:
- All abbreviations must be given in full at their first use in the text; for example, Comprehensive Test Ban Treaty (CTBT).
- Abbreviations should include a final stop in words shortened by omitting the end (such as p., ed., vol.) but not in contractions (words such as Mr, Dr, edn, eds) or between capitals, e.g., USA, SAARC, UN.
- Avoid using "i.e." and "e.g." in the text but use them in the notes if you wish.
- Do not use military abbreviations such as "ops", "int" and "adm" as the CLAWS Journal will have a civilian as well as an international readership. However, those such as CI (counter-insurgency), IS (internal security) and CPMFs (central police and para-military forces) may be used after being given in full at their first use.
- Abbreviated military ranks may be used; e.g., Lt Col, RAdm and Wg Cdr.

Headings and Parts: The only centre heading should be the title of the article. Refrain from dividing an article into several parts. Avoid too many headings, as is the norm in Service writing. While group headings are the norm (bold but not underlined), paragraph headings are best avoided.

Sub-paragraphs and sub-sub-paragraphs:
- Avoid writing in sub-paragraphs unless it is inescapable—e.g. a list needs to be provided.
- Even then, write in complete sentences and not in point form under sub-paragraphs.
- Do not write in sub-sub-paragraphs under any circumstances.

Highlighting Words: Use capitals, bold and italics sparingly but consistently. Italics should be used for titles of books, newspapers, journals and magazines as well as for foreign words not in common usage.

Numbers: Numbers from one to nine should be spelt out, 10 and above will remain in figures; hence, "seven" not "7" and "17" not "seventeen". However, figures should be used for exact measurements (such as "5 per cent," "5 km" and "5-year-old child"). Use "thousand" and "million," not "crore" and "lakh" as the Journal will have international readers. Use fuller forms for inclusive numbers in the case of dates and page numbers (such as "1971-72" and pp. "260-65"). In the text use "per cent", in tables the symbol " per cent."

Figures and Tables: Figures and Tables should be presented on separate sheets of paper and collected at the end of the article while mentioning the location in the article. Figures and Tables must be numbered in separate sequences, i.e., "Fig. 1" and "Table 1" and the titles should be short and crisp. Copyright permission for reproducing figures or photographs that have been cited from other works must be obtained.

Endnotes and References: Endnotes and References should be amalgamated and marked serially in the text of the article by superscript 1, 2, 3, etc.

Referencing Style: References should be typed in the form of the following example on first appearance:

(a) **Books:**
Michael Foucault, *The Archaeology of Knowledge* (London: Routledge, 1989), p. 26.

(b) **Edited Volume:**
James Der Derian (ed), *International Theory: Critical Investigations* (New York: New York University Press, 1995).

(c) **Articles in Journals:**
Samina Yasmeen, "Pakistan's Kashmir Policy: Voices of Moderation?," *Contemporary South Asia*, Vol. 12, No. 2, June 2003, pp. 187-202. In case of two journals having a similar title, the place of publication must be mentioned, e.g., International Affairs (London) and International Affairs (Moscow).

(d) **Articles in Edited Volumes:**
Tom Nairn, "The Curse of Rurality: Limits of Modernisation Theory" in John A. Hall (ed), *The State of the Nation: Ernest Gellner and the Theory of Nationalism* (Cambridge: Cambridge University Press, 1998), pp. 107-34

(e) Articles in Newsmagazines: Gurmeet Kanwal, "Pakistan: On the Brink," *The Week*, November 4, 2007, p. 45.

(f) Articles from Newspapers: M. K. Bhadrakumar, "New Regionalism in Central Asia," *The Hindu*, July 14, 2004.

(g) References to Websites: United Nations Development Programme, "Arab Human Development Report 2003", http://www.undp.org/rbas/ ahdr/english2003.html, accessed on October 27, 2007.

(h) Reports and Documents:
- United Nations, UNCED, The Global Partnership for Environment and Development (New York: United Nations, 1992).
- Canberra Commission, Report on the Elimination of Nuclear Weapons (Canberra: Commonwealth of Australia, 1996). Available on the Internet at <http://www.dfat.gov.au/cc/cchome.html>

(i) Conference Papers:
Michael Williams, "The Discursive Power of Community: Consideration on the European 'Security Community'", Draft Paper presented at the conference on Power, Security and Community: IR Theory and the Politics of EU Enlargement, Copenhagen October 9-12, 1997.

(j) Unpublished Theses and Dissertations:
Christopher Strawn, "Falling of the Mountain: A Political History and Analysis of Bhutan, the Bhutanese Refugees and the Movement in Exile", Dissertation submitted to the University of Wisconsin, USA, 1993, Chap. 4.

On subsequent reference (unless immediately following the first reference, in which case Ibid. will be used) please use n. with the number of the note given earlier e.g. n.1, n.2.

Five offprints of each article will be provided to the author and in case of more than one author, to the senior author. A complimentary copy of the printed journal will be provided to each author.

Mailing Address: All manuscripts should be addressed to:

The Editor
CLAWS Journal
Centre for Land Warfare Studies
RPSO Complex, Parade Road
New Delhi 110010, India
Email: clawsjournal@gmail.com
Website: www.claws.co.in

CLAWS JOURNAL

Journal of the Centre for Land Warfare Studies

CLAWS JOURNAL

Journal of the Centre for Land Warfare Studies

CLAWS JOURNAL

SUBSCRIPTION RATES

IN INDIA	SAARC COUNTRIES	OTHER COUNTRIES
☐ Rs. 500 /- per copy	☐ US $ 15 per copy	☐ US $ 20 per copy

☐ Rs. 1000 /- Annual Subscription (2 issues)

Please Print

Name .....
Complete Address .....
..... Pin .....Phone .....
Please find enclosed cheque/draft number .....dated .....
drawn on .....Favouring Centre for Land Warfare Studies
for Rs./US$ .....

Please mail this form to: Centre for Land Warfare Studies (CLAWS),
RPSO Complex, Parade Road, Delhi Cantt, New Delhi—110010
Tel: +91-11-25691308 • Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com

Note: Kindly add Rs. 200/- (per Edition) as postage charge

CLAWS JOURNAL

SUBSCRIPTION RATES

IN INDIA	SAARC COUNTRIES	OTHER COUNTRIES
☐ Rs. 500 /- per copy	☐ US $ 15 per copy	☐ US $ 20 per copy

☐ Rs. 1000 /- Annual Subscription (2 issues)

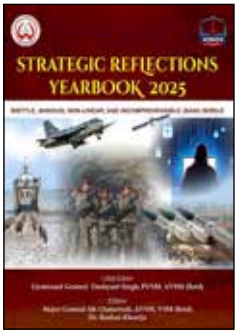
Please Print

Name .....
Complete Address .....
..... Pin .....Phone .....
Please find enclosed cheque/draft number .....dated .....
drawn on .....Favouring Centre for Land Warfare Studies
for Rs./US$ .....

Please mail this form to: Centre for Land Warfare Studies (CLAWS),
RPSO Complex, Parade Road, Delhi Cantt, New Delhi—110010
Tel: +91-11-25691308 • Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com

Note: Kindly add Rs. 200/- (per Edition) as postage charge.

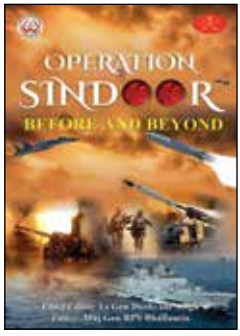
RECENT CLAWS BOOKS



Strategic Reflections Yearbook 2025: Brittle, Anxious, Non-Linear, and Incomprehensible (BANI) World

Edts: Lt Gen Dushyant Singh, Maj Gen AK Chaturvedi & Dr Roshan Khanijo

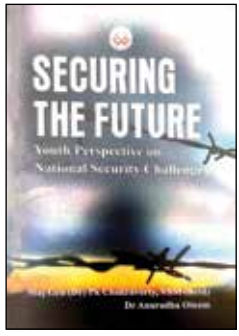
INR 2,599/- (HB)



Operation Sindoor: Before and Beyond

Edts: Lt Gen Dushyant Singh & Maj Gen RPS Bhadauria

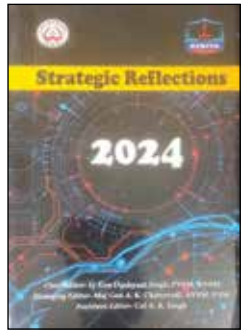
INR 1,199/- (PB)



Securing the Future Youth Perspective on National Security Challenges

Maj Gen (Dr) PK Chakravorty & Dr Anuradha Oinam (Edts)

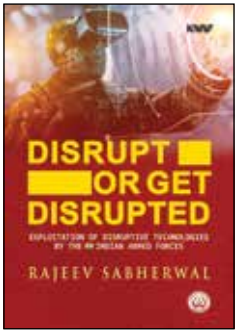
INR 695/- (PB)



Strategic Reflections 2024

Lt Gen Dushyant Singh, Maj Gen AK Chaturvedi & Col AK Singh (Edts)

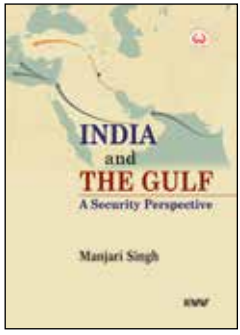
INR 1,495/- (HB)



Disrupt or Get Disrupted Exploitation of Disruptive Technologies by the Indian Armed Forces

Rajeev Sabherwal

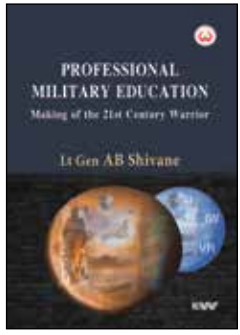
₹ 2580/- (HB)



India and the Gulf A Security Perspective

Manjari Singh

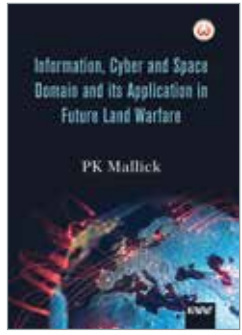
₹ 1880/- (HB)



Professional Military Education Making of the 21st Century Warrior

Lt Gen AB Shivane

₹ 1680/- (HB)



Information, Cyber and Space Domain and its Application in Future Land Warfare

PK Mallick

₹ 1580/- (HB)

The Chanakya Defence Dialogue 2025 Curtain Raiser opened with a wide-ranging fireside chat featuring General Upendra Dwivedi in conversation with Ms Sweta Singh, setting the strategic tone for the Dialogue. Speaking in Hindi to reach a broader audience, the Chief outlined how the Army's reform agenda aligns with the theme "Reform to Transform – Sashakt, Surakshit aur Viksit Bharat" and the larger vision of Viksit Bharat 2047. He framed the transition from the "Year of Transformation" to the "Year of Reform" as part of a longer decade-long roadmap, culminating in a data-centric, AI-enabled force.

Drawing on the lessons of Operation Sindoor, the Chief underscored India's clear deterrence posture, anchored in political will, military capability and the adversary's belief that India will act. He highlighted the changing character of war—compressed, multi-domain and technology-intensive—requiring agility, integration and rapid decision-making. The conversation reinforced that a reforming, modernising and confident Indian Army remains central to national security and development.

The transition from the "Year of Transformation" to the "Year of Reform" is part of a longer decade-long roadmap, culminating in a data-centric, AI-enabled force.
