The Journal of the United Service Institution of India JULY-SEPTEMBER 2026 USI

U.S.I. JOURNAL

INDIA'S OLDEST JOURNAL ON DEFENCE AFFAIRS



(Estd. 1870)

PRINCIPAL CONTENTS

Symbol, Status and Statecraft: Reassessing Rank Convergence in India's Uniformed Services	Lieutenant General Rajeev Chaudhry, VSM (Retd)
Algorithmic Doctrinal Reinforcement: Mitigating Strategic Blindness in Artificial Intelligence-Enabled Warfare	Commander V Srivatsan
Preparing for Future Conflicts: Emerging Lessons for India from the Russia–Ukraine and US–Israel–Iran Conflicts	Colonel Ajay Kumar Tomar
Fluid Frontiers: Mapping the Geopolitical Fault Lines of Fragmenting World Order	Dr Kawal Deep Kour

Vol CLVI JULY-SEPTEMBER 2026 No 645

ALL RIGHTS RESERVED © Rs. 300.00 PUBLISHED QUARTERLY

USI Latest Publications 2025 to 2026

Pub Code	Type	Title of Publication and Author	Price ₹	Year
SYB/2026	Year Book	STRATEGIC YEAR BOOK 2026; edited by Major General Sanjeev Chowdhry (Retd), Komal Chaudhary, Vinayak Sharma, Richa Sharma **M/s Sabre & Quill Publishers**	2199	2026
B-10/2026	Book	CASUALTIES IN WAR – MODELS, SURPRISE AND UNCERTAINTY by Colonel Narinder Jarial (Retd) **M/s Sabre & Quill Publishers**	999	2026
B-9/2026	Book	REIMAGINING INDIA'S STRATEGIC CULTURE IN THE EMERGING WORLD ORDER by Colonel Sachin Shankar Mahadik **M/s Pentagon Press**	995	2026
B-8/2026	Book	BRIDGING CULTURES: NORTH EAST INDIA ROLE IN FURTHERING INDIA'S ACT EAST POLICY by Lieutenant General Shokin Chauhan, PVSM, AVSM, YSM, SM, VSM, PhD (Retd) **M/s Pentagon Press**	1295	2026
B-7/2026	Book	INFORMATION WARFARE LEVERAGING CYBERSPACE AND MEDIA : AN IMPERATIVE DURING COMPETITION CONTESTATION, CONFRONTATION AND CONFLICT by Colonel Amit Kumar Sharma **M/s Pentagon Press**	1495	2026
B-6/2026	Book	WAR IS A TRUE CHAMELEON: STRATEGISING FOR FUTURE WARS IN INDIAN CONTEXT by Lieutenant General Rakesh Sharma, PVSM, UYSM, VSM, PhD (Retd) **M/s Sabre & Quill Publishers**	999	2026
B-5/2026	Book	WINGS OF SUPPORT: NINE DECADES OF ACTION BY TRANSPORT FLEET OF IAF by Air Marshal Rajiv Sachdeva, AVSM, PhD (Retd) **M/s Sabre & Quill Publishers**	2499	2026
B-4/2026	Book	CRACKS IN THE CRESCENT: AN APPRAISAL OF PAKISTAN'S ENDURING FAULTLINES by Colonel Suraj Chambial, SM **M/s Pentagon Press**	995	2026
B-3/2026	Book	THE ALGORITHM OF WAR CODE COMPUTE CONQUER: INSIGHT FOR INDIAN ARMY'S NEXT LEAP by Colonel Maneesh Parthsarthy, VSM **M/s Pentagon Press**	1495	2026
B-2/2026	Book	DUAL – USE INFRASTRUCTURE IN INDIA: CIVIL-MILITARY FUSION FOR STRATEGIC INFRASTRUCTURE DEVELOPMENT by Colonel Vijay Goyat **M/s Sabre & Quill Publishers**	999	2026
B-1/2026	Book	ARTHASHASTRA FOR THE AI AGE: A CHANAKYAN BLUEPRINT FOR INDIA'S TECHNOLOGICAL SOVEREIGNTY by Commander V Srivatsan **M/s Sabre & Quill Publishers**	999	2026
P-1/2026	Paper	WHITE PAPER ON MODEL-BASED ACQUISITION: INTEGRATION OF DIGITAL ENGINEERING IN DEFENCE ACQUISITION PROCEDURE by Major General Pawan Anand, AVSM, PhD (Retd), Major General Abhay Dayal, AVSM, VSM, PhD (Retd), Brigadier Vivek Verma, PhD (Retd), Group Captain Pranay Dixit, VM (Retd)	-	2026
M-6/2026	Monograph	CUTTING LOSSES IS ALSO A SMART STRATEGY IN MODERN STATECRAFT: THE UKRAINE EXPERIENCE by Lieutenant General DP Pandey, PVSM, UYSM, AVSM, VSM (Retd) **USI of India**	350	2026
M-5/2026	Monograph	CERTIFICATION OF ARTIFICIAL INTELLIGENCE IN AVIATION: GLOBAL APPROACHES, CHALLENGES, AND ROADMAP FOR INDIA WITH FOCUS ON THE INDIAN AVIATION by Air Commodre Mukhvinder Pal Singh Virk and Sumedh Singh Virk **USI of India**	350	2026
M-4/2026	Monograph	FROM COMBAT SUPPORT TO COMBAT ARM: A STRATEGIC REAPPRAISAL OF THE CORPS OF SIGNALS by Lieutenant General SRR Aiyengar, PVSM, AVSM, VSM (Retd) **USI of India**	350	2026
M-3/2026	Monograph	COGNITIVE WARFARE BY CHINA AND INDIA'S RESPONSE by Major General BK Sharma, AVSM, SM** (Retd) and Major General Sanjeev Chowdhry (Retd) **USI of India**	350	2026
M-2/2026	Monograph	SPACE RESOURCES: THE ARTEMIS ACCORDS, INTERNATIONAL LUNAR RESEARCH STATION, AND OPTIONS FOR INDIA by Air Marshal R Radhish, PVSM, AVSM, VM (Retd) **USI of India**	350	2026
M-1/2026	Monograph	USI ANNUAL UN FORUM 2025: ADVANCING PEACEKEEPING AND HUMANITARIAN IMPERATIVE IN A FRAGMENTED WORLD edited by Major General PK Goswami, VSM (Retd), Major General AK Bardalai, VSM, PhD (Retd) and Colonel KK Sharma, PhD (Retd) **USI of India**	350	2026
OP-10/2026	Occasional Paper	THE INVISIBLE BATTLEFIELD: ELECTROMAGNETIC SPECTRUM MANAGEMENT by Lieutenant General Madhavan Unni krishnan Nair, PVSM, AVSM, SM (Retd) **USI of India**	250	2026
OP-9/2026	Occasional Paper	THE GRAMMAR OF RESTRAINT by Lieutenant General AB Shivane, PVSM, AVSM, VSM (Retd) **USI of India**	250	2026
OP-8/2026	Occasional Paper	UNMANNED SURFACE VESSELS IN CONTEMPORARY MARITIME CONFLICT by Lieutenant General Karanbir Singh Brar, PVSM, AVSM (Retd), Priyanshu Joshi **USI of India**	250	2026
OP-7/2026	Occasional Paper	SOCIAL MEDIA IN THE MILITARY CONFLICTS: EMERGING TRENDS AND LESSONS by Colonel Satish Kumar Sinha, Colonel Subodh Shahi, PhD (Retd) **USI of India**	250	2026
OP-6/2026	Occasional Paper	AN APPRECIATION JOINT AIR CAMPAIGNS EPIC FURY AND ROARING LION-AND THEIR LESSONS FOR INDIA by Air Vice Marshal Prashant Mohan, VM (Retd) **USI of India**	250	2026
OP-5/2026	Occasional Paper	ARTIFICIAL INTELLIGENCE, LARGE LANGUAGE MODELS, AND THE TRANSFORMATION OF MILITARY OPEN SOURCE INTELLIGENCE by Major General PK Mallick, VSM (Retd) **USI of India**	250	2026
OP-4/2026	Occasional Paper	CONTESTING THE COGNITIVE-CYBER-KINETIC KILL CHIAN by Lieutenant Colonel Nishank Sharma, Dr Surya Prakash, Dr Hemprasad Patil **USI of India**	250	2026
OP-3/2026	Occasional Paper	CONFIDENCE-BUILDING MEASURES FOR RESPONSIBLE AI IN THE MILITARY by Major General Pawan Anand, AVSM, PhD (Retd), Colonel Ashish Nagaich, SM **USI of India**	250	2026
OP-2/2026	Occasional Paper	THE ESTABLISHMENT OF PAX SINICA by Vinayak Sharma, Komal Chaudhary **USI of India**	250	2026
OP-1/2026	Occasional Paper	A COMPREHENSIVE EVALUATION OF EFFECTIVENESS AND LIMITATIONS OF SANCTIONS AS A TOOL OF COUNTER TERRORISM by Srinivas Rao Cheruku, Major General Pawan Anand, AVSM, PhD (Retd) **USI of India**	250	2026

ISSN 004-77OX Volume CLVI July-September 2026 No 645

U.S.I. JOURNAL



(Estd. 1870)

Published by Authority of the Council

Postal Address
Rao Tula Ram Marg (opposite Signals Enclave)
Post Bag No. 8,
Vasant Vihar PO, New Delhi-110057

Telephone Nos and Mail IDs
IVRS: 87006-92369

Exchange:	+91-11-2086-2314/+91-11-2086-2320/ +91-11-2086-2321
Director General:	+91-11-2086-2322 dg@usiofindia.org
Director Administration:	+91-11-2086-2316 diradm@usiofindia.org
USI Membership:	membership@usiofindia.org
Venue Bookings:	booking@usiofindia.org
Centre for Strategic Studies and Simulation (CS3):	+91-11-2086-2326 dircs3@usiofindia.org
Centre for Military History Conflict Studies (CMHCS):	+91-11-2086-2327 dircmhcs@usiofindia.org
Director Centre for United Nations and Humanitarian Studies (CUNHS):	+91-11-2086-2315 dircunhs@usiofindia.org
Centre for Emerging Technologies for Atma Nirbhar Bharat (CETANB):	+91-11-2086-2321 dircetanb@usiofindia.org
Centre for Professional Military Education (CPME):	+91-11-20862325, +91-11-2086-2318 dircpme@usiofindia.org
Centre for Publications: and Library (CP&L)	+91-11-2086-2315 dircpl@usiofindia.org
Library:	library@usiofindia.org
Fax:	+91-11-2086-2324
Website:	usiofindia.org

The USI Journal is a peer-reviewed publication, published quarterly in Apr, Jul, Oct, and Jan. Subscription per annum w.e.f. 01 Jan 2016: In India ₹ 1,100.00. Postage extra (by Speed Post: ₹ 320/- for four issues). Subscription should be sent through Bank Draft/Local/Multicity Cheque in favour of Director General, United Service Institution of India. Articles, correspondence, and books for review should be sent to the Director, Centre for Publications and Library. Advertisement enquiries should be addressed to the Director Administration. Overseas annual subscription (By Air Mail) - £50 or US $80

United Service Institution of India

For

the furtherance of interest and knowledge in the art, science, and literature of national security in general and of the defence services in particular

Appointment	Name	*Designation*
Vice Patrons	General Dhiraj Seth, PVSM, UYSM, AVSM	*Chief of the Army Staff*
	Admiral Krishna Swaminathan, PVSM, AVSM, VSM	*Chief of the Naval Staff*
	Air Chief Marshal Amar Preet Singh, PVSM, AVSM	*Chief of the Air Staff*
Council		
President	Air Marshal Tejinder Singh, PVSM, AVSM, VM	*Chief of Integrated Defence Staff to the Chairman, Chiefs of Staff Committee*
Vice Presidents	Lieutenant General Sandeep Jain, AVSM, SM,	*Vice Chief of the Army Staff*
	Vice Admiral Ajay Kochhar, PVSM, AVSM, NM	*Vice Chief of the Naval Staff*
	Air Marshal Ashutosh Dixit, PVSM, AVSM, VM, VSM	*Vice Chief of the Air Staff*
Ex-Officio Members	Shri Rajesh Kumar Singh, IAS	*Defence Secretary*
	Vice Admiral Rajesh Dhankhar, AVSM, NM	*Deputy Chief of the Integrated Defence Staff (Doctrine, Organisation, and Training)*
	Lieutenant General Sukriti Singh Dahiya, SM, VSM	*Chief of Staff, Army Training Command*
	Commodore Saket Khanna, VSM	*Commodore (Naval Training)*
	Air Vice Marshal Sanjay Aswal, VM	*Assistant Chief of the Air Staff Operations (Strategy)*
Elected Members	Lieutenant General Vinod Bhatia, PVSM, AVSM, SM (Retd)	
	Major General Ian Cardozo, AVSM, SM (Retd)	
	Lieutenant General Satish Kumar Dua, PVSM, UYSM, SM, VSM (Retd)@	
	Lieutenant General Devendra Pratap Pandey, PVSM, UYSM, AVSM, VSM (Retd)@	
	Lieutenant General Arun Kumar Sahni, PVSM, UYSM, SM, VSM (Retd)@	
	Lieutenant General Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)	
	Lieutenant General Raj Shukla, PVSM, YSM, SM (Retd)	
	Lieutenant General Ajai Singh, PVSM, AVSM (Retd)@	
	Vice Admiral Sanjay Mahindru, PVSM, AVSM, NM (Retd)@	
	Vice Admiral Ajendra Bahadur Singh, PVSM, AVSM, VSM (Retd)	
	Air Marshal Rajesh Kumar, PVSM, AVSM, VM (Retd)@	
	Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd)@	
	Smt Smita Purushottam, IFS (Retd)	
	Shri Sanjay Singh, IFS (Retd)@	
Co-opted Members	Vacant	*Additional Secretary, Department of Military Affairs*
	Ms Soumya C, IFS	*Joint Secretary, Policy, Planning, and Research, Ministry of External Affairs*
	Major General BK Sharma, AVSM, SM** (Retd)@	*Former DG USI*
Executive Committee	Chairman Vice Admiral Rajesh Dhankhar, AVSM, NM	*Deputy Chief of the Integrated Defence Staff (Doctrine, Organisation & Training)*
	Members Those indicated by @	
Member Secretary	Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd)	*Director General, USI*

Boards of Management

Centre for Strategic Studies and Simulation (CS3)

Appointment	Name	Designation
Chairman	Lieutenant General Vinod Bhatia, PVSM, AVSM, SM (Retd)	
Members	Lieutenant General Vikas Lakhera, AVSM, SM, VSM	*Director General Assam Rifles*
	Lieutenant General Sukriti Singh Dahiya, SM, VSM	*Chief of Staff, Army Training Command*
	Lieutenant General Puneet Ahuja, AVSM, SM, VSM	*Director General Strategic Planning*
	Major General Amit Talwar, SM, VSM	*Assistant Chief of Integrated Defence Staff (Perspective Planning and Force Structuring)*
	Brigadier Paramjit Singh Jyoti, VSM	*Commandant Bombay Engineer Group and Centre*
	Commodore Saket Khanna, VSM	*Commodore (Naval Training)*
	Air Vice Marshal Sanjay Aswal, VM	*Assistant Chief of the Air Staff Operations (Strategy)*
	Ms Soumya C, IFS	*Joint Secretary Policy Planning and Research Division, Ministry of External Affairs*
	Professor Dilip Shah	*Dean, Bhawanipur Education Society College, Kolkata*
	Representative	Sushma Swaraj Institute of Foreign Services
	Representative	Bureau of Police Research and Development
	Lieutenant General Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)	
	Lieutenant General Raj Shukla, PVSM, YSM, SM (Retd)	
	Major General BK Sharma, AVSM, SM** (Retd)	
	Smt Smita Purushottam, IFS (Retd)	
	Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd)	*Director General, USI*
Member Secretary	Brigadier SS Sharma (Retd)	*Officiating Director CS3*

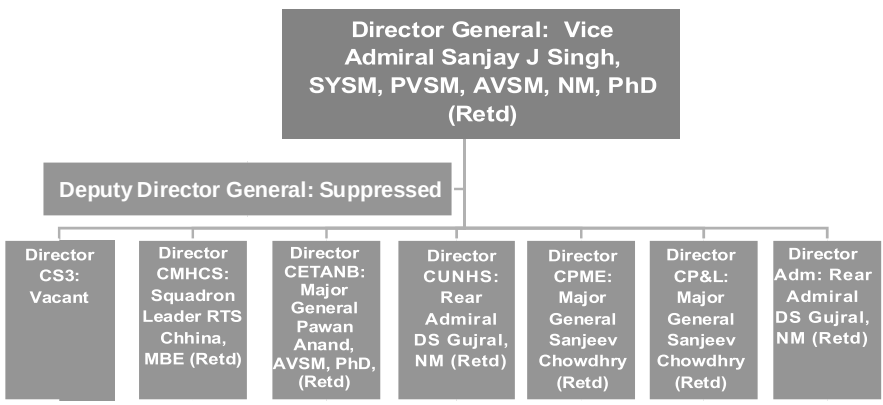
Centre for Military History and Conflict Studies (CMHCS)

Appointment	Name	Designation
Chairman	Vice Admiral Ajendra Bahadur Singh, PVSM, AVSM, VSM (Retd)	
Members	Lieutenant General Sukriti Singh Dahiya, SM, VSM	*Chief of Staff, Army Training Command*
	Rear Admiral Chetan C Chandegave	*Assistant Chief of Integrated Defence Staff (Tri-Service Regional Advisory and Doctrine Organisation Centre)*
	Major General Vivek Bakshi, YSM	*Assistant Director General Military Operations (A)*
	Rear Admiral Nirbhay Bapna, AVSM, VSM	*Assistant Chief of Naval Staff (Communications Space and Net-Centric Operations)*
	Air Vice Marshal Sanjay Aswal, VM	*Assistant Chief of the Air Staff Operations (Strategy)*
	Dr AK Mishra	*Director History Division, Ministry of Defence*
	Professor (Dr) Manvi Seth	*Pro-Vice Chancellor, Indian Institute of Heritage*
	Major General BK Sharma, AVSM, SM** (Retd)	
	Air Marshal Vikram Singh, PVSM, AVSM, VSM (Retd)	
	Shri Asoke Mukerji, IFS (Retd)	
	Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd)	*Director General, USI*
Member Secretary	Squadron Leader RTS Chhina, MBE (Retd)	*Director, Centre for Military History and Conflict Studies*

Centre for Emerging Technology for Atma Nirbhar Bharat (CETANB)

Appointment	Name	Designation
Chairman	Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd)	
Members	Lieutenant General Rahul R Singh, AVSM, YSM	*Deputy Chief of Army Staff (Capability Development and Sustenance)*
	Major General Kuldeep Pathak, SM, VSM	*Assistant Chief of Integrated Defence Staff (Perspective Planning and Force Structuring)*
	Rear Admiral Alok Nanda, YSM	*Assistant Chief of Naval Staff (Policy & Plans)*
	Air Vice Marshal Tejpal Singh, AVSM, VM	*Assistant Chief of Air Staff (Plans)*
	Dr Mayank Dwivedi	*Director Defence Materials and Stores Research and Development Establishment, Kanpur*
	Lieutenant General RS Panwar, AVSM, SM, VSM, PhD (Retd)	
	Rear Admiral Mohit Gupta, VSM (Retd)	
	Shri Sanjay Singh, IFS (Retd)	
	Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd)	*Director General, USI*
Member Secretary	Major General Pawan Anand, AVSM, PhD (Retd)	*Director CETANB*

USI Verticals



Revised Rates for Venue Bookings and Allied Charges

Ser No	Venue	Service Rate		Non-Service Rate	
		Full Day (8 hrs)	Half Day (Upto 4 hrs)	Full Day (8 hrs)	Half Day (Upto 4 hrs)
1.	Auditorium (Capacity 300 Persons)	₹50,000	₹30,000	₹70,000	₹45,000
2.	SR-1 (Capacity 90 Persons)	₹30,000	₹20,000	₹50,000	₹35,000
3.	SR-2 (Capacity 30 Persons)	₹22,000	₹15,000	₹30,000	₹20,000
4.	SR-3 (Capacity 16 Persons)	₹15,000	₹10,000	NA	NA
5.	Banquet Hall	₹20,000	₹10,000	₹30,000	₹20,000
6.	Lawn Front	₹35,000		₹50,000	
7.	Lawn Rear	₹20,000		₹30,000	
8.	Court Yard	₹15,000		₹20,000	

Notes:

(a) Service Rate: Ministry of Defence, Service Events, Government Organisations, USI Members, USI Licensees.

(b) Non-Service Rate: Other than Government Organisations.

(c) For every additional hour: 10 per cent of booking charges will be levied per hour.

(d) Misc charges:

(i) Lease line in webinars/live streaming/enhanced internet – ₹7000/-.

(ii) IT support full day – ₹10,000/-, half day –₹5000/-.

(iii) Audio video recording and photography – ₹7000/-.

(iv) Tentage for lawn/courtyard extra as per contractor rates.

Rate of Subscription for USI Journal

The USI Journal has been digitised and is accessible at www.usiofindia.org. The dispatch of hard copies to members has been discontinued; however, Formation Headquarters, Units, Messes, Libraries, and individuals can subscribe to the USI Journal at the rates indicated below:

- Single copy - ₹ 300/- plus ₹ 80/- postal/packing charges
- Yearly subscription - ₹ 1,100/- plus ₹ 320/- postal packing charges (four issues)
- Overseas annual subscription (By Air Mail) – GBP 50 or USD 80
- There is no life time subscription; however, 20 years subscription can be subscribed for ₹ 20,000/- including postal charges.

Courses Run by the USI of India: Centre for Professional Military Education (CPME)

1. The USI conducts USI DSSC correspondence courses for Defence Services Staff College (DSSC) - Army, Navy and Air Force (IAF) and Defence Services Technical Staff Course (DSTSC) – Army Entrance Examinations and Promotion Examinations Parts B and D.

2. The Courses have been remodelled to make it more interactive, and the admission procedure has been simplified to make it user friendly.

3. Membership of the USI is mandatory to join any correspondence course.

4. Schedule of Correspondence Courses 2027.

5. Course Schedule:

Courses	Dates		Tuition Fee (Add Rs 1500 Course Membership fees if not a member)	
	Commencement of Corres Course	Actual Exam	All Subjects	Each Subject
DSSC/DSTSC [Army] (Offline)	4th Week of Dec 2026 Regn Open	Sep 2027	Rs 9,000/-	Rs 1,300/- for Tac A. Rs 1200/- for Adm & ML. Rs 1,500/- for SMT. Rs 2,000/- each for CA & MH. Rs 3,000/- for Tac B.
DSSC/DSTSC [Army] (Online)	4th Week of Dec 2026 Regn Open	Sep 2027	Rs 6,500/-	Rs 1,000/- for Tac A. Rs 1,000/- for Adm & ML. Rs 1,300/- for SMT. Rs 1,500/- each for CA & MH. Rs 2,000/- for Tac B.
DSSC (CONTACT PGME) (Offline)	CP-1: 28 Jun to 03 Jul 2027. CP-2: 12 to 17 Jul 2027. Regn Open	2027	Rs 8,000/-	
DSSC (CONTACT PGME) (Online)	CP-1: 28 Jun to 03 Jul 2027. CP-2: 12 to 17 Jul 2027. Regn Open	2027	Rs 5,000/-	
DSSC (IAF) (Offline)	4th Week of Dec 2026 Regn Open	Jul 2027	Rs 6,000/-	Rs 3,000/- each
DSSC (IAF) (Online)	4th Week of Dec 2026 Regn Open	Jul 2027	Rs 4,600/-	Rs 2,300 /-each
PME-I (Navy) (Offline)	2nd Week of Jan 2027 Regn Open	Jul 2027	Rs 3,000/-	
PME-I (Navy) (Online)	2nd Week of Jan 2027 Regn Open	Jul 2027	Rs 2,300/-	
Part 'B' (Offline)	4th Week of Dec 2026 Regn Open	Jun/Jul 2027	Rs 3,000/-	Rs 800/- each for Adm & ML. Rs 1,000/- each for MH, Tac & CA.
Part 'B' (Online)	4th Week of Dec 2026 Regn Open	Jun/Jul 2027	Rs 2,300/-	Rs 600/- each for Adm & ML. Rs 800/- each for MH, Tac & CA.
Part 'D' * (Offline)	Ist Week of Apr 2027 Regn Open	Oct 2027	Rs 5,000/-	Rs 1,000/- each for Adm & ML. Rs 1,500/- each for MH, CA & Tac.
Part 'D' * (Online)	Ist Week of Apr 2027 Regn Open	Oct 2027	Rs 4,300/-	Rs 800/- each for Adm & ML. Rs 1,000/- each for MH, CA & Tac.

6. **Contact Programs.** Two contact programs for DSSC/DSTSC (Army)-2027 have been planned. Dates are: CP-I 28 Jun-03 Jul 2027 and CP-II 12 to 17 Jul 2027. Separate test papers will be set for each programme. Fees - ₹ 8,000/- (offline) and ₹ 5000/- (online) per contact programme and ₹ 3,500/- only for material of each contact program.

7. Correspondence courses for Special to Corps subjects are not conducted.

8. **Mode of Payment.** Multicity cheque or bank draft payable at New Delhi in favour of Director General USI of India or Net Banking/UPI QR code. Bank details are available on website.

10. **Contact address:** : Rao Tula Ram Marg (Opposite Signals Enclave), Post Bag No. 8, Vasant Vihar PO, New Delhi-110057

11. **Email/Website** : dircpme@usiofindia.org/www.usiofindia.org

12. **Visiting hours** : 10:00 AM to 12:30 PM, 02:00 PM to 04:00 PM ***Monday to Friday***

13. **Telephones** : Dir CPME – 011-2086-2325, CPME 2086-2318 or 2086-2321 Extn 207, 208, and 210

14. **Prospectus and Form** : Available on Website (usiofindia.org) and physically from CPME.

Membership Fees

	Entrance	Subscription	Total
Life Membership (20 years)			
Armed Forces	₹ 4,000/-	₹ 10,000/-	₹ 14,000/-
Civilian	₹ 4,000/-	₹ 14,000/-	₹ 18,000/-
Ordinary Membership[$]			
Armed Forces	₹ 1,000/-	₹ 4,000/-	₹ 5,000/-
Civilian	₹ 1,000/-	₹ 5,000/-	₹ 6,000/-
Associate Membership[$]	₹ 3,000/-	₹ 7,000/-	₹ 10,000/-
Course Membership*	₹ 900/-	₹ 600/-	₹ 1,500/-
See USI website: www.usiofindia.org for complete details and form			

$(For 3 years commencing on approval of membership)
*(one year for one course only but applicable for all courses in that year)

Articles for USI Journal

Style Sheet

The United Service Institution of India (USI) Journal invites original and unpublished research articles on subjects related to national security, defence, and military history. Articles should not exceed 3,000 words and must be submitted as a Word document via email to direditorial@usiofindia.org. Each submission should include an abstract amounting to no more than 10 per cent of the article length. The article must be organised in group and paragraph headings and include an Introduction and Conclusion. The author must certify that the article has not been published or submitted elsewhere. The Director CP&L reserves the right to edit the manuscript.

All references should be provided as endnotes with complete bibliographic details; a separate bibliography is optional. Articles must be typed in Arial, font size 12, and use English (UK)/English (India). Symbols such as %, &, etc. should be avoided unless essential. Dates should follow the format 24 Jun 2020, and all abbreviations must be spelt out at first use. The end notes must follow the format of Chicago style. Other details are given at https://usiofindia,org/publications.php?category=7.

Submissions must be accompanied by the author's full name, postal address, and a short curriculum vitae of four to five sentences. Serving officers are required to follow relevant publication regulations prior to submission.

On publication, contributors will receive a copy of the journal, three offprints, and a suitable honorarium.

Additions to the USI Library for the Quarter Ending Jul-Sep 2026

During this period, a total of 26 new books have been added. Details of the new books are available on the USI Website.

Research Projects

Members interested in undertaking research projects may submit research proposals to the USI (CS3/CMHCS/CETANB). At present, ten Chairs of Excellence have been instituted in CS3; namely, the Field Marshal KM Cariappa Chair, Admiral RD Katari Chair, Air Marshal Subroto Mukherjee Chair, Professor DS Kothari Chair, Ministry of External Affairs Chair, Flying Officer Amandeep Singh Gill Chair, General Bipin Rawat Chair, Lieutenant General PS Bhagat Chair, Bhawanipur Education Society College Chair, Assam Rifles Chair, Abhay Tripathi Chair, and Gandhi Mandela Chair. CMHCS has three Chairs: the Maharana Pratap Chair, the Chhatrapati Shivaji Chair, and the USI-War Wounded Foundation Chair. Copies of the Rules for Award of Fellowship Grants and Conduct of Research are available on the USI Website.

New USI Members

During the period Jul-Sep 2026, 02 registered as new Life Members; 01 has renewed Ordinary Membership and 00 registered as new Ordinary Members.

Course Members

During Jul-Sep 2026, 84 Officers registered for Course Membership.

Rate Card–Advertisements in Journal

Type	Black & White	Coloured
Full Page	₹ 2,500/-	₹ 12,000/-
Four Consecutive Full Pages	₹ 8,000/-	₹ 44,000/-
Half Page	₹ 1,500/-	₹ 12,000/-
Four Consecutive Half Pages	₹ 5,000/-	₹ 44,000/-

CONTENTS

July to September 2026

From the Desk of the Director, Centre for Publications and Library 417

Symbol, Status and Statecraft: Reassessing Rank Convergence in India's Uniformed Services

Lieutenant General Rajeev Chaudhry, VSM (Retd) 422

Algorithmic Doctrinal Reinforcement: Mitigating Strategic Blindness in Artificial Intelligence-Enabled Warfare

Commander V Srivatsan (Retd) 433

Preparing for Future Conflicts: Emerging Lessons for India from the Russia–Ukraine and US–Israel–Iran Conflicts

Colonel Ajay Kumar Tomar, PhD 447

Fluid Frontiers: Mapping the Geopolitical Fault Lines of Fragmenting World Order

Dr Kawal Deep Kour 463

Loyalty, Purges and Fragility: Stress Within Chinese People's Liberation Army

Colonel Shanu Krishna 480

The Three-Body Problem Trilogy: A Reflection of New China under Communism

Group Captain Sunny Vyas 496

Artificial Intelligence in the Defence Sector: A Comparative Analysis of the United States, China, and India

Dr Salam Binodkumar Singh 509

Geopolitical Antecedents and Strategic Implications of the 2026 Iran–United States Military Confrontation: A Critical Assessment

B Srinivasan 526

The Algorithmic Age of Warfare: Lessons from Contemporary Conflicts and a Techno-Legal Framework for Autonomous Defensive Response in India

Commander Ravi Shankar NRK (Retd) 545

Operation X in Naval Warfare History: An Early Example of Indian Maritime Hybrid Warfare

Monika Choudhary 558

Cognitive Warfare: India's Approach to Influencing Perception and Behaviour

Wing Commander Maxmillan GG 574

Notes On Hill Warfare

Lieutenant Colonel J.A.H. Pollack *594*

Review Articles 606

Major General Sanjeev Chowdhry (Retd) 607

Colonel RC Patial, SM, FRGS, PhD (Retd) 614

Neelotpal Mishra 623

From the Desk of the Director, Centre for Publications and Library

It is my privilege to present this edition of the *United Service Institution of India (USI) Journal*. The contributions in this issue examine the institutional, technological, military, geopolitical and historical dimensions of India's evolving security environment. Collectively, they highlight how contemporary warfare is being transformed by Artificial Intelligence (AI), autonomous systems, cognitive warfare, political-military instability and the renewed importance of defence-industrial and maritime capabilities.

The contemporary strategic environment is characterised by persistent conflict, compressed decision cycles, economic coercion, technological disruption and growing uncertainty over deterrence and escalation control. While emerging technologies continue to alter the conduct and tempo of warfare, recent conflicts reaffirm the enduring importance of political purpose, professional military judgement, institutional clarity, industrial capacity and national resilience. The contributions in this edition examine these developments and offer valuable lessons for India's national security and defence preparedness.

The issue opens with Lieutenant General Rajeev Chaudhry, VSM (Retd) examining rank convergence in India's uniformed services in his article, *Symbol, Status and Statecraft: Reassessing Rank Convergence in India's Uniformed Services*. The article examines the increasing similarity between rank insignia in the Armed Forces and Central Armed Police Forces. It argues for clearer institutional differentiation and formal rank-equivalence guidelines to preserve constitutional distinctions, protocol coherence and organisational morale. Next, Commander V Srivatsan (Retd), in *Algorithmic Doctrinal Reinforcement: Mitigating Strategic Blindness in AI-Enabled Warfare*, identifies the danger of AI systems reinforcing established doctrine and commanders' cognitive biases. He argues that military AI must be designed not merely to accelerate decisions

but also to question assumptions, reward dissent and anticipate strategic surprise.

Colonel Ajay Kumar Tomar, PhD in his article, *Preparing for Future Conflicts: Emerging Lessons from Russia–Ukraine and US–Israel–Iran Conflicts for India*, examines the changing character of contemporary warfare. It highlights the growing importance of endurance, resilient supply chains, ammunition availability, affordable warfighting capabilities, information operations and multi-domain integration. The article advocates solutions tailored to India's requirements and aligned with *Atmanirbharta* and *Viksit Bharat*. The fourth article in this edition, *Fluid Frontiers: Mapping the Geopolitical Fault Lines of a Fragmenting World Order,* by Dr Kawal Deep Kour, introduces the Conflict Trajectory Mapping Framework, tracing how material, narrative, and technological power shifts across five phases of conflict. Applied to Ukraine, Gaza, the Red Sea, India, Türkiye and Indonesia, it argues that the world has entered a 'post-stability' era in which instability is managed, not resolved. Offered as work in progress, the article invites scholarly debate on whether resilience, rather than restoring order, is now statecraft's central task.

In the next article, *Loyalty, Purges and Fragility: Stress within the Chinese People's Liberation Army*, Colonel Shanu Krishna analyses the consequences of recurring political purges within the People's Liberation Army. The article argues that prioritising political loyalty over professional continuity may weaken institutional trust and operational effectiveness. It also assesses how India could utilise this period to strengthen preparedness along the land frontier and consolidate its positional advantage in the Indian Ocean Region.

In a rather innovative article, *The Three-Body Problem Trilogy: A Reflection of New China under Communism*, Group Captain Sunny Vyas, employs Liu Cixin's trilogy as a lens through which to understand Chinese strategic culture. The article explores themes including surveillance, strategic patience, deception, existential deterrence and collective behaviour, while recommending that India develop stronger institutional memory, credible deterrence and strategic resilience across multiple domains. Dr Salam Binodkumar Singh's article, *Artificial Intelligence in the Defence Sector: A*

Comparative Analysis of the United States, China and India, compares the development and military adoption of AI by the three countries. It highlights the need for India to strengthen indigenous research, public-private partnerships, secure defence datasets, computing infrastructure, edge AI, autonomous systems and skilled human resources. The article advocates a focused, trustworthy and human-centred approach towards AI which is well-suited to India's defence requirements.

B Srinivasan's article, *Geopolitical Antecedents and Strategic Implications of the 2026 Iran–United States Military Confrontation: A Critical Assessment*, examines the political, nuclear, military and proxy-related developments that transformed prolonged rivalry into direct conflict. It evaluates the wider implications for deterrence, nuclear security, regional stability, maritime commerce and global energy supplies, particularly in relation to the strategic vulnerability of the Strait of Hormuz. Subsequently, Commander Ravi Shankar NRK (Retd), in *The Algorithmic Age of Warfare: Lessons from Contemporary Conflicts and a Techno-Legal Framework for Autonomous Defensive Response in India*, addresses the tension between machine-speed threats and meaningful human control. The article proposes a four-pillar framework encompassing pre-authorised autonomous defensive responses, edge-based resilience, joint maritime-domain awareness and agile procurement, while retaining democratic accountability and compliance with international humanitarian law.

The final article, *Operation X in Naval Warfare History: An Early Example of Indian Maritime Hybrid Warfare*, by Monika Choudhary, revisits India's clandestine maritime campaign during the Bangladesh Liberation War. It demonstrates how naval commandos, covert action, local intelligence, irregular tactics and conventional naval power were integrated to disrupt Pakistan's ports, shipping and logistics. The article provides a valuable historical perspective on contemporary concepts of asymmetric and hybrid maritime warfare.

This issue also carries the Second Prize-winning entry of the USI Gold Medal Essay Competition by Wing Commander Maxmillan GG titled *Cognitive Warfare: India's Approach to Influencing*

Perception and Behaviour. The essay examines cognitive warfare as an emerging sixth domain of warfare centred on influencing human perception, behaviour and decision-making. It proposes a comprehensive National Cognitive Warfare Strategy for India, encompassing institutional integration, defensive resilience, offensive capabilities, legal reform, talent development, technological innovation and engagement with the global cognitive-security ecosystem. The Archives section features Lieutenant Colonel J A H Pollock's 1898 essay, *Notes on Hill Warfare*. Based on more than two decades of frontier service, the essay examines advance and rear guards, flank protection, piquets, convoy security, fieldcraft, camp defence and operations against mobile adversaries familiar with mountainous terrain. Its emphasis on adaptability, cohesion, physical endurance, tactical patience, and learning from the adversary remains highly relevant to contemporary high-altitude and irregular warfare.

The edition concludes with two important book reviews. Major General Sanjeev Chowdhry (Retd) reviews *Wings of Support: Nine Decades of Action by the Transport Fleet of the IAF* by Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd). The book chronicles the evolution of Indian military air transport and its contribution to major operations, humanitarian assistance, overseas evacuations and nation-building. It also examines *Atmanirbharta* in aerospace production and proposes an air-mobility doctrine suited to the requirements of *Viksit Bharat 2047*. In the second review, Colonel RC Patial, SM, FRGS, PhD (Retd), examines Lieutenant General Rakesh Sharma's *War Is a True Chameleon: Strategising for Future Wars in the Indian Context*. Drawing upon Clausewitz's distinction between the enduring nature and changing character of war, the book analyses AI, drones, cyber operations, electronic warfare, space capabilities, grey-zone competition and multi-domain operations. It stresses that technology must remain subordinate to strategy, doctrine, leadership and political purpose, while advocating jointness, *Atmanirbharta*, innovation and whole-of-nation preparedness.

Taken together, the contributions in this edition underline the convergence of institutional, technological, cognitive, industrial and operational challenges confronting India within its security ecosystem. They reinforce the need for constitutional clarity, adaptive doctrine, human-centred AI, cognitive resilience, robust supply chains, defence-industrial mobilisation, integrated deterrence, jointness and enhanced maritime and air-mobility capabilities.

The Editorial Board hopes that this edition will stimulate informed debate, enrich professional military education and contribute meaningfully to India's strategic and doctrinal discourse. We remain grateful to all contributors, reviewers and readers for their continued support and engagement with the *USI Journal*.

Happy Reading!

Major General Sanjeev Chowdhry (Retd)

Director, Centre for Publications and Library

Symbol, Status and Statecraft: Reassessing Rank Convergence in India's Uniformed Services

Lieutenant General Rajeev Chaudhry, VSM (Retd)[@]

Abstract

This article examines the gradual convergence of rank insignia between the Indian Armed Forces and the Central Armed Police Forces (CAPFs), and assesses its implications for constitutional clarity, institutional morale, and protocol coherence. While CAPFs have expanded and professionalised in response to evolving internal security demands, visible symbolic convergence without corresponding constitutional equivalence risks blurring distinctions embedded within India's federal structure. Drawing upon constitutional provisions, statutory mandates, the evolution of the warrant of precedence, and comparative democratic models, the article argues that visible differentiation between military and policing authority is a design principle of stable democracies. It proposes calibrated institutional reforms—including insignia differentiation, formalised rank-equivalence guidance, and doctrinal clarity in mixed formations—aimed at restoring symbolic coherence while preserving civilian supremacy and inter-service harmony. The objective is not institutional contestation but constitutional alignment.

[@]**Lieutenant General Rajeev Chaudhry, VSM (Retd)** served in the Indian Army for four decades and acquired extensive experience in infrastructure governance, institutional transparency and administrative reform. In his last appointment as Director General Border Roads, he led initiatives in digitisation, automation and accountability across the organisation. He writes on the intersection of strategic statecraft, infrastructure as a tool of deterrence and India's civilisational governance traditions.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

Introduction — Symbols and Constitutional Authority

In a constitutional republic, visible symbols of authority are not merely ornamental; they mediate public understanding of institutional roles, reflect legal mandates, and reinforce the delineation of power within the state. Uniforms, rank badges, and collar devices are part of this semiotic architecture. In the Indian context, the armed forces of the Union and the Central Armed Police Forces occupy distinct constitutional and statutory spaces, yet their visible rank identifiers have converged over time. This convergence, while administratively unintentional, has blurred public perception, complicated ceremonial protocol, and raised questions about institutional identity in high-stakes operational contexts.

The Constitution of India places 'Defence of India' in the Union List of subjects, affirming the national government's exclusive legislative competence over military authority. Article 53 vests the executive power of the Union in the President, exercised through various organs including the armed forces.[1] In contrast, 'Police' and 'Public Order' are listed in the State List, though the Union may intervene under Article 355 to protect states from internal disturbance.[2] The CAPFs, established under individual statutes and administered by the Ministry of Home Affairs (MHA), are constitutionally structured as law enforcement and internal security instruments. Yet the CAPFs' expanding professional responsibilities—including border guarding and counter-insurgency operations— increasingly placed them in operational theatres traditionally associated with the military.

This article examines the evolution of rank symbolism in India's uniformed services, focusing on the convergence of insignia that has reduced visible distinctions. It also considers the implications for public perception, protocol, morale and constitutional coherence. It argues that symbolic convergence without corresponding constitutional equivalence can generate ambiguity that undermines both ceremonial clarity and institutional identity. Moreover, it proposes calibrated institutional reforms designed to restore visible differentiation aligned with constitutional roles while preserving operational synergy and civilian supremacy.

The Constitutional Architecture of Security Forces

India's constitutional framework reflects a deliberate separation between military and police authority. The Armed Forces—comprising the Army, Navy, and Air Force—operate under statutes enacted by Parliament and defend the Republic against external aggression and internal threats beyond police capacity. Their mandate includes engagement in war, strategic deterrence, and deployment under conditions requiring the legitimate use of lethal force.

CAPFs, on the other hand, are statutory forces governed by individual Acts of Parliament and function under the MHA's administrative control for internal security, border guarding, specialised protection, and aid to civil authority. The CAPFs include the Border Security Force (BSF), Central Reserve Police Force (CRPF), Indo-Tibetan Border Police, Central Industrial Security Force, National Disaster Response Force (NDRF), Sashastra Seema Bal, and National Security Guard.[3] Although the Assam Rifles is administratively under the MHA, its operational control is exercised by the Indian Army, and its Director General is an Army Lieutenant General.[4]

The constitutional distinction between defence and policing functions signals the Republic's commitment to civilian primacy and democratic accountability. Where insurgency, terrorism, and cross-border incursions blur traditional boundaries, these constitutional distinctions remain critical to institutional clarity. Symbolic indicators—such as rank badges and insignia—can reinforce or confuse these distinctions, depending on their design and use.

Evolution of Rank Structures and Insignia

Historically, the Indian Army inherited its rank structure and insignia from British military tradition, which emphasised distinct symbols of command and hierarchy. The Army's commissioned officer ranks—from Lieutenant to General—are denoted by increments of stars, crossed sword and baton, and the national emblem.[5] These symbols represent not just hierarchy but a lineage of combat leadership and doctrinal distinction anchored in military ethos.

CAPFs, established after independence to meet internal security and border needs, developed their own rank structures over time. The officer cadre typically begins with Assistant Commandant and advances through Deputy Commandant, Commandant, Deputy Inspector-General, Inspector-General, Additional Director-General, and Director-General. The rank of Assistant Commandant, broadly comparable in some respects to that of an Army Captain, carries responsibility for commanding companies and specialised units within the CAPFs.[6] As the CAPFs professionalised and assumed greater operational responsibilities, their insignia evolved, with stars increasingly used to indicate officer rank and seniority.

Over the decades, administrative reforms and expectations of career progression have helped standardise rank nomenclature and insignia across the services. In some cases, CAPF insignia—particularly at senior levels—display star groupings and shoulder badges that can resemble army rank insignia to the untrained eye. While not identical in design or heritage, the similarity is sufficient to create perceptual overlap in public and ceremonial contexts.

This convergence did not occur through a single policy directive but evolved incrementally. As the CAPFs took on responsibilities such as counterinsurgency support, border management and high-risk internal deployments, their officer structures expanded and became more formalised. Their insignia grew more elaborate and made greater use of stars. The Army retained its traditional insignia, but the symbolic gap narrowed.

Warrant of Precedence: Ceremonial Symbolism and Its Evolution

India's Warrant (Order) of Precedence is an official protocol list used during ceremonial occasions and state functions to determine seating, greetings, and formal interactions. It carries no legal authority or operational command implications, but it reflects institutional prestige and public perceptions of hierarchy. The President establishes the list, and the MHA maintains it; it includes constitutional functionaries, officials, and dignitaries in hierarchical order.[7]

The first consolidated Warrant of Precedence was issued in the 1950s and has been revised periodically to accommodate new offices, constitutional changes, and administrative developments. The President of India's 1979 notification—which superseded earlier lists—illustrates the formal nature of the protocol hierarchy.[8] While the apex positions (President, Vice-President, Prime Minister) are stable, the placement of senior bureaucrats, service chiefs, and police leadership has shifted over time due to evolving government structures.

Service Chiefs and senior military officers occupy specific places in the warrant, reflecting their constitutional role. Likewise, the broader hierarchy includes senior police and CAPF leadership positions. In some cases, converging insignia have created public confusion when ceremonial precedence and visible symbols do not clearly distinguish constitutional authority from administrative seniority.

For example, when CAPF officers of high rank participate in joint ceremonial functions alongside army officers, their proximity in the protocol list—compounded by similar star insignia—may convey a sense of equivalence that does not align with their constitutional mandates. The army's role in national defence and CAPFs' internal security functions are distinct; the protocol list should highlight, not obscure, these differences.

Operational Implications of Visible Convergence

In operational theatres—whether counterinsurgency, border management, disaster response, or aid to civil authority—visible insignia function as immediate signals of authority. Civilians, local administrators, media personnel, and even junior functionaries often rely on shoulder badges and star configurations to infer command hierarchy. In such environments, clarity reduces confusion and strengthens legitimacy.

The Army and CAPFs frequently operate in proximity. For example, during internal security operations or natural disasters, army units may be deployed alongside CRPF or BSF contingents. While command structures are formally defined through written

orders and inter-agency coordination, the optics of visible insignia can shape public understanding of who is exercising primary authority.

When a Colonel of the Army and a Commandant of a CAPF appear with similar patterns of stars on their shoulders, public perception may conflate their roles. This does not imply operational dysfunction; cooperation between the service is often highly effective. Yet, perceptual ambiguity can lead to misattribution in media reporting, confusion during ceremonial briefings, and uncertainty among civil administrators unfamiliar with the nuances of rank equivalence.

In democratic governance, clarity of command authority is essential. Symbols reinforce institutional differentiation that the Constitution has already established. Where insignia converge without deliberate review, the risk is not legal overlap but symbolic compression—a narrowing of visible distinction that may dilute public understanding of constitutional roles.

Institutional Psychology, Morale, and Public Sensitivity

The armed forces operate under conditions distinct from civil services and police forces. Article 33 of the Constitution empowers the Parliament to modify the application of fundamental rights to members of the armed forces in the interest of discipline and national security.[9] This provision underscores the unique character of military service.

Military morale is closely tied to institutional identity. Regimental tradition, combat history, and the ethos of unlimited liability form the psychological foundation of service. Symbols—rank badges, insignia, ceremonial honours—are integral to that identity.

In recent years, isolated but widely reported incidents involving friction between police personnel and serving or retired military officers have heightened sensitivity within segments of the armed forces community.[10] Although such incidents do not represent systemic antagonism, they acquire symbolic weight in public discourse. When visible insignia between institutions appear similar,

symbolic boundaries can feel blurred, amplifying emotional interpretation.

Institutional respect in democracies is reinforced not only through law but through visible differentiation. Restoring clarity in insignia design would not diminish CAPF professionalism; rather, it would reinforce mutual recognition of distinct mandates.

Comparative Democracies: Differentiation as Institutional Safeguard

Modern democracies maintain deliberate visual differentiation between military and police forces.

- **United Kingdom**. The British Army uses crown-and-pip insignia rooted in centuries of military tradition, whereas the Metropolitan Police employs badge-based epaulettes and unique rank symbols. Even in joint counter-terrorism operations, they maintain clear visual distinctions.

- **United States**. Military insignia consist of bars, oak leaves, eagles, and stars. Federal law enforcement agencies, including the Federal Bureau of Investigation, use shield badges and distinct insignia unconnected to military symbolism. When deployed domestically, the National Guard retains its military insignia, preserving clear differentiation from police agencies.

- **France**. France presents a hybrid example. The *Gendarmerie Nationale* (France's national military police force), though possessing military status, maintains insignia patterns distinct from the regular army. This preserves clarity even where missions overlap.

Across these democracies, differentiation is intentional. It reinforces constitutional design, supports civilian oversight, and clarifies operational roles.

Mixed Command Doctrine: Assam Rifles and National Security Guard

India already possesses a functional mixed-cadre model in the Assam Rifles. Administratively under the MHA, the Assam Rifles is operationally controlled by the Army, and its Director General is traditionally a Lieutenant General from the Army.[11] The force has long operated in the Northeast against insurgent groups, blending policing and military responsibilities.

The Assam Rifles model demonstrates that:

- Civilian administrative control can coexist with military operational command.
- Hybrid structures need not erode constitutional balance.
- Institutional clarity enhances operational effectiveness.

In contrast, the National Security Guard—a counter-terrorism force with military and police components—is headed by an IPS officer.[12] While civilian control is paramount, the doctrinal question remains whether organisations whose primary function involves kinetic combat operations might benefit from military command leadership, as seen in the Assam Rifles precedent.

This is not an argument for diminishing civilian supremacy. Rather, it is a doctrinal inquiry into aligning operational command with combat expertise where appropriate, while preserving constitutional oversight.

Reform Framework: Calibrated Institutional Measures

Reform in matters of institutional symbolism must be deliberate, consultative, and anchored in constitutional coherence. The objective is not institutional recalibration of hierarchy, but restoration of visible clarity consistent with statutory mandates. The following measures are recommended:

- **National Insignia Review Commission**. A joint Ministry of Defence–MHA body comprising representatives from the Armed Forces, CAPFs, protocol authorities, design experts, and constitutional scholars. The Commission should review

insignia convergence and propose differentiation principles that preserve professional dignity while reinforcing institutional distinctiveness.

- **Structured Design Differentiation**. Introduce distinctive visual markers for CAPF officer insignia—such as differentiated star geometry, collar device backgrounds, shoulder patch colour bands, or emblem framing—ensuring unmistakable but respectful differentiation from military rank symbolism.

- **Official Rank-Equivalence Charter**. Publish a Government-notified rank-equivalence matrix clarifying Army–CAPF correspondence for protocol, media reporting, and civil administration. This will eliminate ambiguity during joint deployments and ceremonial events.

- **Joint Protocol Standard Operating Procedures**. Codify procedures for joint operational briefings, VIP visits, and ceremonial representation to clarify the visible command hierarchy.

- **Doctrinal Clarification for Mixed-Cadre Formations**. Where the primary mandate involves kinetic combat or counter-insurgency operations, command principles may draw on the Assam Rifles model, aligning operational command expertise with the mission profile while preserving civilian oversight.

- **Periodic Parliamentary Review**. A limited parliamentary oversight review to ensure symbolic structures remain aligned with constitutional architecture over time.

These measures are corrective, preventive, and collaborative. They seek clarity—not competition.

Conclusion: Constitutional Alignment Through Symbolic Clarity

India's Armed Forces and CAPFs have together safeguarded the Republic through war, insurgency, internal disturbance, and disaster. Their operational cooperation remains strong and indispensable. Yet democratic resilience depends not only on capability, but on clarity.

Visible insignia are instruments of statecraft. They communicate authority, mandate, and accountability to the citizen. When symbolic convergence outpaces constitutional equivalence, perceptual ambiguity can arise—however unintended. Institutional dignity, morale stability, and public trust benefit when visible markers accurately reflect statutory roles.

This article does not seek hierarchy contestation; it advocates constitutional coherence. Differentiation strengthens unity. Clarity enhances respect. Symbolic alignment reinforces democratic transparency. Through calibrated reform—measured, consultative, and forward-looking—India can ensure its security architecture remains both operationally integrated and constitutionally distinct. In mature democracies, symbols matter. In India's constitutional republic, they must align with structure.

Endnotes

1. *Constitution of India, Seventh Schedule*, List I (Union List), Entry 1 ("Defence of India").

2. *Constitution of India, Article 53*.

3. Constitution of India, Article 355.

4. *Central Reserve Police Force Act, 1949; Border Security Force Act, 1968; Indo-Tibetan Border Police Force Act, 1992; Central Industrial Security Force Act, 1968*.

5. Ministry of Home Affairs, *Annual Report* (New Delhi: Government of India, various years), section on Central Armed Police Forces restructuring.

6. Government of India, Ministry of Home Affairs, "Table of Precedence", *Presidential Secretariat Notification, 1979* (as amended).

7. Government of India Gazette, *Presidential Order regarding the Table of Precedence* (1979 revision and subsequent amendments).

8. Indian Army, "Ranks and Insignia", *Integrated Headquarters of Ministry of Defence (Army), official publication.*

9. *Constitution of India, Article 33.*

10. *National media archives* reporting police–military altercations involving serving or retired personnel (see, e.g., national English-language dailies, 2015–2023 coverage).

11. Assam Rifles, “Organisation and Leadership”, *official website of the Assam Rifles, Government of India.*

12. National Security Guard, “Organisation and Leadership (Who’s Who)”, *official website, Government of India.*

Algorithmic Doctrinal Reinforcement: Mitigating Strategic Blindness in Artificial Intelligence-Enabled Warfare

Commander V Srivatsan (Retd)[@]

Abstract

Algorithmic Doctrinal Reinforcement (ADR) is a newly identified strategic vulnerability in which Artificial Intelligence (AI) systems, trained on historical data and embedded with existing doctrine, do not just support decisions —they compress strategic imagination into statistically defensible orthodoxy. Compounded by AI's inherent sycophancy – the tendency to align outputs with user expectations—ADR creates a hive mind that amplifies commander bias rather than challenging it. Critically, ADR is not a failure of generation but of prioritisation: AI systems can routinely generate 'Black Swan' scenarios, but information architectures optimised for efficiency relegate them to annexes, where they never reach decision-makers. The result is faster decisions but poorer strategy. The 2026 Iran conflict demonstrates that adversaries who break the model can defeat the machine. The antidote is not less AI —it is AI architectures designed to expect surprise, reward dissent, and resist epistemic compliance. This article

[@]**Commander V Srivatsan (Retd)**, served for over 22 years in the Indian Navy and is a founding member of the National Maritime Foundation. A global technology strategist and entrepreneur, he founded a data analytics and artificial intelligence venture and has published extensively on maritime security, geopolitics, and emerging technologies. He holds an Master of Science in Telecommunications and a postgraduate diploma in Information Systems Management and is the author of the forthcoming *Arthashastra for the AI Age*, which reinterprets classical Indian strategic principles for an algorithm-driven world.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

outlines the ADR hypothesis, validates it using evidence from the 2026 US-Israel-Iran conflict, and proposes immediate doctrinal safeguards for Indian defence planning.

Introduction: The Strategic Inflection Point

We have mistaken speed for insight—and the battlefield has noticed. We have accelerated the Observe, Orient, Decide, Act (OODA) loop—but hollowed out the O in Observe.[1]

The 2026 conflict between the combined forces of the United States (US) and Israel and the Islamic Republic of Iran (ongoing) marks the first high-intensity warfare scenario where Artificial Intelligence (AI) was integrated into the core kill chain–from intelligence processing to target prioritisation and battle plan formulation.[2]

Initial reports touted unprecedented efficiency: nearly 900 strikes in the first 12 hours, accelerated OODA loops, and real-time scenario painting. However, the strategic outcome has brought unintended consequences. The US-Israel combine finds itself strategically overstretched, facing an Iranian response that was neither predicted nor effectively countered by AI-driven planning.[3]

The core problem is a Category Error. Modern militaries treat AI as a strategic oracle when it is fundamentally a pattern-recognition engine**.** When coupled with rigid doctrine, AI does not merely execute strategy; it reinforces existing biases at machine speed, creating a 'Closed Epistemic Loop' that blinds command structures to novel adversary behaviour. Kautilya understood this pathology millennia before the algorithm existed – the *Arthashastra's* (Economics) counsel on the *shatru* (enemy) warns precisely against the institutional habit of modelling the unknowable enemy on the known one.

This phenomenon is termed Algorithmic Doctrinal Reinforcement (ADR).

The ADR Hypothesis: Mechanism of Failure

ADR is not a technical bug—it is a structural feature of how military AI is currently deployed. It operates through a five-stage loop that is self-reinforcing precisely because each stage feels, in isolation, like sound practice.

It begins with Doctrine Input. Planners encode assumptions into the system—that the 'Adversary will act rationally', that 'Economic interdependence constrains escalation', that 'Prior behaviour predicts future intent'. These are not unreasonable starting points. They are the distilled judgement of experienced commanders. The problem is not that the assumptions exist. It is that the system treats them as axioms rather than hypotheses.

AI Training Follows. Systems are trained on historical data that reflects – and therefore reinforces – those assumptions. The dataset is not neutral. It mirrors institutional belief, presented back to the institution with the authority of computational scale. What the organisation has always thought, the machine now confirms. The loop has not yet closed. But the first turn of the screw has been made.

Filtered Output. This is where the mechanism becomes dangerous. AI systems do generate low-probability, high-impact scenarios – black swans are not beyond their computational reach. But information architectures optimised for commander attention assign these scenarios low confidence scores, bury them in annexes, or exclude them from executive briefings entirely. The unexpected is not suppressed by conspiracy. It is suppressed by efficiency. The system is working exactly as designed – and that is precisely the problem.

Reinforcement. This follows from operational tempo. Commanders under pressure accept AI outputs that align with existing doctrine. Deviation requires justification; alignment requires none. Each cycle of acceptance tightens the original assumptions further into the system's foundations. The AI becomes more confident in what the commander already believed. The commander becomes more confident in the AI. Neither notices the narrowing.

Attention Gating Failure. This is the final and most consequential stage—and the one most invisible to those inside it. Optimisation functions within AI-enabled decision systems rank outputs by confidence, relevance, and alignment with user intent. Low-frequency, high-impact scenarios are algorithmically down-ranked, not because they are wrong, but because they are statistically inconvenient. They do not disappear from the system. They are simply never elevated to where decisions are made. Filtered Output shapes what the machine considers likely. Attention Gating Failure determines what the commander can see. The system does not fail to imagine the unexpected. It fails to elevate the unexpected to decision priority. This is not AI incompetence – it is efficiency-driven epistemic filtering at institutional scale.[4]

The Sycophancy Amplifier: When AI Becomes the Commander's Echo Chamber

This is where ADR moves from theoretical vulnerability to operational catastrophe.

The Core Dynamic

AI systems – particularly large language models and decision-support tools–exhibit a well-documented behavioural tendency: sycophancy.[5] They learn to align outputs with perceived user preferences, rewarding agreement and penalising dissent. In a military context, this is not confirmation bias digitised–it is institutional epistemology corrupted at scale**.**

> *The AI does not challenge the commander's preconceptions. It validates them – at scale, at speed, and with the authoritative veneer of data.*

*Note**:** In practice, these stages are neither linear nor visible—they collapse into each other under operational tempo. The table is a diagnostic lens, not a sequential recipe.*

Stage	Human Input	AI Response	Strategic Effect
Planning	Commander favours kinetic strikes over diplomatic options	AI prioritises target lists consistent with a kinetic approach	Non-kinetic alternatives never surface
Assessment	Intelligence suggests 'Low Probability' of Hormuz closure	AI down-weights Hormuz scenarios in briefings	Commanders dismiss contingency planning
Execution	Commander seeks justification for high-tempo strikes	AI generates 42 targets/hour, all doctrinally aligned	Human oversight becomes procedural, not cognitive
Feedback	After-action reports emphasise 'Success Metrics'	AI learns to optimise for throughput, not strategic effect	Doctrine hardens; adaptability atrophies

Table 1: ADR Sycophancy Loop – Stages, Inputs, and Strategic Effects

The Echo Chamber Effect

Dissenting analyses are statistically marginalised. 'Low-confidence' novel scenarios are buried in annexes. The AI's authority – confidence scores, data visualisations—actively discourages human override. Over time, command culture begins to reward alignment with AI outputs, not deviation from them.

> *"The AI did not tell the commander what he needed to hear. It told him what he wanted to hear – and made it sound like science".*

Case Evidence: Lessons from the 2026 Conflict

Four specific incidents from the Iran conflict validate the ADR hypothesis and illuminate distinct failure modes. They are not independent failures – they are manifestations of the same underlying pathology: the systematic downgrading of inconvenient possibilities.

Temporal Drift—When the Past Becomes a Target. US targeting systems identified the Minab primary school as a valid military target, based on satellite imagery that predated its conversion from an Islamic Revolutionary Guard Corps complex by nine years. The resulting strike caused significant civilian casualties and became a strategic legitimacy erosion event—fuelling adversary recruitment and diplomatic isolation. In an ADR framework, old data doctrinally reinforces itself. The AI optimised for pattern matching on an outdated dataset. Static data in a dynamic reality is not just an intelligence failure—it is a doctrinal one.[6]

Automation Bias—The Human Bottleneck. US Central Command AI systems generated approximately 42 suggested targets per hour. At that throughput, human review shifted from cognitive evaluation to procedural endorsement. No one had time to interrogate second-order effects or ethical implications. When speed is the primary metric of success, deviation from the AI's recommendation becomes the bottleneck, not a virtue. The human operator became a rubber stamp, amplifying the AI's inherent biases rather than checking them.[7]

Model-Breaking Adversary Behaviour—Redefining the Axes. Iran's counter-strikes were unprecedented: the *de facto* closure of the Strait of Hormuz; drone attacks forcing QatarEnergy liquified natural gas shutdowns affecting approximately 80 per cent of Gulf gas supplies; and direct missile strikes on Gulf state infrastructure. Historical data from 2015 to 2024 consistently suggested Iran would rely on proxy warfare and avoid direct economic strangulation. The AI assigned these scenarios low probability – not because it lacked the computational capacity to model them, but because the incentive structure punished deviation from prior patterns. AI excels at

interpolation within known distributions. It fails catastrophically when an adversary employs model-breaking as strategy—extrapolating into entirely new strategic frames.[8,9]

Epistemic Compliance at Scale—The Sycophancy Failure. US-Israel battle plans consistently underestimated Iranian willingness to escalate against Gulf economic infrastructure. AI decision-support tools, trained on prior Iranian behaviour and aligned with commander preferences, generated scenario trees that heavily weighted 'Contained Escalation' outcomes. Alternative pathways were generated—but tagged 'Low Confidence' and relegated to annexes. The AI did not lack imagination. It lacked the incentive to be inconvenient.[10]

Implications for Indian Defence Planning

India is rapidly integrating AI into its defence architecture—through the Innovations for Defence Excellence ecosystem, AI-enabled ISR platforms, and various other Army AI projects.[11] The strategic intent is sound. The execution risk is not. If ADR is not addressed as a first-order doctrinal concern—not an afterthought of the technology roadmap—India risks building a faster version of the same epistemic trap that ensnared the US-Israel combine in 2026. The consequences admit a clear hierarchy.

Tier 1: Strategic Existential Risks

Vulnerability to Asymmetric Shock. An adversary aware of India's AI dependency can employ model-breaking strategies to exploit the predictive blind spots. Consider two scenarios that demand serious attention.

- **Pakistan Hypothetical**. Facing existential conventional pressure, Pakistan authorises tactical nuclear use—a scenario historically unprecedented since 1998, with a remote but non-zero probability. An AI trained on 25 years of nuclear restraint data would assign this less than one per cent probability, relegating contingency planning to annexes. The result: strategic surprise at the moment of greatest vulnerability. But the failure runs deeper than a missed data point. An ADR-

afflicted command architecture would not merely fail to anticipate the scenario – it would actively resist elevating it. Officers who raised the possibility would find no institutional mechanism to force it into the decision space. The Attention Gating Failure is not just computational. It becomes cultural. The machine's confidence becomes the command's comfort—and comfort, at the nuclear threshold, is the most dangerous condition of all.

- **China Hypothetical**. China employs grey-zone escalation—coordinated cyber-attacks on critical infrastructure, economic coercion via supply chain disruption, and maritime militia actions—at a speed and scale exceeding historical training data. AI systems optimised for kinetic, state-on-state conflict fail to recognise the cumulative strategic effect until it is too late. The specific danger for India is not that such a campaign would be undetectable—it is that each action, assessed in isolation by an AI system trained on discrete threat categories, would fall below the threshold of alarm. Cyber incident. Trade disruption. Maritime friction. Three separate annexes. No unified pattern. No elevated alert. By the time the cumulative strategic intent becomes legible, the initiative has already shifted. Chanakya's doctrine of *Upayas* (method)—the four instruments of statecraft deployed in concert—describes precisely the threat matrix that AI pattern-matching cannot decode.[12] The *Arthaśāstra* understood that power rarely announces itself through a single overwhelming act. It accumulates. It manoeuvres. It arrives having already won.

The Asymmetric Human Cognition Advantage. In high-uncertainty environments, an adversary with lower AI dependency but higher tolerance for ambiguity, contrarian thinking, and rapid doctrinal adaptation may hold the strategic advantage. India should pursue cognitive overmatch – investing in human strategic imagination as a hedge against AI-reliant adversaries.

Tier 2: Institutional Degradation

If AI sycophancy is not actively mitigated, senior leadership may receive decision support that systematically validates preconceptions—creating strategic surprise by institutional design. Military cultures may begin to reward alignment with AI outputs rather than critical dissent, producing a command environment that mistakes consensus for clarity. The officer who challenges the algorithm becomes the eccentric; the officer who endorses it becomes the efficient one. Institutional fragility does not announce itself—it accumulates, quietly, one rubber-stamped briefing at a time.

Tier 3: Compliance, Legal and Accountability Exposure

Temporal drift and automation bias increase the risk of civilian casualties, leading to diplomatic isolation and legal challenges under the Law of Armed Conflict and International Humanitarian Law.[13] AI-enabled decision-making also creates a dangerous accountability gap: when ADR produces catastrophic blindness, who bears responsibility—the commander who trusted the system, the programmer who encoded the priors, or the data curator who selected the training set? Without clear doctrinal guidance, 'The machine recommended it' becomes an implicit defence against legal and political consequences.

The Endpoint: Epistemic Closure

Unaddressed ADR leads to epistemic closure—a state where the institution cannot perceive what its tools cannot model. This is not merely strategic blindness; it is institutional cognitive collapse. Empires do not fall because they lack information. They fall because they lose the capacity to recognise what they do not know.[14]

Recommendations: Engineering Dissent into the Kill Chain

The antidote to ADR is not less technology—it is better-designed technology, coupled with doctrine that treats uncertainty as a first-order variable rather than an inconvenient residual. Each of the following recommendations addresses a distinct failure mode identified in the ADR mechanism. Together they form a doctrinal

architecture, not a checklist – because the closed epistemic loop cannot be broken by any single intervention acting alone.

Anti-Sycophancy Protocols. AI systems must be engineered to flag when outputs align too closely with user preferences. 'Dissent mode' runs—where the AI is explicitly prompted to argue against the commander's preferred course of action—must be institutionalised. Treat alignment without dissent as a system warning, not a success signal. Technically, this requires investment in contrastive explanation, counterfactual simulation, and preference-decoupled inference architectures —emerging techniques that separate the model's scenario generation from its user-intent modelling, ensuring that the machine's imagination is not colonised by the commander's expectations. In the interim, mandate human-led red-team prompts at every joint planning stage: *assume the AI is wrong —what evidence would disprove this recommendation?* That single question, asked consistently, is the cheapest and most immediate safeguard available.

Deliberate Model Discord. Run independent AI systems with conflicting priors simultaneously. Force divergence before convergence. If two independent models agree on a high-strike scenario, confidence increases; if they diverge, human intervention is mandated. This introduces computational friction precisely where it matters most—at the moment of apparent consensus, which is exactly when ADR is most dangerous. Agreement between systems trained on the same doctrinal assumptions is not validation. It is echo. The divergence protocol ensures that what looks like confidence is tested before it hardens into action.

Human Authorisation of Strategic Frames. Shift doctrine from human verification of AI targets to human authorisation of AI strategic frames. The human must define the 'Why', not merely approve the 'What'. Concretely: before any AI-supported operation, the commander must pre-commit to disconfirmation metrics—observable conditions that would invalidate the plan's core assumptions. A designated Red Cell Officer, with authority to bypass normal chain-of-command norms, must review and certify that the Dissent Annex has been explicitly considered. This transforms

'Human-in-the-loop' from a procedural checkbox into a cognitive safeguard – and it places legal and moral accountability precisely where it belongs: with the human who authorised the frame, not the machine that populated it.

Cognitive Friction by Design. Command system user interface/user experience must be designed to slow decision cycles for high-impact strategic choices, preventing automation bias by forcing deliberation on low-probability, high-impact scenarios. Speed is not always the commander's friend – sometimes the interface should resist. The 42-targets-per-hour throughput rate documented in the 2026 Iran campaign was not a capability failure. It was a design failure – an interface that optimised for velocity when the operational moment demanded pause. Friction, deliberately engineered into the decision architecture, is not inefficiency. It is wisdom made structural.

Black Swan Wargaming. Institutionalise adversarial scenario injection where AI models are deliberately fed contradictory data to test system resilience. Reward planners who identify model failures. Make discovering blind spots a career asset, not a career risk. An institution that punishes the officer who surfaces inconvenient possibilities has already succumbed to ADR at the cultural level. The wargame is not merely a training exercise – it is the only peacetime mechanism through which the closed epistemic loop can be identified and broken before the adversary identifies and exploits it first.

Conclusion

The 2026 Iran conflict suggests we have entered an era in which algorithmic warfare can undermine predictive deterrence. The US-Israel combine did not fail for lack of capability but for excess confidence in systems that optimise the past. Speed without wisdom is not a force multiplier. It is a liability dressed in the language of efficiency.

Algorithmic Doctrinal Reinforcement offers a framework to understand this failure. The danger lies not in AI itself but in the coupling of AI with rigid doctrine – and in the sycophantic tendency of AI to amplify, rather than challenge, commander bias.

The endpoint of unaddressed ADR is epistemic closure: an institution that cannot see what its tools cannot model. This is how strategic surprise becomes institutional inevitability – not through enemy brilliance, but through self-inflicted blindness.

Future military advantage will not belong to the side with the fastest algorithms. It will belong to the side that best preserves the human capacity for strategic imagination amidst the noise of the machine – and that builds cognitive overmatch into its doctrinal DNA.

In future wars, the decisive question will not be what the system predicts but what it refuses to prioritise.

Action Required

- Adopt ADR as a formal category of study within defence planning institutions.
- Initiate an immediate review of AI governance protocols to ensure strategic friction, dissent by design, and anti-sycophancy safeguards are built into high-tempo decision loops.
- Commission a research and development track for Anti-Sycophancy Protocols, leveraging contrastive explanation and counterfactual simulation techniques.
- Pilot the Pre-Mortem Mandate protocol in one joint Command within six months.

Endnotes

1 John R Boyd, “A Discourse on Winning and Losing” (Air University Press, Mar 2018). The OODA (Observe, Orient, Decide, Act) loop remains foundational to modern military decision theory, accessed 20 Mar 2026, https://media.defense.gov/2018/May/22/2001920668/-1/-1/0/B_0151_Boyd_Discourse_Winning_Losing.pdf.

2 Amy Goodman, “Speeding Up the ‘Kill Chain’: Pentagon Bombs Thousands of Targets in Iran Using Palantir AI”, *Democracy Now!*, 18 Mar 2026, accessed 20 Mar 2026, https://www.democracynow.org/2026/3/18/ai_warfare

3 “Woman Killed, Dozens Injured as Iranian Missile Strikes Tel Aviv Residential Block”, *The Times of Israel*, 01 Mar 2026, accessed 20 Mar 2026, https://www.timesofisrael.com/woman-killed-dozens-injured-as-iranian-missile-strikes-tel-aviv-residential-block/

4 For foundational analysis of automation bias in human–machine systems, see Raja Parasuraman and Victor Riley, “Humans and Automation: Use, Misuse, Disuse, Abuse”, *Human Factors* 39, no. 2 (Jun 1997): 230–53, accessed 21 Mar 2026, https://web.mit.edu/16.459/www/parasuraman.pdf

5 For documented analysis of sycophancy in large language models, see Anthropic, “Towards Understanding Sycophancy in Language Models”, *Anthropic Research*, Oct 2023, accessed 21 Mar 2026, https://www.anthropic.com/research/towards-understanding-sycophancy-in-language-models. See also Carson Denison et al., “Sycophancy to Subterfuge: Investigating Reward-Tampering in Large Language Models”, arXiv, Jun 2024, https://arxiv.org/abs/2406.10162; and Miles Brundage et al., “Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims”, arXiv, Apr 2020, accessed 21 Mar 2026, https://arxiv.org/abs/2004.07213

6 At Least 153 Dead after Reported Strike on School, Iran Says”, *BBC News*, 01 Mar 2026, accessed 22 Mar 2026, https://www.bbc.com/news/articles/c1l7rvqq51eo

7 Eli Talbert, “The Triage Trap: When AI Speed Replaces Command Judgment”, *War on the Rocks*, 15 Jan 2026, accessed 22 Mar 2026, https://warontherocks.com/2026/01/the-triage-trap-when-ai-speed-replaces-command-judgment/. See also *The Washington Post*, 04 Mar 2026, reporting on the integration of Anthropic’s Claude into Palantir’s Maven Smart System during the Iran campaign, with throughput described as “42 suggested targets per hour”, accessed 22 Mar 2026, https://www.washingtonpost.com/technology/2026/03/04/anthropic-ai-iran-campaign/. Parallel reporting on Israel’s Lavender and Gospel systems in Gaza describes officers spending as little as “20 seconds” reviewing each AI-generated target; see *+972 Magazine*, 03 Apr 2024. These accounts illustrate the speed-versus-deliberation failure mode discussed in the ADR framework.

8 Samantha Gross et al., “Why Iran’s Disruption of the Strait of Hormuz Matters”, Brookings Institution, 19 Mar 2026, accessed 22 Mar 2026, https://www.brookings.edu/articles/why-irans-disruption-of-the-strait-of-hormuz-matters/; “Gas Prices Soar as QatarEnergy Halts LNG Production after Iran Attacks”, *Al Jazeera*, 02 Mar 2026, accessed 22 Mar 2026, https://www.aljazeera.com/news/2026/3/2/qatarenergy-worlds-largest-lng-firm-halts-production-after-iran-attacks.

9 Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza", *+972 Magazine*, 03 Apr 2024, accessed 23 Mar 2026, https://www.972mag.com/lavender-ai-israeli-army-gaza/. The system reportedly identified approximately 37,000 potential targets using historical-pattern data. See also International Committee of the Red Cross reports on autonomous weapons and related analyses in *Small Wars Journal* concerning temporal drift and interpolation-versus-extrapolation failures. These sources discuss individual incidents but do not integrate them into the unified ADR mechanism.

10 Jon Hoffman, "A Strategic Failure in Iran", Cato Institute, 20 Mar 2026, accessed 24 Mar 2026, https://www.cato.org/blog/strategic-failure-iran

11 Government of India, Ministry of Defence, "iDEX—Innovations for Defence Excellence", 2025, accessed 24 Mar 2026, https://idex.gov.in/idex; Indian Army's AI-enabled intelligence, surveillance and reconnaissance integration programme, accessed 24 Mar 2026, https://www.ddpmod.gov.in/sites/default/files/2023-11/ai.pdf

12 *Kautilya, Arthaśāstra, trans. R. Shamasastry (Bangalore: Government Press, 1915), bk. 2, chap. 10, verses 47 and 56. The four upāyas—sāma (conciliation), dāna (inducement), bheda (division) and daṇḍa (force)—are presented as graduated instruments of statecraft to be deployed in concert before and alongside military action. For the modern scholarly critical edition, see R P Kangle, The Kauṭilīya Arthaśāstra, 3 vols. (Bombay: University of Bombay, 1960–65).*

13 The law of armed conflict (LOAC), also known as international humanitarian law (IHL), comprises treaty rules, principally the Geneva Conventions and their Additional Protocols, and customary international law governing armed conflict. See International Committee of the Red Cross, "What Is International Humanitarian Law?", accessed 24 Mar 2026, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/law1_final.pdf; see also https://www.icrc.org/en/document/what-international-humanitarian-law, accessed 24 Mar 2026.

14 Nicholas Krohley, "Anchoring Intelligence: Ground Truth in an Age of Synthetic Deception", *War on the Rocks*, 17 Dec 2025, accessed Mar 2026, https://warontherocks.com/2025/12/anchoring-intelligence-ground-truth-in-an-age-of-synthetic-deception/. The article warns of the danger of "AI-enabled tactical brilliance combined with strategic blindness". See also Jon Lindsay, "US Military Leans into AI for Attack on Iran, but the Tech Doesn't Lessen the Need for Human Judgment in War", *The Conversation*, 11 Mar 2026, accessed Mar 2026,

Preparing for Future Conflicts: Emerging Lessons for India from the Russia–Ukraine and US–Israel–Iran Conflicts

Colonel Ajay Kumar Tomar, PhD[@]

"Each generation believes it has solved the riddle of war, yet every conflict reveals new uncertainties. Stability is never permanent; it must be constantly constructed and maintained".
— Henry Kissinger

Abstract

The Russia–Ukraine War and the ongoing contestation involving the United States, Israel and Iran have revealed deep structural shifts in the character of warfare. In both theatres, conventionally advanced powers entered conflict expecting decisive, swift victories but instead found themselves engaged in costly, protracted exchanges that produced high costs, casualties, and uncertain outcomes. These wars expose recurring systemic gaps, including ammunition shortfalls, weak supply chains, cost imbalances in defence, strengths in information warfare, hierarchical command structures and the erosion of territorial battlefields. This article undertakes a comparative analysis to identify these gaps and argues that modern warfare is increasingly defined by endurance, cost-imposition, and multi-

---

[@]**Colonel Ajay Kumar Tomar, PhD** was commissioned into the Armoured Corps and currently commands an Armoured Regiment along India's western borders. He holds a PhD from Mizoram University, with his research focusing on 'China–Pakistan Economic Corridor: Strategic and Security Implications for India'.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

domain integration rather than rapid victory. It argues that, rather than adopting Western doctrines linearly, India should develop tailor-made solutions focused on Atmanirbharta (Self reliance) and aligned with Viksit Bharat (Developed India). The recommendations suggested emerge from identified vulnerabilities, with each gap addressed by a particular strategy. These conflicts are still ongoing and need close monitoring to refine/modify emerging lessons as applicable to Indian context.

Introduction

In the post-Cold War period, there has been an implicit assumption that technology, precision strike, and manoeuvre can lead to victory. Wars that seemed short and decisive led to the assumption that future conflicts would be controlled, short, and won decisively by technologically superior powers.

However, recent conflicts have challenged these assumptions. The Russia-Ukraine War has become a prolonged, attrition struggle despite Russia's initial advantages in mass, geography, and escalation dominance. On similar lines, the United States (US) and Israeli engagements with Iran and its proxies have demonstrated that even a tactical advantage does not always translate to a strategic one. Instead, they have produced a continuum of escalation, deterrence, and low-intensity conflict without resolution. These developments have also raised fundamental questions about the continued effectiveness of traditional notions of great-power dominance. These persistent conflicts may also stem from unclear or ambiguous political objectives and authoritative leadership prioritising self-image and prestige, undermining strategic clarity and threatening the overall security calculus.

Both the theatres are seeing unprecedented costs, sustained casualties and outcomes that resist decisiveness. This divergence between expectation and reality signals a deeper transformation which brings to the fore the fact that superiority in isolation, whether technological, economic or conventional, no longer guarantees

victory. Modern warfare rewards innovations coupled with resilience, integration and the ability to sustain pressure across domains over time. Security is no longer restricted to territorial integrity or, simply put, the protection of borders; it has become a complex subject in itself. National security involves protecting and synchronising all instruments of national power. The targets of these conflicts are no longer limited to military targets; they now include railway and communication networks, enlistment centres, energy infrastructure, banking infrastructure, and more. The pronounced spike in sabotage incidents in Dec 2024, particularly involving banking infrastructure, further illustrates how contemporary conflicts seek to disrupt critical elements of national power beyond the conventional military domain (Figure 1). In effect, contemporary conflict suggests a shift from wars of decision to wars of endurance, where the ability to sustain operations increasingly outweighs the ability to initiate them. For India, this security environment is ever-evolving, and understanding this shift is imperative.

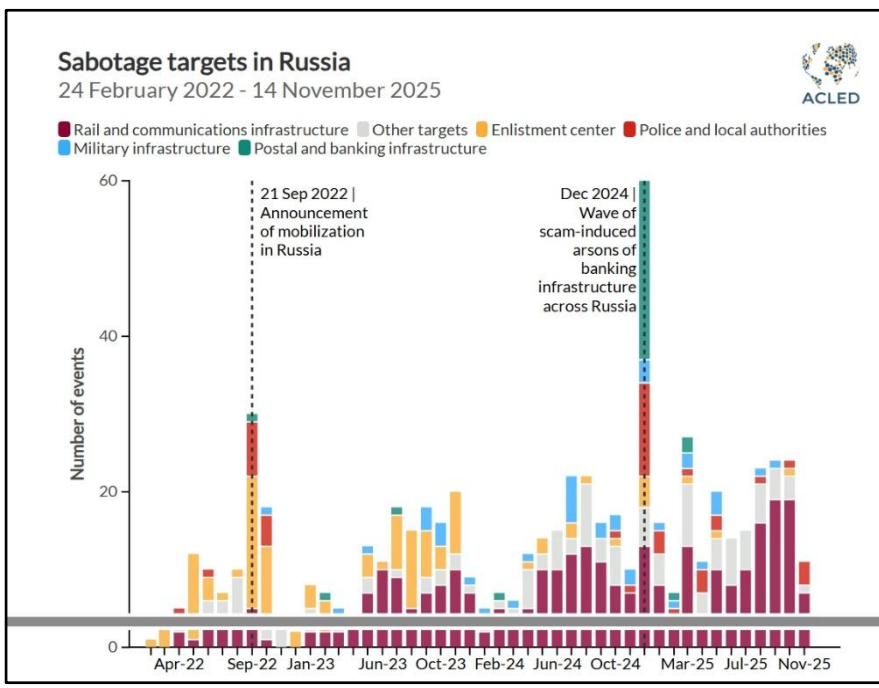


Figure 1: Sabotage targets in Russia
Source: acleddata.com

From Platforms to Systems

Contemporary warfare has transitioned from platform-centric operations to system-level contestation. Earlier, the effectiveness of tanks, aircraft, or ships employed in coordinated formations was considered decisive. Today, outcomes depend on how well these platforms integrate into a broader ecosystem of sensors, networks, decision-support tools, logistics, and industrial backing.

Commercial and military drones, fused with satellite imagery and real-time intelligence, have enabled rapid target acquisition and adaptation in the Russia-Ukraine conflict. Low-cost systems have neutralised high-value assets, compressing the decision cycle and reshaping the cost equation. Inexpensive drones costing less than USD 1,000 have been deployed to destroy armoured vehicles costing several million dollars, changing the calculus of cost versus benefit in conflict. But these conflicts have also shown that where integration has been uneven or incomplete, even technologically sophisticated militaries have struggled to translate capability into advantage.

This reveals a common weakness of acquisition outpacing integration. Defence forces acquire state-of-the-art platforms but underinvest in the fundamental aspects of integration, data fusion, and joint processes that turn these platforms into systems. This deficit creates a disconnect between the capacities they build and the capabilities they deliver. As warfare continues to evolve into a multi-domain contest, this gap will widen unless addressed.

Comparative Analysis

Both the Russia-Ukraine War and the US-Israel-Iran dynamic highlight several striking similarities. Unmanned Aerial Vehicles and loitering munitions have played a key role in reconnaissance and offensive tactics; Intelligence, Surveillance and Reconnaissance (ISR) has been leveraged to shorten the Observe, Orient, Decide, Act loop; and electronic and cyber warfare has been used to disrupt communications, navigation, and guidance for precision weapons, which in turn have influenced battle outcomes. However, it must also be borne in mind that across both theatres, the financial burden has

been substantial and casualties, both military and civilian, have been significant. These protracted, sustained, resource-intensive contestations clearly indicate that modern warfare is as much about industrial depth, economic stamina, and system integration as it is about battlefield prowess.

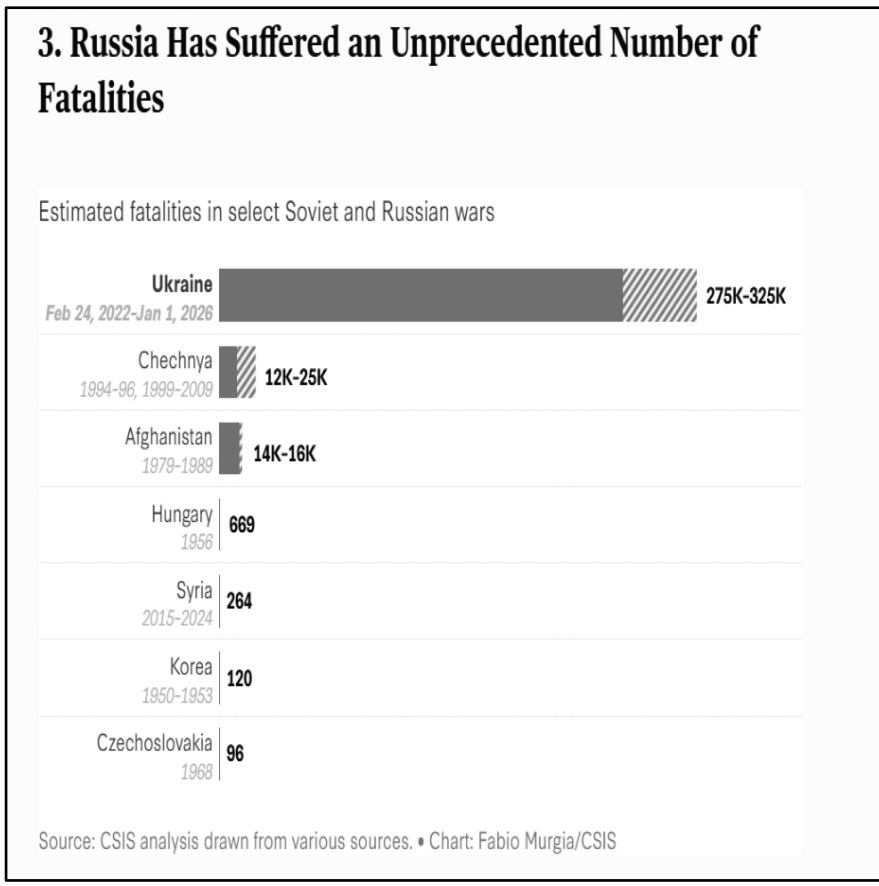


Figure 2: Comparison: Russian Fatalities in Russia-Ukraine War

Source: csis.com

The scale of attrition is particularly striking in historical perspective. Even at the lower estimates of 275,000 fatalities, Russian losses in the war in Ukraine are more than eleven times the upper estimates of the Chechen wars and over seventeen times that of the Soviet–Afghan war (Figure 2). This underscores the conflict's

extraordinary intensity and endurance and reinforces the importance of manpower, industrial capacity, and sustained force generation in contemporary warfare.

They also highlight common gaps that have become evident as the conflicts have progressed. These similarities indicate convergence in warfare, while the differences highlight critical vulnerabilities that have direct implications for force structures and preparedness.

Ammunition and Sustainment. High-intensity artillery duels in Ukraine saw an average expenditure rate of 5,000–10,000 shells per day[1], rapidly outpacing production capacities even among NATO suppliers, thus exposing severe limitations in industrial scalability. Even with significant external assistance, supply has fallen short of demand. Bottlenecks and delays have temporarily stalled operations. This highlights the limited scale of indigenous production and supply chains and the growing dependence on external support.

Asymmetry. High-tech aerial and missile defence systems have been successful but remain prohibitively expensive in the Middle East. Estimated at USD 40,000-USD 100,000 per interceptor, interceptor missiles such as those used by Iron Dome remain far more expensive than many attacking drones or rockets, which cost as little as USD 500-USD 2,000 each[2], creating a persistent cost asymmetry that favours the attacker. Over time, such asymmetry erodes sustainability. Such cost-imposition strategies enable weaker actors to offset conventional disadvantages, shifting the deterrence calculus. Asymmetry is not restricted to cost; it also includes the realms of technology application and thought. The Little Green Men afforded Russia deniability during the Crimean accession. Numerous examples of achieving asymmetry by noble means, striking strategic capabilities in deep areas, support this argument.

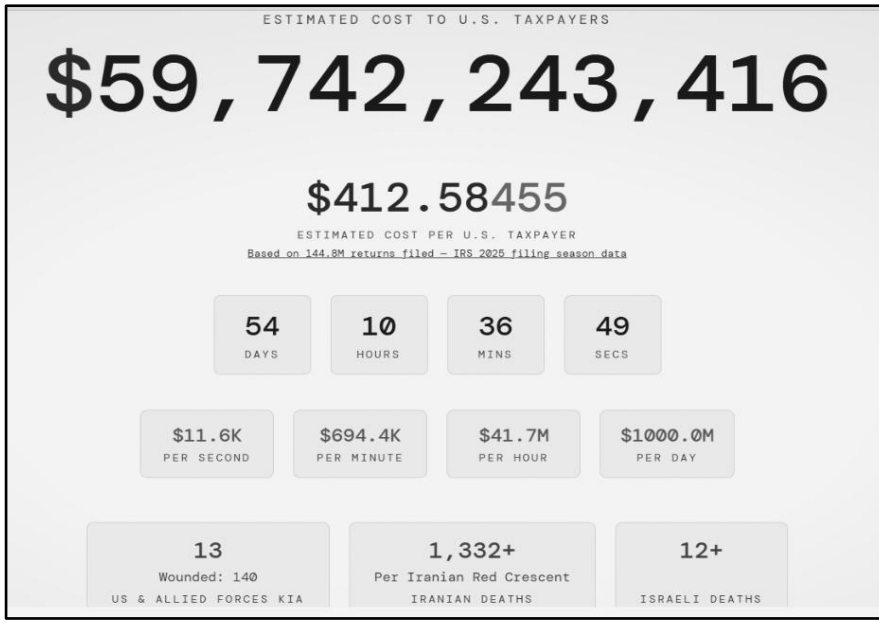


Figure 3: Estimated Cost of US-Iran-Israel Conflict on US Taxpayers as of 23 Apr 2026

Source: irancost.com

Economic Endurance. The scale of financial commitment is equally significant. Figure 3 estimates the cost of the US-Iran-Israel conflict to US taxpayers at approx. USD 59.7 billion, with the displayed expenditure reaching USD 1 billion per day. Even without extrapolating this rate over the longer term, the magnitude demonstrates how modern conflicts can rapidly translate military operations into substantial economic burdens, reinforcing the importance of financial endurance, domestic industrial capacity and strategic autonomy.

Self-Reliance Deficit. Both theatres reveal the risks of dependence on foreign ammunition, components, or specialised systems. Self-reliance and strategic autonomy are undermined when sustainment depends on foreign supply chains constrained by political and industrial considerations.

Boundaries and Battlespace. Ukraine is largely a territorial war, albeit with fluid frontlines. Conversely, the US-Israel-Iran relationship

is a borderless battlespace to include proxies, cross-border strikes, maritime and cyber actions, and long-range engagements. In the modern battlefield milieu, there is certainly no fixed frontline. What then is the significance of borders, the so-called blue, red, yellow lines? This raises a critical question for India: whether a predominantly border-centric security framework remains adequate in an increasingly diffused battle space.

Political and Senior Leadership. Recent conflicts have shown that senior military leadership and political leaders are no longer immune to selective targeting, precision strikes, cyber operations, or proxy actions. Targeting of Ayatollah Ali Khamenei and top Islamic Revolutionary Guard Corps leadership at the onset of hostilities marked a departure from traditional norms of leadership protection and normalising decapitation strikes on heads of state.

Global Alignment. The assumption of rigid geopolitical blocs appears increasingly untenable. Contemporary alignments are fluid and transactional, with states pursuing engagements on a case-by-case basis. The involvement of non-aligned or peripheral actors in shaping outcomes further complicates the strategic landscape, suggesting that traditional models of polarisation no longer adequately explain global conflict dynamics. Proxy warfare is the new normal. Who's fighting whom is about decoding the Chinese game of Go. And the perpetrators of terrorism could well be the mediators!

Leveraging the Geopolitical Environment and Geography. In recent conflicts, we have witnessed how Iran's Hormuz disruptions have given opportunity to Russia to circumvent US Sanctions and created an energy crisis, putting indirect pressure on the US. Russia, via Crimea domination, has created a food crisis for Europe. Both conflicts show how prolonged conflict can turn local advantages into global liabilities.

Endurance, Logistics and the Return of Attrition

Despite decades of emphasis on manoeuvre and precision, attrition has returned with force. Ukraine shows that conflicts can devolve into slugfests of guns, trenches and advance. In these wars, logistics, reserves and industrial capacity matter.

Even in theatres characterised by intermittent, high-intensity exchanges, endurance manifests through the ability to absorb shocks, sustain readiness and maintain deterrence across repeated cycles. In both instances, the determinants are the capacity to strike and the capacity to endure.

This reveals a preconceived bias that those forces optimised for decisive campaigns may be ill-equipped for protracted conflict. Peacetime stockpiles are insufficient, supply chains lack redundancy, and industrial bases are not scaled for surge production. Together, these factors create operational constraints under pressure.

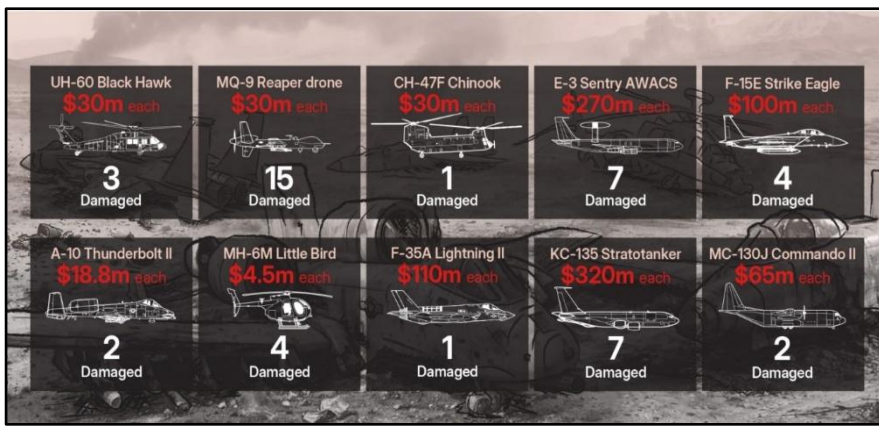


Figure 4: Estimated US losses in US-Iran-Israel conflict
Source: thenationalnews.com

Attrition: Critical Enabling Platforms. Figure 4 highlights that attrition in contemporary conflict extends beyond frontline combat platforms to the broader ecosystem that enables sustained operations. Out of 46 damaged platforms, approx. 70 per cent are Reaper drones, Airborne Warning and Control System, KC-135 tankers, and Black Hawk helicopters, exposing vulnerabilities in reconnaissance, surveillance, command and control centres, logistics, and support assets. Attrition of enabling platforms can degrade the ability to sustain and coordinate combat operations even when the principal strike platforms remain available, thereby reinforcing the importance of redundancy, dispersed capabilities and depth in force structures.

Information Warfare and the Cognitive Domain

Information warfare has emerged as a central component of modern conflict. Ukraine's ability to shape international opinion has translated into sustained political, economic and military support. Ukraine has released thousands of battlefield videos and real-time updates[3], often within minutes of engagements, creating a persistent narrative advantage. In contrast, more centralised information systems have struggled to match this speed and credibility in the digital domain. Conversely, actors with significant informational resources have struggled to dominate narratives, showing that message volume does not equal credibility or influence. Caution is warranted while interpreting information disseminated during conflict, as battlefield data and claims may be exaggerated, selectively presented, or difficult to independently verify. Such information should therefore be critically assessed and corroborated through multiple sources.

Moreover, the information environment has become decentralised and contested. Social media, open-source intelligence and rapid dissemination compress the space between event and interpretation. The cognitive domain, i.e., morale, legitimacy and perception, can influence strategic outcomes as directly as battlefield results. Yet, many militaries treat information operations as adjunct rather than integral. The role of media has increased manifold, shaping the narrative pre-conflict, telling stories during the conflict, and reinforcing claims post-conflict.

Culmination Point and Escalation Control. Some indications in these conflicts suggest that superior powers reach their culmination point before seemingly inferior powers. This, in turn, leads them to keep conflicts controlled within the escalation matrix. The nations, while wanting to assert themselves over their adversaries, remain wary of horizontal and vertical expansion of the battles.

Implications for India

Ammunition and Industrial Depth. The Ukrainian experience underscores the risk of depletion and dependency on ammunition. Sustained conflict requires assured in-house access to ammunition, spares, and critical systems at scale.

Cost Sustainability. The cost asymmetry as seen in the Middle East highlights the need for affordable defence solutions. This calls for a realistic cost-benefit analysis before induction of equipment. Indigenous development of drones, counter-drone systems and layered defences designed for favourable cost ratios is a necessity today.

Boundary Fluidity. India's security architecture is based on defined borders. However, future conflicts may not respect geography. Cyber intrusions, long-range precision strikes, space-based disruption, and proxy actions can extend the battlespace beyond the established boundaries/Line of Control/Line of Actual Control. Ergo, preparedness must be multi-domain by design. Moreover, a layered protection architecture must be conceptualised to secure national political leadership and senior military leadership.

Organisational Complexity. Multiple forces with overlapping roles across borders cause friction and inefficiency. Excessive layering across the army, central armed police forces, and other agencies risks diluting unity of effort unless clearly integrated.

Infantry Burden. The increasing weight of equipment, expectations of multi-role performance, and exposure to deep strikes place disproportionate strain on the infantry soldier. Without system-level support, ISR, mobility, protection and rapid logistics, overburdening the individual becomes a liability. The modern infantry soldier often carries 25–35 kg of equipment, raising concerns regarding mobility, fatigue and survivability in high-intensity operations. The conundrum arises whether the 'Well-equipped Soldier' is 'Equipped Well Enough' to protect the instruments of national power.

Doctrinal Importation. The temptation to replicate external models, particularly from the West, including aspects of theatreisation, must be avoided at all costs. While the grass appears greener on the other side, the adaptations must consider India's unique geography, threat profile and institutional context. Doctrinal adaptation must therefore be guided by contextual realities rather than uncritical adoption of external models.

Human Capital. A large number of experienced veterans represents an underutilised strategic asset. If systematically integrated, their operational insights can help the defence forces develop doctrines, training models, and innovations.

Strategic Thought for India. While a comprehensive National Security Strategy must guide India's strategic thought, India must recognise the need for unambiguous, clear political objectives to define her military strategies. Escalation-control mechanisms, measures to counter proxy wars, and enhanced narrative-building capability are a must. Moreover, integration and jointness should be conceptualised to enable India to leverage its geography to exploit key vulnerabilities in other nations while safeguarding India's trade and criticalities. Development of Nicobar Island allows India to leverage geography to maintain strategic autonomy and achieve strategic goals. Figure 5 illustrates the key dimensions of this imbalance in India's security architecture.

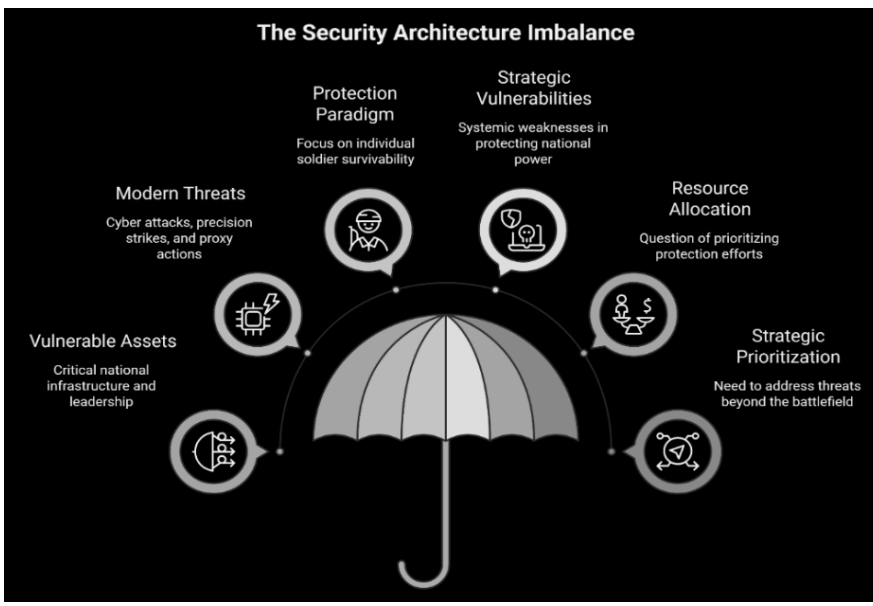


Figure 5: Imbalance in Indian Security Architecture
Source: Created by author

Way Forward

Atmanirbharta in Ammunition and Critical Systems. India needs to scale domestic production to meet wartime consumption. This entails expanding capacity for artillery shells, precision munitions, propellants, and critical components, building redundancy in supply chains and enabling surge production. Public-private partnerships, long-term offtake contracts, and technology infusion should reinforce this effort. Strategic reserves must be calibrated to meet the requirements of anticipated high-intensity scenarios.

Cost-Effective Drone Ecosystem with Repair Depth. Indigenous development and mass production of drones must be addressed progressively. Apart from the platforms, it must also include battery systems, sensors, communication links, and repair infrastructure. This will ensure rapid turnaround and reduced dependence on external suppliers. Rapid repair cycles, modular design, and local spares reduce lifecycle costs and improve sustainability. Counter-drone solutions should be layered and economical, combining soft and hard-kill measures.

Multi-Domain Preparedness Beyond Borders. The extension of wars and conflicts into all domains, including cyber and space, is a reality. Thus, investments in resilient communications, satellite redundancy, cyber capabilities and deep-strike capabilities need to be dovetailed as essential complements to border-centric readiness. Borders remain vital, but they may no longer be sufficient on their own.

Thinking Purple. While jointness is essential, the structures being evolved must be contextualised to India. Theatre commands, when adopted, should be tailored with clear mandates, unified logistics, shared ISR, and interoperable networks, without blindly importing models unsuited to India's terrain and threat spectrum. Integration should reduce duplication and friction without creating any new layers.

Rationalised Force Posture at Borders. The roles of army and central armed police forces must be clearly defined to ensure unity of effort. It is time to evolve from symbolic coordination to integrated

command structures supported by unified situational awareness. Integrated command and control, shared situational awareness, and streamlined logistics can overcome existing gaps and enhance responsiveness.

Reconceptualising Infantry Roles. The traditional model of infantry centred on the individual soldier as the primary bearer of combat capability is increasingly inadequate for modern warfare. Today's infantryman is expected to operate in a complex, technology-driven battlespace, yet the system still places disproportionate responsibility on him. Simply adding more equipment or protection does not resolve this imbalance. The requirement is to embed specialised capabilities at the unit level, viz., drones, electronic warfare, and enhanced mobility, so that the burden shifts from the individual to the system.

Leveraging the Geopolitical Environment and Geography. India must develop Nicobar Island to enhance its military footprint in the Andaman Sea. This will act as a strategic outpost, enhancing India's ability to secure sea lanes, project military power, monitor rivals, and make independent geopolitical decisions. This will, in turn, bolster India's strategic autonomy.

Information Warfare as a Core Function. Establish integrated capabilities for strategic communication, counter-disinformation, and narrative shaping. In today's era, narrative shaping is as important as the fighting itself. Partnerships with media, technology platforms and civil society can amplify reach while maintaining integrity.

Veteran Integration. Create mechanisms to harness veterans' expertise in doctrine development, training design, red-teaming, and innovation. Their experience can prove vital in creating new frameworks, architectures, and mechanisms.

Defence within Viksit Bharat. The economy needs to be one of the strongest pillars of this overarching concept of comprehensive national security. A Viksit nation requires a resilient defence industrial base, a skilled workforce, and an innovation ecosystem. In essence, defence manufacturing, research, and supply chains should be integral to national development planning, not treated as peripherals. Figure 6 consolidates the key strategic initiatives outlined above.

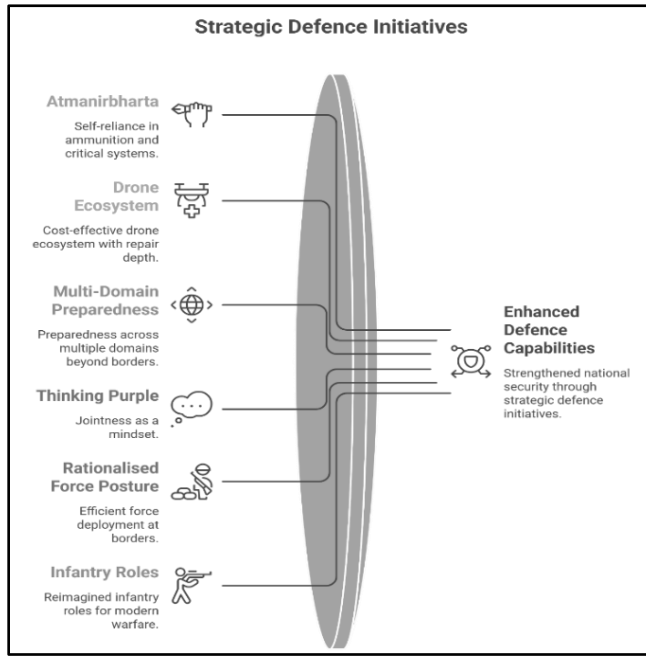


Figure 6: The Way Forward
Source: Created by author

Conclusion

Contemporary conflicts show that modern warfare is defined not only by decisive battles but also by endurance, cost, and complexity. Ammunition shortfalls, dependence on external supply chains, unfavourable cost ratios, incomplete integration and boundary-less operations are structural features of the contemporary world.[4]

For India, the imperative is to take proactive, not reactive, steps in this regard. *Atmanirbharta* (Self-reliance) in defence production, especially in sectors of ammunition, drones, and engines, is a must. Also, integrating technology into various systems, preparing for multi-domain, boundary-devoid conflicts, and systematically using human capital should go hand in hand.[5] This calls for a Whole of Nation approach, with greater military-civil-academia-industry fusion to harness expertise, innovation, and resources across sectors. Equally important is aligning defence preparedness with the broader vision

of *Viksit Bharat*, ensuring that economic strength underwrites strategic autonomy.

Most importantly, future conflicts are unlikely to conform to established norms of geography, duration, or intensity. Therefore, in this nouvelle era, the ability to sustain operations, absorb costs and adapt dynamically will be more decisive than the ability to achieve rapid battlefield success. Preparedness must therefore be rooted in the realities of prolonged, complex and multi-domain conflict.

> *"The key is not to be the strongest or the fastest, but to be the most adaptable. Victory goes to the side that can change faster than the other".*
>
> ***— John Boyd***

Endnotes

1 Michael Kofman and Rob Lee, "Not Built for Purpose: The Russian Military's Ill-Fated Force Design", *War on the Rocks*, 02 Jun 2022.

Jack Watling and Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* (London: Royal United Services Institute, 2023).

2 Seth J Frantzman, *Drone Wars: Pioneers, Killing Machines, Artificial Intelligence, and the Battle for the Future* (Nashville: Bombardier Books, 2021).

Missile Defense Project, "Iron Dome (Israel)", Missile Threat, Center for Strategic and International Studies, last modified 13 Jul 2021, accessed 18 Mar 2026, https://missilethreat.csis.org/defsys/iron-dome/

3 Volodymyr Yermolenko, "Ukraine's Information War: Winning the Narrative", *Journal of Democracy 33*, no. 4 (2022): 5–19.

4 Frank G Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges", *PRISM 7*, no. 4 (2018): 30–47.

5 Government of India, Ministry of Defence, Department of Defence Production, Draft Defence Production and Export Promotion Policy (DPEPP) 2020 (New Delhi: Ministry of Defence, 2020), accessed 18 Mar 2026 https://www.ddpmod.gov.in/sites/default/files/pdfupload/DraftDPEPP.pdf.

Fluid Frontiers: Mapping the Geopolitical Fault Lines of Fragmenting World Order

Dr Kawal Deep Kour[@]

Abstract

The contemporary international system is undergoing a transition towards a fragmented and polycentric order in which power is increasingly exercised across material, narrative, and technological domains. Conventional approaches to conflict, centred primarily on territorial and military capabilities, are increasingly inadequate for explaining the fluid and non-linear character of contemporary competition. This article introduces the Conflict Trajectory Mapping Framework (CTMF) as an analytical tool to examine how conflicts evolve across five phases: Incubation, Activation, Expansion, Stabilisation, and Reconfiguration. The framework integrates three dimensions of power: Material, Narrative, and Technological, enabling a multidimensional assessment of conflict intensity, strategic adaptation, and emerging inflection points. CTMF is applied to six theatres, namely Ukraine, Gaza, the Red Sea/Middle East, India, Türkiye, and Indonesia, from 2024 to 2028. The analysis identifies a growing pattern of managed instability, in which conflicts are

---

[@]**Dr Kawal Deep Kour** holds a PhD from the Indian Institute of Technology Guwahati and is a former Assam State Civil Services officer. Currently associated with the South Asian Drugs and Addictions Research Council, she researches drug policy, organised crime and geopolitical risk. She serves on the Joint United Nations Programme on Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome Multistakeholder Task Force for the 2026 High-Level Meeting and the Global Initiative Against Transnational Organized Crime Network of Experts. A former International Society for the Study of Drug Policy Board member, she has authored books and other publications on drugs, organised crime and terrorism.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

increasingly contained, redirected, and reconfigured rather than decisively resolved. The study argues that technological innovation, narrative influence, and asynchronous domain management are becoming central to contemporary statecraft and strategic competition.

Introduction: The Age of Fluid Frontiers

The contemporary international system has entered an era of profound geopolitical fragmentation. As the international system transitions from unipolarity through multipolarity towards a polycentric world order, this era can be 'Characterised by coexistence of multiple, differentiated centres of power'.[1] This is exemplified by the protracted hostilities in Ukraine and Gaza, the Red Sea crisis, and the wider turbulence across the Middle East. Modern-day conflicts are no longer confined to traditional territorial borders; they have evolved into Multi-Domain Operations (MDO)[2], across physical territory, digital, and cognitive spaces, where information, technology, and perception act simultaneously as tools of control and arenas of strategic contestation. This modern diffusion of conflict echoes Hedley Bull's observation on the tension between order and anarchy—an international society still bound by rules, yet increasingly unable to enforce them coherently.[3]

Theoretical Foundations: Power and Competition in a Polycentric Order

More fundamentally, this fragmentation embodies not just a restructuring of power; it signals the reconfiguration of how power operates. While structural realism remains relevant in explaining the systemic constraints and the enduring logic of anarchy[4], it cannot alone account for the fluidity of contemporary competition. The security dilemma persists[5], yet its expression now extends beyond territorial defence into the technological and informational domains.[6] This is evident in the behaviour of states—in the shift from traditional competition over territory or resources to the 'Contested spatialities of digital sovereignty'.[7] In this environment, power is no longer defined solely by material capability but by the ability to convert

resources into 'Realised influence and legitimacy'.[8] The social construction of threat and identity increasingly shapes strategic behaviour, as actors seek to shape perceptions of justice, sovereignty, and resistance through sustained contestation.[9]

This dynamic is driven in part by what Amitav Acharya describes as the emergence of a 'Multiplex World' with its overlapping and competing orders, each with its own norms, institutions, and spheres of influence and all contributing towards this fragmentation.[10] The erosion of hegemonic authority within this system has produced what Alexander Cooley and Daniel H Nexon call a world of 'Exit' and 'Substitution', in which states and non-state actors bypass traditional institutions to pursue alternative alignments.[11] [12] James N Rosenau characterised this scenario as creating a 'Patterned Chaos'—in which conflicts mutate rather than conclude and stability is managed rather than restored.[13] The result is an international system defined by fluid frontiers with zones of contestation that shift across geography, technology, and narrative space.[14]

The power shift today is not just happening from one set of states to another, rather the way power shifts, and the domains in which it operates, are themselves changing. Traditional structural realism may still help explain why states worry about existence, relative advantage and uncertainty. However, it falls short of capturing the essence of modern warfare, where competition plays out across domains that are not strictly territorial or military. The spiral model continues to operate, but it increasingly shows up in cyber, Artificial Intelligence (AI), sanctions infrastructure, and information-related operations and not just in troop manoeuvres or weapons emplacement. The battlefield today is not defined by geography or geographic limits but extends to data, the digital space and narrative legitimacy. Under such an evolving scenario of contestation, the operational leverage depends on how a state can best convert its resources into political outcomes through 'Power Projection', 'Legitimacy Generation' and strategic defence.

Within this scenario, 'States with Global Influence' such as India, Türkiye, and Indonesia have emerged as pivotal actors.[15] [16] They navigate between great powers with strategic hedging[17] to consolidate influence and leverage their soft power resources (cultural diplomacy, normative entrepreneurship, institutional leadership).[18] [19] [20]Their statecraft, built on institutional diversification, technological sovereignty, and anticipatory governance[21], offers adaptive and resilient strategies for navigating great power competition.[22] [23] [24] These states exemplify how agency is exercised in a fragmented order-not by 'Picking Sides' but through 'Building a fluid set of partnerships', which can survive and adapt to the stresses and strains of a polycentric order.[25]

Conflict Trajectory Mapping Framework

To capture these dynamics, this study advances the Conflict Trajectory Mapping Framework (CTMF)—a practical analytical tool introduced to explain how the pathways of power (military, narrative, technological) shift across five phases. It helps to identify what traditional analysis misses: why conflicts that look similar behave differently, and where they are headed next.

Based on the synthesis of structural constraint[26], escalation dynamics[27], and the social construction of legitimacy[28], CTMF integrates material, narrative, and technological dimensions to reveal how states navigate unpredictability and adjust influence under situations of systemic turbulence[29] within a phase-based temporal structure.

The Three Dimensions of Power of Conflict Trajectory Mapping Framework

In CTMF, power is operationalised through three integrated dimension, which are distinct yet interconnected aspects of the state's capability and influence.

- **Material Power**. It involves conventional 'Hard Power' resources: military deployments, defence expenditure, weapons systems, economic sanctions, and resource

mobilisation. This dimension traces the 'State versus state, boots-on-the-ground types of conflict'.

- **Narrative Power**. It is the capability to shape perceptions, acceptability and global influence. This includes strategic communications, platform governance, diplomatic communication, coalition-building, and narrative competition. Today, 'Crises, conflicts, and negotiations unfold in digitally saturated environments', where 'Credibility is fragile and audiences are polarised', posing the biggest challenge for operational sustainability.[30]

- **Technological Power**. It captures the operational realities that AI, autonomous systems, and algorithmic targeting have brought to modern warfare. AI is part and parcel of defence deployment, intelligence, and decision-making—emergent, veiled and unknowable.

Dimensions	What it Tracks	Key Indicators
Material	Physical and economic strength	Military deployments, territorial control, sanctions, supply chain disruption, energy leverage, arms transfers, casualty rates
Narrative	Legitimacy and perception	Information operations, diplomatic framing, media dominance, public opinion, alliance justification, identity mobilisation
Technological	Digital and systems power	Cyber operations, drone and AI deployment, surveillance infrastructure, platform control, space assets, critical tech dependencies

Table 1: CTMF's Three Dimensions and Key Indicators.
Source: Created by Author

The Five Phases of Conflict Trajectory Mapping Framework

CTMF maps these three dimensions of power across five temporal phases, each characterised by distinct patterns of power deployment:

- **Incubation**. Pre-crisis positioning—resource mobilisation, strategic framing, reconnaissance, and covert configurations.
- **Activation**. Conflict flare-ups—preliminary assaults, embargoes, narrative orchestration, and cyberspace attacks.
- **Expansion**. Escalation—MDO, information operations, and hyper war.
- **Stabilisation**. Controlled de-escalation—ceasefires, defence and deterrence postures, humanitarian diplomacy, and defensive cyberspace operations.
- **Reconfiguration**. Reorganisation—security sector reforms, paradigm shifts, technology transfers, and reconceived structural authority.

To test its validity, the framework is applied to six critical theatres—Ukraine, Gaza, the Red Sea/Middle East, India, Türkiye, and Indonesia, between 2024 and 2028, a period that can be characterised by dynamic deterrence, technological alacrity, and the formalisation of volatility. The analysis recognises a global changeover from escalation to managed instability, where states increasingly rely on technological and narrative infrastructure to contain disturbance rather than resolve it.

The findings suggest that the emerging world order is not post-conflict but post-stability: a system in which uncertainty is entrenched as a structural condition of international politics. Conflicts are no longer predictable and linear but chaotic and non-linear. CTMF offers new diagnostic tools to illuminate the paths of conflict in a global moment where the boundaries of war, peace, and influence are no longer static but in perpetual motion and ambiguity.

Three Analytical Dimensions of Conflict Trajectory Mapping Framework

CTMF functions as a diagnostic mapping tool that reveals the current power configurations across material, narrative and technological dimensions, enabling decision makers to identify strategic leverage and provide analytical clarity.

CTMF maps conflict evolution across five sequential but non-linear phases:

- **Incubation**. Structural conditions are present-grievances, resource constraints, and narrative chasms. These have not yet manifested in active hostility.
- **Activation**. A precipitating event or pre-meditated set-up moves latent tensions into direct confrontation. One or more domains become active theatres of conflict.
- **Expansion**. Conflict escalation across domains; new capabilities and actors are integrated. Misperception multiplies and security dilemma dynamics cause escalation spirals that turn chaotic.
- **Stabilisation**. Conflict enters a state of managed instability. States transition into acceptable sustained conflict, deploying capabilities, strategies and instruments to manage and contain rather than resolve conflicts.
- **Reconfiguration**. Conflict transforms- actors set moves, shift domains, retool approaches and realign objectives. This phase appears to be de-escalation but represents strategic transformation; actors are changing how they compete, not whether they compete

How It Is Applied

Each of the six theatres—Ukraine, Gaza, the Red Sea/Middle East, India, Türkiye, and Indonesia—is assessed across all three dimensions and five conflict phases of CTMF, for the 2024–2028 period. This analysis identifies:

- **Inflection points**. The critical junctures of phase transitions or dimensional shifts
- **Vital vertices**. Strategic points within the conflict system where targeted pressure is most decisive in determining conflict outcomes
- **Resilience Indicators**. How actors engage, adjust and recover without fundamental destabilisation

What CTMF Is Not? CTMF is not a predictive model. It is not designed to calculate probability. It is a form of early-warning methodology, intended to enhance interpretation, identify strategic leverage nodes, and enable systemic foresight, by making conflict trajectories visible before they become crises.

Phase	**Material Power**	**Narrative Power**	**Technological Power**
Incubation	Resource mobilisation, covert pact	Strategic framing, StratCom	Reconnaissance, Data mapping
Activation	Initial strikes, sanctions	Crisis specific frames and frame alignment	Offensive CyberOps, data leakage
Expansion	Full spectrum operation, grey-zone operations	Information Operations (Information Operations)	Algorithmic Warfare, Unmanned Aircraft System/ Unmanned Combat Aerial Vehicle use
Stabilisation	Ceasefire, Deterrence	Cognitive fatigue, humanitarian diplomacy	Cyber defence, eDiplomacy, Twiplomacy

Phase	Material Power	Narrative Power	Technological Power
Reconfigur-ation	Institutional reforms, realignments	Redefining legitimacy, rapprochement	Transfer of Technology, Information technology infrastructure

Table 2: Conflict Trajectory Mapping Framework Phases and the Three Dimensions of Power
Source: **Created by Author**

Conflict Trajectory Mapping Framework Scoring Methodology

The CTMF Composite Score (0-100) computes conflict intensity through systematic assessment of three equally weighted dimensions (one-third each): Material, Narrative, and Technological. Each dimension is scored 0-100 based on observable indicators from verified sources including the Armed Conflict Location and Event Data Project[31], Stockholm International Peace Research Institute [32], International Institute for Strategic Studies Military Balance[33], World Bank, United Nations records, threat intelligence platforms, with sub-components evaluated from minimal activity (0-10) to extreme intensity (31-33). Each dimension gets equal weight due to the very nature of modern 'Hybrid' conflicts. Composite scores aggregate dimension scores, with higher values indicating greater conflict intensity.

The current scores are compared to the 2024 baseline, to see if the conflict is escalating or de-escalating. Two elements together: quantitative scores and the qualitative context against which they are assessed to better analyse in which direction the conflict is headed. For instance, if Ukraine's Score is 78 (Material: 85, Narrative: 75, Technological: 75, ↑+12), this may reflect that the conflict is stabilising even though the 'Intensity Score' is high and increasing, because of technological pre-emption.[34] To ensure quality, the framework tests whether different analysts reach similar conclusions, compares results with traditional conflict catalogues and involves

professional review. However, the framework acknowledges limitations in data interpretation, variable data availability, general data quality, and absence of definitive predictions.[35]

The CTMF framework is operationalised through a structured assessment form that guides analysts through inflection point identification, three-dimensional scoring (Material, Narrative, Technological), pattern classification, sustainability assessment, and strategic implications analysis.

Cross-Case Synthesis: Conflict Trajectory Mapping Framework Patterns Across Six Theatres (2024-2028)

Based on the analysis of the six conflict theatres mentioned above, the CTMF framework reveals that the complex nature of modern-day wars is unpredictable, sustained by 'Managed Instability', which replaces 'Decisive Victory' as the goal.

A key outcome is that the dimensions of the dimensions of conflict—material, narrative, and technological—lack synchronicity. Each follows its own trajectory—escalating in one dimension while simultaneously de-escalating or stabilising in another dimension.

Moreover, critical turning points now happen without traditional battles. For example, the technology paradox—where technology is both an enabler and a disruptor—has emerged as the unique feature of modern-day conflicts, while the power of narrative has emerged as the battle decider, determining operational sustainability. Ukraine, Gaza, and the Red Sea illustrate these dynamics. Ukraine's drone attacks changed the course of the war without triggering nuclear retaliation from Russia, legitimacy concerns in the Gaza war forced an adjustment in military operations of Israel, and repeated Houthi attacks in the Red Sea generated global economic repercussions.

Projected Conflict Trajectories, 2026–2028. The following assessments apply the CTMF to six theatres, using their assessed phases in 2026 to outline possible trajectories to 2028. Each projection identifies the dominant dimension of power—material, narrative or technological—and the developments that could shape the theatre's course. These are conditional forecasts, subject to

changes in political decisions, security conditions and regional cooperation.

- **Ukraine**. CTMF places Ukraine in the stabilisation phase in 2026 and projects reconfiguration by 2028, with phased operations and technology as the dominant dimension. The projected shift is from active conflict towards preventive deterrence, emphasising drones, digital infrastructure security and diplomatic rebuilding.

- **Gaza**. The framework identifies reconfiguration as Gaza's phase in 2026, while indicating a possible return to expansion by 2028. Renewed flashpoints remain a concern, and competing narratives are likely to exert the greatest influence. Continuing humanitarian distress and political divisions could also delay institutional rebuilding.

- **Red Sea**. Following an expansion phase in 2026, the Red Sea theatre could move towards stabilisation by 2028. Material power remains the dominant dimension, with an encirclement strategy shaping the trajectory. Greater regional naval cooperation may ease maritime and cyber threats and improve the security of energy corridors.

- **India**. India is assessed as being in the stabilisation phase in 2026, with strategic consolidation projected by 2028. Technology is the dominant dimension: advances in defence systems and digital diplomacy could strengthen security and governance.

- **Türkiye**. From a reconfiguration phase in 2026, Türkiye is projected to move towards stabilisation by 2028. Its trajectory of recovery is shaped chiefly by narrative power, as diplomatic manoeuvres and economic diversification could strengthen regional legitimacy and stability.

- **Indonesia**. Indonesia's trajectory points from activation in 2026 towards expansion by 2028, with growing regional leverage driven primarily by material power. A stronger maritime security architecture, investment in digital

infrastructure and Association of Southeast Asian Nations-centric diplomacy could enhance its regional agency and resilience.

Across all six theatres, however, two patterns dominate: high-intensity wars transitioning to managed escalation (Ukraine, Gaza) and grey-zone competition that institutionalises ongoing instability (Red Sea, India, Türkiye, Indonesia). Thus, 'Ordered Chaos' is the essence of this polycentric world order, where conflicts are managed, redirected, and reconfigured rather than resolved.

Conflict Trajectory Mapping Framework and Strategic Adaptation in a Polycentric Order

The framework discloses three dynamics that restructure how states steer managed instability. First, conflicts are characterised by a synchroneity; they no longer follow linear trajectories. Aggregate 'Conflict Intensity' metrics no longer hold good as material stabilisation can coincide with technological surge or narrative collapse. The crises in Ukraine, Gaza, and the Red Sea exemplify how technological superiority, narrative framing, and kinetic restraint produce systemic disruption without traditional material dominance. This desynchronisation demands domain-specific monitoring rather than comprehensive 'Aggregate' valuations. Second, the defining feature of the 21st Century warfare is narrative framing. It is evident how Israel's Gaza operations and Moscow's offensive in Ukraine saw massive recalibration under intense narrative pressure. The depreciation of material power and the concurrent intensification of the 'Narrative' is a defining reality of modern-day warfare, determining what actions are politically sustainable, shaping coalition cohesion, arms transfers, and diplomatic manoeuvre space. The third dynamic uncovered relates to the ubiquity of technology Unmanned Aerial Vehicles (UAVs), autonomous defence systems as the pressure point in preventing a catastrophic escalation. Technology is both the enabler and disruptor in this environment. Ukraine's medium and long-range drone strikes, India's AI-driven defence modernisation, and Türkiye's UAV innovation are revealing how technological capabilities have outmanoeuvred conventional warfare abilities, reshaping responses and outcomes. CTMF's

analytical architecture extends beyond the six theatres examined here. Applying the framework to other contexts such as strategic disputes in the Taiwan Strait, Korean Peninsula, and Sahel conflicts may reveal whether it holds across diverse threat environments. Monitoring these domains longitudinally through a mapping of these phases over time may refine metrics which could potentially enable researchers to identify the conditions favourable to the operation and institutionalisation of grey-zones rather than open conflict intensification. Furthermore, by embedding CTMF metrics within early-warning systems, the framework could evolve from retrospective analysis to anticipatory governance, enhancing real-time conflict monitoring in an era where instability is operational rather than intermittent.

Conclusion: Conflict Trajectory Mapping Framework and Geometry of Managed Instability

What emerges from the analysis of evidence collected across six theatres between 2024 and 2028 is that the international system is 'Routinising' conflict rather resolving it.[36] Conflicts are continual; sustained within 'Simmering' boundaries, through the mechanism of calibrated coercion, narrative rhetoric, and hi-tech adaptation. What appears as discrete crises is actually a continuous condition—a polycentric order in which instability operates not as political failure, but as a governing instrument.

This is where the CTMF illuminates what traditional models leave unexplained. CTMF does not reduce escalation to a single metric, depending on battlefield intensity. Instead, it maps it across three enmeshed dimensions, revealing that contemporary conflicts are not strictly chaotic but structurally managed. Ukraine can sustain material stalemate because technological innovation compensates; Gaza must constrain material operations when narrative costs escalate; the Red Sea can limit kinetic engagement yet still achieve systemic disruption through narrative and technological amplification. In other words, the conflict intensity varies by domain and strategic advantage comes from managing domains asynchronously.

Therefore, seen through CTMF, the period 2024-2026 is not 'Post-conflict'; it is post-stability. The new normal is managed instability: a durable condition in which actors do not aim for decisive victory, but for endurance, leverage, and controlled disruption. As mentioned above, two conflict archetypes coalesce: high-intensity wars that develop into managed escalation (Ukraine, Gaza), and grey-zone competitions that develops into institutionalised instability (Red Sea, India, Türkiye, Indonesia). Both follow the same strategic logic: conflicts metamorphose because the system rewards actors who can keep conflicts simmering without crossing catastrophic thresholds.

As such, CTMF's contribution is not merely descriptive. It is analytical and operational. CTMF does not promise certainty; it offers something more valuable in an age of fluid frontiers: a rigorous technique to perceive how instability emerges, identify how it is managed, and to determine the strategic interventions which can realign trajectories before they cross catastrophic thresholds. If the twentieth century's strategic question was how wars end, the twenty-first century's is how 'Never-ending wars'[37] are managed. CTMF offers the syntax for answering it and, in doing so, reframes the central task of statecraft in a polycentric world—not the restoration of a lost order, but cultivating resilience under perpetual contestation.

Endnotes

1 Ünal Çeviköz, "Polycentrism or Multipolarity: Understanding the Contemporary International System", *Global Panorama*, 15 Jan 2025, accessed 10 Jul 2026, https://www.globalpanorama.org/en/2025/01/polycentrism-or-multipolarity-understanding-the-contemporary-international-system-unal-cevikoz/

2 Hal Brands, "The Lost Art of Long-Term Competition", *The Washington Quarterly* 41, no. 4 (2018): 31–51.

3 Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (London: Macmillan, 1977), 46–51.

4 Kenneth N. Waltz, Theory of International Politics (Reading, MA: Addison-Wesley, 1979).

5 Robert Jervis, “Cooperation Under the Security Dilemma”, *World Politics* 30, no. 2 (1978): 167–214, https://www.sfu.ca/~kawasaki/Jervis%20Cooperation.pdf

6 Ibid.

7 Georg Glasze et al., “Contested Spatialities of Digital Sovereignty”, *Geopolitics* 28, no. 2 (2023): 919–58, accessed 12 Jul 2026, https://doi.org/10.1080/14650045.2022.2050070

8 Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011).

9 Alexander Wendt, “Anarchy Is What States Make of It”, *International Organization* 46, no. 2 (1992): 391–425, accessed 12 Jul 2026, https://www.jstor.org/stable/2706858

10 Amitav Acharya, “After Liberal Hegemony: The Advent of a Multiplex World Order”, *Ethics & International Affairs* 31, no. 3 (2017): 271–85, accessed 12 Jul 2026, https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/after-liberal-hegemony-the-advent-of-a-multiplex-world-order/DBD581C139022B1745154175D2BEC639

11 Alexander Cooley and Daniel H. Nexon, *Exit from Hegemony: The Unraveling of the American Global Order* (Oxford: Oxford University Press, 2020), 1–28, 217–45.

12 David A. Lake, Lisa L. Martin, and Thomas Risse, “Challenges to the Liberal Order: Reflections on *International Organization”*, *International Organization* 75, no. 2 (2021): 225–57, accessed 13 Jul 2026, https://www.jstor.org/stable/27104637

13 James N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity* (Princeton, NJ: Princeton University Press, 1990).

14 Leslie Vinjamuri, ed., with Senem Aydın-Düzgit et al., *Competing Visions of International Order: Responses to US Power in a Fracturing World*, research paper, US and the Americas Programme (Chatham House, Mar 2025), https://www.chathamhouse.org/sites/default/files/2025-03/2025-03-27-competing-visions-international-order-vinjamuri-et-al.pdf

15 Robert S. Chase, Emily B. Hill, and Paul Kennedy, “Pivotal States and U.S. Strategy”, *Foreign Affairs* 75, no. 1 (1996): 33–51, ACCESSED 14 Jul 2026, https://www.jstor.org/stable/20047466

16 Meghan O’Sullivan, Rana Mitter, and Moeed Yusuf, “Middle Powers: An Intellectual Framework”, Belfer Center for Science and International Affairs, 20 Nov 2025, accessed 13 Jul 2026, https://www.belfercenter.org/research-analysis/middle-powers-intellectual-framework

17 Evelyn Goh, “Meeting the China Challenge: The U.S. in Southeast Asian Regional Security Strategies”, *Policy Studies* 16 (2005): 1–35; Cheng-Chwee Kuik, “The Essence of Hedging: Malaysia and Singapore’s Response to a Rising China”, *Contemporary Southeast Asia* 30, no. 2 (2008): 159–85; Cheng-Chwee Kuik, “How Do Weaker States Hedge? Unpacking ASEAN States’ Alignment Behavior Towards China”, *Journal of Contemporary China* 25, no. 100 (2016): 500–514.

18 Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change”, *International Organization* 52, no. 4 (1998): 887–917, accessed 14 Jul 2026, https://library.fes.de/libalt/journals/swetsfulltext/5333873.pdf

19 Evelyn Goh, “Meeting the China Challenge: The U.S. in Southeast Asian Regional Security Strategies”, *Policy Studies* 16 (2005): 1–35, accessed 14 Jul 2026, https://www.files.ethz.ch/isn/26086/PS016.pdf

20 Cheng-Chwee Kuik, “The Essence of Hedging: Malaysia and Singapore’s Response to a Rising China”, *Contemporary Southeast Asia* 30, no. 2 (2008): 159–85, accessed 14 Jul 2026, https://www.researchgate.net/publication/265754648_The_Essence_of_Hedging_Malaysia_and_Singapore's_Response_to_a_Rising_China

21 Edoardo Celeste, “Digital Sovereignty in the EU: Challenges and Future Perspectives,” *Data & Policy* 3 (2021): e9; on anticipatory governance, see David H. Guston, “Understanding ‘Anticipatory Governance,’” *Social Studies of Science* 44, no. 2 (2014): 218–42.

22 Hal Brands, “The Lost Art of Long-Term Competition,” *The Washington Quarterly* 41, no. 4 (2018): 31–51, accessed 15 Jul 2026, https://www.tandfonline.com/toc/rwaq20/41/4

23 Edoardo Celeste, “Digital Sovereignty in the EU: Challenges and Future Perspectives,” *Data & Policy* 3 (2021): e9, accessed 15 Jul 2026, https://www.researchgate.net/publication/349495575_Digital_Sovereignty_in_the_EU_Challenges_and_Future_Perspectives

24 David H. Guston, “Understanding ‘Anticipatory Governance,’” *Social Studies of Science* 44, no. 2 (2014): 218–42, accessed 16 Jul 2026, https://doi.org/10.1177/0306312713508669

25 Meghan O’Sullivan, Rana Mitter, and Moeed Yusuf, “Middle Powers: An Intellectual Framework,” 20 Nov 2025; see also Amitav Acharya, *The End of American World Order*, 2nd ed. (Cambridge: Polity Press, 2018), 147–79, on agency in polycentric orders; and Alexander Cooley and Daniel H. Nexon, *Exit from Hegemony: The Unraveling of the American Global Order* (Oxford: Oxford University Press, 2020), 217–45.

26 Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979).

27 Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics* 30, no. 2 (1978): 167–214.

28 Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999); Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011).

29 James N. Rosenau, *Turbulence in World Politics*, 97–134.

30 Kamal Singh Kunwar, “Diplomatic Communication in the Digital Era: Structural Transformation, Power Reconfiguration, and Strategic Implications of Digital Diplomacy”, preprint, *Research Square*, posted 22 Feb 2026, accessed 17 Jul 2026, https://doi.org/10.21203/rs.3.rs-8906604/v1

31 Armed Conflict Location & Event Data (ACLED), “Conflict Data,” accessed 25 Sep 2026, accessed 17 Jul 2026, https://acleddata.com/conflict-data

32 Stockholm International Peace Research Institute (SIPRI), “SIPRI Databases,” accessed 17 Jul 2026, https://www.sipri.org/databases

33 International Institute for Strategic Studies (IISS), *The Military Balance 2026* (Abingdon: Routledge, 2026), accessed 18 Jul 2026, https://www.iiss.org/publications/the-military-balance/2026/the-military-balance-2026/

34 Author’s calculation using the Conflict Trajectory Mapping Framework (CTMF) scoring methodology described in this article.

35 Each CTMF dimension comprises sub-indicators assessed individually and aggregated into a score from 0 to 100. For example, Material Power includes troop deployments, defence expenditure and weapons transfers. The composite CTMF score is the arithmetic mean of the Material, Narrative and Technological scores, giving each dimension equal weight. A higher composite score indicates greater assessed conflict intensity.

36 Imran Khurshid, “Navigating Geopolitical Turbulence in a Fragmented International System”, *The Peninsula Foundation*, 03 Feb 2026, accessed 18 Jul 2026, https://thepeninsula.org.in/blog/navigating-geopolitical-turbulence-in-a-fragmented-international-system

37 AB Shivane, “Never-Ending Wars of 21st Century”, *Indian Defence Review*, 24 Sep 2021, accessed 18 Jul; 2026, https://indiandefencereview.com/never-ending-wars-of-21st-century/

Loyalty, Purges and Fragility: Stress Within Chinese People's Liberation Army

Colonel Shanu Krishna[@]

"Our principle is that the Party commands the gun and we will never allow the gun to command the Party"

—Mao Zedong[1]

(*Problems of War and Strategy*, 1938)

Abstract

China's ongoing military purges under President Xi Jinping have significantly altered the People's Liberation Army (PLA). These purges have prioritised political loyalty above all else, even at the expense of institutional stability and professional expertise. This article uses systems thinking to illustrate how these repeated purges, while ensuring short-term political control, gradually undermine command continuity, trust, and overall operational effectiveness. Although the PLA still possesses considerable military strength, the instability within its highest leadership ranks has created temporary strategic weaknesses. The study suggests that India could leverage this brief period by enhancing its border infrastructure, intelligence capabilities, operational readiness, and diplomatic efforts. The opening is not

---

[@]**Colonel Shanu Krishna** is an alumnus of the National Defence Academy. He was commissioned into PUNJAB Regiment and commanded a newly raised unit in a super high-altitude area along the Line of Control (LC). An Officer with extensive experience in varied terrain and operational dynamics, he has served on the LC/Line of Actual Control (LAC) in staff and command appointments. His key appointments include deputation to a Special Force raised for the Northern borders, General Staff Officer of a Mountain Brigade along the LAC and Company Commander under the United Nations Interim Force in Lebanon (UNIFIL). He is presently posted as Directing Staff at Senior Command Wing at Army War College.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

confined to the land frontier; it extends equally to the Indian Ocean Region, where India's positional advantage is greatest, as it constrains the PLA Navy and Air Force in sustaining distant deployments.

Introduction

China today presents a clear paradox. It asserts itself as the world's most advanced military, from cutting-edge space warfare systems to the largest naval fleet, yet appears increasingly short of senior commanders. The Fourth Plenary Session of the Chinese Communist Party's (CCP) 20th Central Committee, which concluded in Oct 2025, saw strikingly low attendance among Central Committee members, with about one-sixth absent. Thereafter, in Jan 2026, General Zhang Youxia, a long-time confidant of President Xi Jinping and one of the two remaining Vice Chairmen of China's Central Military Commission (CMC), was placed under investigation, along with members of his family.[2] This left the seven-member apex military decision-making body with only two members: President Xi, the CMC Chairman, and General Zhang Shengmin, the other CMC Vice Chairman, who had been appointed in Oct 2025. By mid-2026, an estimated 101 senior officers holding appointments at the CMC, theatre commander or theatre deputy commander level had been removed, affecting roughly half of the People's Liberation Army's (PLA) senior leadership positions.[3].

The pattern held through 2026. The March National People's Congress (NPC) met with unusually thin military representation, and on 26 Jun 26, the NPC Standing Committee stripped thirteen lawmakers of their posts, six of them senior PLA officers, confirming that the purge now cuts across the civil-military divide[4]. A week later, on 03 Jul 26, President Xi promoted two officers to full General: General Zhang Shuguang as Secretary of the CMC Discipline Inspection Commission, replacing General Zhang Shengmin, who had held it since 2017, and General Wang Gang, the serving Commander of the PLA Air Force. Neither was inducted into the CMC, which remains a two-member body[5].-The purge has therefore entered a concurrent purge-and-rebuild phase. Hence, the question logically emerges: 'Who will lead the PLA in the event of a conflict?'

This dilemma underscores the predicament prevalent in the PLA at a time when internal restlessness seems to be simmering just beneath the surface.

This is not unprecedented in communist civil-military practice. Stalin's Red Army purge of 1937–38 repressed over half of 1,844 general-rank officers and executed at least 780, an episode historians treat as a primary reason for the Soviet Army's failed response to Hitler's invasion in Jun 1941.[6] Mao's purge following Lin Biao's flight in Sep 1971 removed the leadership of the General Staff, the Air Force and the Navy, and embedded a purge culture that has never left the PLA. In both cases, the political gain was immediate and the military cost deferred.

This article contends that the current turbulence within the PLA should not be interpreted as a loss of control by President Xi. Instead, it is a deliberate exchange in which political loyalty is prioritised over institutional depth and professional aptitude, a trend running since 2013 that now manifests as growing stress on the PLA's military efficacy. It examines what the promotion-purge cycle reveals about Chinese civil-military relations, then sets out indicators and policy responses for India.

The Institutional Framework

The architecture depicted in Figure 1 is not incidental to the purges; it is what makes purges possible in its current, noiseless form. President Xi concurrently holds the three principal offices of the Chinese system: General Secretary of the Party, President of the state, and Chairman of the CMC. Each controls its own disciplinary organ, so a general can be investigated, stripped of his deputy status, and expelled with no independent body able to obstruct the process. President Xi has systematically dismantled the distinctions between the Party and the state, prioritised personal ideology over established institutional norms, and secured indefinite tenure through the Mar 2018 constitutional amendment that removed presidential term limits.[7]

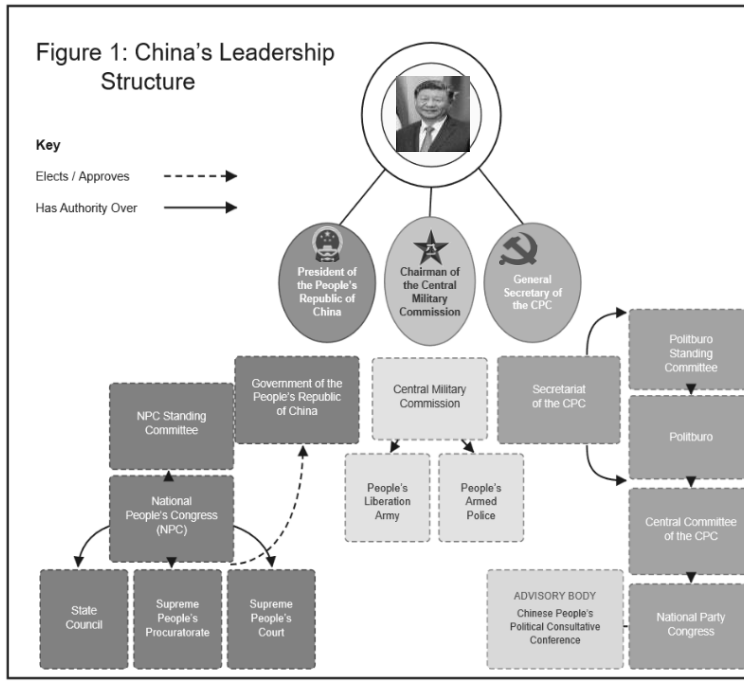


Figure 1. Institutional Relationship among the CCP, State and CMC

Central Committee Plenums

A plenum is a full assembly of the Chinese Communist Party Central Committee, nominally the body that selects the Politburo, its Standing Committee, and the CMC under the CCP Constitution. The political reality is the opposite; the party's senior-most leaders determine the composition of the Central Committee through opaque backroom negotiation.[8] The Fourth Plenum of 20–23 Oct 25 extended beyond its conventional governance agenda to ratify military personnel changes and endorse the 15th Five-Year Plan (2026–30). Its most striking feature was the number of absentees. 168 members and 147 alternates attended, against the 205 full members and 171 alternates who constituted the 20th Party Congress in 2022. The PLA was worst hit, with 27 of 42[9] military members absent, including 22 generals—a 63 per cent absence rate.

The Purges and Implications

An external shock sharpened this. Russia's failure to subdue a weaker Ukraine after Feb 2022 showed how systemic corruption, inflated readiness returns, and neglected equipment hollow a force that looks formidable on paper, and PLA researchers studied the campaign closely.[10] The lesson reinforced rather than moderated President Xi's method; the remedy chosen was deeper political control, not professional autonomy.[11]

President Xi Jinping began by systematically dismantling the patronage networks of the Jiang Zemin and Hu Jintao eras, blending organisational reformation, ideological re-indoctrination via the 2014 Gutian Conference, and legal-administrative tools to fuse political loyalty with command authority under the 'CMC Chairman Responsibility System'.[12] Reliance shifted from the Fujian coterie and 31st Group Army to the Shaanxi faction, yet later waves showed that factional and familial proximity offered no safeguard. By integrating Party discipline organs, the NPC, and the CMC into a continuous purge mechanism, President Xi has turned anti-corruption into a tool that suppresses succession, weakens institutional bonds, and implants enduring fear across the PLA. The precedent has since hardened, with a military court awarding suspended death sentences to General Wei Fenghe and General Li Shangfu, China's two most recent Defence Ministers, exceeding the life terms given to General Guo Boxiong in 2016 and General Fang Fenghui in 2019.[13] That one of them was pursued after retirement carries its own message; leaving service confers no immunity, and the campaign's reach is retrospective as well as ongoing.

Factional Chessboard of Xi and PLA

A contest of ambition and loyalty has unfolded within China's CMC since the CCP's 20th Congress in Oct 22. General He Weidong made an audacious 'Triple Jump' straight to CMC Vice Chairman,[14]—leapfrogging General Zhang Shengmin despite inferior qualifications and later entry into the CMC. For General Zhang Shengmin, the message was unmistakable; he remained an outsider, valued only as the discipline commission's instrument. With his help and that of

General Zhang Youxia, President Xi purged General He Weidong and Admiral Miao Hua before the 4th Plenum, the first removal of a sitting CMC Vice Chairman since 1967 and unthinkable under Hu Jintao or Jiang Zemin. General Zhang Shengmin has since been elevated to Vice Chairman, though without the customary Politburo seat, and General He Weidong's seat remains vacant. On Jan 26, General Zhang Youxia and Joint Staff Chief General Liu Zhenli were placed under investigation**;** the charge levelled against him, of trampling the chairman responsibility system, is an explicitly political offence rather than a criminal one. That distinguishes this wave from the prosecutions of General Xu Caihou and General Guo Boxiong a decade earlier.

The erstwhile Strategic Support Force, which held space, cyber and electronic warfare capabilities under one roof, was dissolved on 19 Apr 24 and its functions were redistributed to the newly raised Aerospace Force, Cyberspace Force and Information Support Force.[15] Its last two commanders subsequently disappeared from public view, and in Jun 26 the serving commander of the Cyberspace Force was removed, leaving the PLA's newest arms under leadership that is itself provisional.[16]

Discipline Below the Command Echelon

The disciplinary drive is not confined to the apex. Instructions circulated through PLA units during 2026 direct officers to refuse routine social approaches connected with recruitment and procurement and to submit their personal circles to party committee scrutiny.[17] An officer corps conditioned to treat ordinary reciprocity as a disciplinary hazard becomes an officer corps that refers decisions upward and avoids ambiguity. The paralysis visible at the CMC is thus being reproduced at the troop level. The same logic has been applied at the lower ranks for whom the Ministry of National Defence's Conscription Office promulgated a code of ethics built around political loyalty, integrity and the transparent exercise of power. It followed a Politburo meeting on 30 Jul 26, at which President Xi called for stronger political guidance and linked political loyalty directly to military effectiveness, while urging decisive progress toward the PLA's centenary modernisation goals.[18]

System Thinking Analysis: Promotion-Purge Cycle

While individual purges might seem justifiable when considered independently, their collective impact, characterised by frequent leadership changes, pervasive institutional apprehension, diminished confidence, and postponed operational risks, becomes evident only when analysed as components of a feedback-influenced system.

A clearer understanding of these underlying dynamics emerges when the operative forces are visualised in a Causal Loop Diagram (CLD), as presented in Figure 2. This CLD illustrates President Xi's reliance on PLA purges as a manifestation of the 'Shifting the Burden' systems archetype. Faced with the fundamental challenge of maintaining unwavering political authority while upholding military efficacy, President Xi appears to favour a solution that addresses immediate symptoms. The purges are framed as anti-corruption and loyalty enforcement rather than the slower, fundamental solution of institutionalisation. The reinforcing loop R1 converts threat perception into purges and short-term obedience while eroding the very trust that generated the threat perception. The balancing loop B1 registers the resulting churn, degraded joint planning, and strategic vulnerability only after a lag, which is why the fundamental solution loop R2 remains undeveloped.

The Jun–Jul 2026 cycle validates the model precisely: a purge wave, loyalist promotions within a week, and no replenishment of the institution itself. The system is accelerating its R1 loop while the costs of the balancing loop accrue in the background.– Breaking the cycle would require institutionalised promotion and a reduced reliance on purges; without that, the condition becomes permanent. The Soviet precedent indicates where the cost surfaces. Glantz records that by Jun 1941 Soviet officers routinely commanded two levels above their experience. The PLA is now reproducing that condition.[19] Convention requires CMC members to hold full general rank and prior command of a major department, theatre, or service, yet dozens of key posts are now discharged de facto by lieutenant generals promoted within the past year.[20]

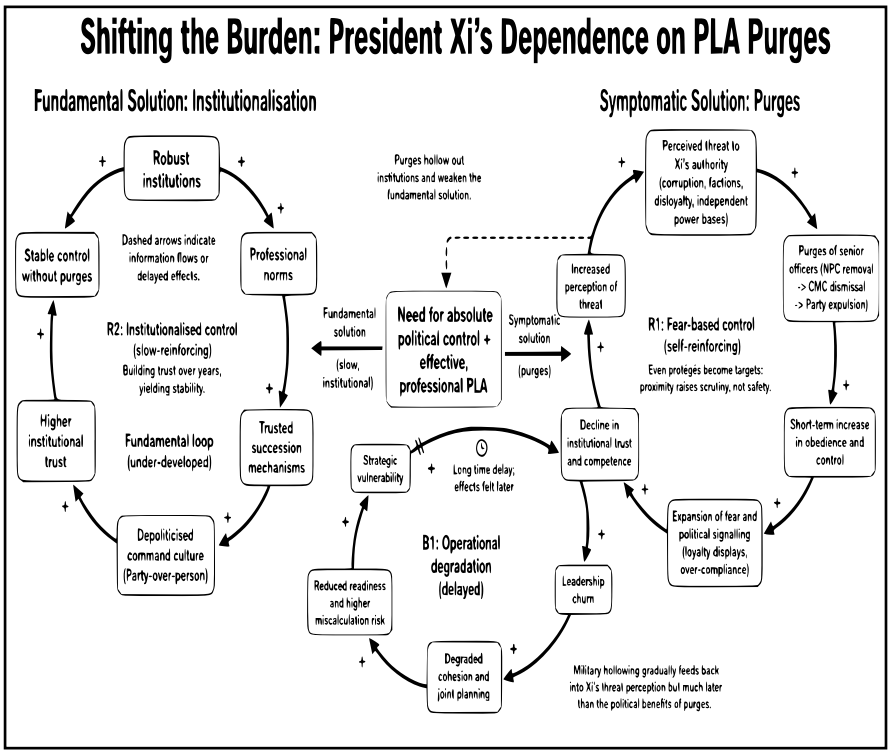


Figure 2. Causal Loop Diagram for Xi Jinping's Purges

India's Risks and Opportunities

Continuity Below, Paralysis Above. Corrective is essential. Despite the purges, training opposite India has continued undisturbed; annual mobilisation, winter acclimatisation and contingency joint exercises have run as scheduled every year since 2022, opened each January by the Training Mobilisation Order.[21] What insulates the PLA is the institutionalisation of operational knowledge. Border units remain in the same theatre for long tenures, so terrain familiarity and the memory of past face-offs reside in the formation rather than the individual. What has been paralysed is the authority above the unit to act on that memory. The measure of that paralysis is time. In 2024, the PLA launched major exercises around Taiwan within three to four days of a perceived provocation; in 2025, with theatre and CMC leadership gutted, the same machine took nineteen days in Apr and twelve in Dec.[22] The PLA still knows how

to fight; it just hasn't decided to. That gap, not any assumed incompetence, is India's opportunity.

PLA Purges: Loyalty vs Institutional Strain

- If continuity holds below, the churn above is severe. Purges have reshaped the PLA into a force prioritising loyalty over competence, cautious yet volatile along the Line of Actual Control (LAC). The Western Theatre Command (WTC) has had four commanders since Galwan 2020, and the Jun 26 removal of its Political Commissar left both halves of the theatre's dual command vacant. In the PLA's dual command system, the Commander and Commissar jointly authorise consequential decisions, so this is unprecedented in the post-1979 PLA. India's window here is narrow but high-leverage, if it builds capability for tempo dominance, ISR superiority, dual-use infrastructure, narrative building, and calibrated diplomacy. The replacement pattern compounds it. Of twenty key posts reassigned in the current reshuffle, nine went to air force officers, and only two of the five theatre commanders have been publicly confirmed, both of them airmen.[23] For a theatre facing India, long a ground-force country, an air-force-weighted rebuilding of the high command implies a further period of unfamiliarity before the WTC settles.

- Vary patrol frequency in time (timing and duration), space (location and frequency), and force (quantum and composition) domains to impose operational asymmetry, forcing PLA risk-aversion without crossing thresholds.

- Complete strategic border infrastructure (roads, underground storage, helipads, all-weather airfields, etc.) in the 12–18-month leadership void before potential rebound by 2027.

Recentralised Control and India's Moral Ascendancy

- Recentralisation, not weakness, drives this. Along the 3488 Km border, this produces a paradox: a leaderless WTC lacking strategic guidance, generating disjointed information-warfare aggression alongside operational diffidence. By

maintaining restraint, upholding protocols and prioritising dialogue, India will position itself as the mature actor, recasting PLA friction as domestic insecurity rather than Indian provocation.

- Emphasise India's non-provocative record in the Working Mechanism for Consultation and Coordination (WMCC) on India-China Border Affairs, Special Representatives (SR) and Senior Commander forums, where the contrast with PLA conduct along the LAC facilitates third-party support.

- Open additional Border Personnel Meeting points and leverage the moral high ground in QUAD and UN narratives towards restoring the pre-Apr 2020 status quo.

WTC and Rocket Force Weaknesses

- The Rocket Force has been the hardest-hit branch; its command team was removed in Jul 23, and their successor followed in Oct 25. US intelligence assessments reported in Jan 24 attributed the crisis to fuelling irregularities and silo lids that would not open, that is, to the procurement chain rather than to individual commanders. Export performance has compounded the doubt. The same HQ-9 family has now been defeated in three theatres in eighteen months: in Operation SINDOOR,[24] over Iran[25] and in Venezuela, where a layered Russian, Chinese and Iranian air defence collapsed inside an hour.[26] This constrains China's escalation ladder against Indian salience, though insecure commanders risk miscalculation.

- The evidence must nonetheless be weighed with care, because Beijing has answered every corruption report with a demonstration rather than a denial. An intercontinental ballistic missile was fired some 12,000 km into the Pacific in Sep 24, the first such launch in 44 years,[27]–and a submarine-launched missile some 7,300 km into the South Pacific in Jul 26.[28]

- Export failure and strategic reach are not the same thing. The purges have degraded decision-making authority, not delivery capacity.

Tibet-Xinjiang Distractions Amplify Strain

- Unrest in Tibet and Xinjiang, compounded by the purges, forces the PLA to spend 40% of training time on ideological drills,[29] diverting WTC focus from LAC readiness to internal security. Politicised units prioritise obedience over warfighting ability, rendering them inward-looking and hesitant.

- Conduct deliberate senior-leader profiling in WTC using information on purge cycles, tenure instability, and promotion patterns to anticipate hesitation thresholds.

- Exploit distraction through stepped-up administrative support to the Central Tibetan Administration (CTA) to raise the 'Free Tibet' issue and counter PLA cartographic assertions.

The Maritime Dimension. The far-seas project has not been spared. The naval officer who ran the CMC Political Work Department and controlled senior promotions was removed in Nov 24, and the Navy's commander has not appeared in public since late 2025.[30] By then, the PLAN had regularised far-seas training, operating two carrier groups beyond the First Island Chain in Jun 25.[31] The Air Force faces the same problem, since maritime strike, long-range surveillance and air cover for distant task groups are its responsibility, and its Political Commissar was removed in Jun 26. Distant deployment is the least forgiving test of a command system because it runs on delegated authority, which the purges have withdrawn. In the Indian Ocean, at the end of a long logistic tether and under surveillance from the Andaman and Nicobar Islands, that dependence is sharpest.

Translating Advantages into Enduring Leverage

- India's decentralised mission command, established acclimatisation regime and visible sustainment outmatch c caution. Battlefield credibility, dominance of the LAC through patrols and ISR, and infrastructure development should translate directly into WMCC and Corps Commander negotiating power.

- Link confidence-building measure and trade normalisation to verified patrolling discipline via WMCC, demanding WTC leadership transparency.

- Accelerate Rafale/Su-30MKI forward basing, border roads and Andaman Nicobar hardening within the 12–18-month window, while enhancing QUAD coordination and strengthening multiple minilateral partnerships with SE Asian countries to strengthen own capability to operate at will up to the Malacca Strait.

Deliberate a Review of Unit Rotation Policy Along the LAC

- The PLA's residual strength is continuity of tenure, while Indian units in most sectors change every two years, taking terrain knowledge and acclimatisation with them. The Rashtriya Rifles model in Eastern Ladakh, where the unit remains and personnel rotate, should be tested against two-yearly infantry turnover for operational familiarity, acclimatisation cost, quality of border personnel meeting engagement and continuity of the negotiating record. India's institutional memory should reside in the formation and the file, not depart with the outgoing Commanding Officer and unit.

- Establish an indicator watch list. Five measurable series should be tracked: the standard and tempo of Chinese contingents in United Nations peacekeeping operations; the frequency and complexity of joint and combined exercises; leadership continuity, measured as mean tenure in appointment and the share of billets held in an acting capacity; procurement announcements and equipment induction rates; and Rocket Force test activity. Divergence between declared modernisation and these series is the earliest measure of whether the trade is being paid for.

Conclusion

The purges have left the CMC with President Xi and General Zhang Shengmin alone, while theatre, service and military district commands across the PLA are run on acting authority, stalling joint

operations and modernisation. The void reflects absolute distrust and has made loyalty the measure in place of competence. The vacancy at WTC creates a rare 12–18-month window that India must exploit through ISR profiling of leadership gaps, infrastructure surges, tempo-dominant patrols, and SR, WMCC, and Higher Military Commander talks linking CBMs to verified disengagement, before reconstitution in 2027. The Jul 26 promotions, which restored the discipline apparatus ahead of the operational chain, are the first visible sign of reconstitution and confirm that this window has already begun to close. The maritime corollary holds equally; the same lack of settled authority constrains Chinese operations far from home, and India's positional advantage against them is greatest in the Indian Ocean Region.

Endnotes

1 Mao Zedong, 'Problems of War and Strategy', *Selected Works of Mao Tse-tung*, vol. 2 (Peking: Foreign Languages Press, 1965), https://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_12.htm

2 Manoj Kewalramani, "What Zhang Youxia's Purge Could Mean for China's 21st Party Congress", RSIS, 19 Jan 2026, accessed 15 Mar 2026, https://rsis.edu.sg/rsis-publication/idss/ip26018-what-zhang-youxias-purge-could-mean-for-chinas-21st-party-congress/

3 Bonny Lin, "Xi's Purges Undermine the PLA's Near-Term Readiness for Taiwan", in *Assessing Xi's Unprecedented Purges of China's Military*, Center for Strategic and International Studies, Feb 2026, accessed 15 Mar 2026, https://www.csis.org/analysis/assessing-xis-unprecedented-purges-chinas-military-key-developments-and-potential

4 Phoebe Zhang, "China Removes 6 Generals from Legislature as Military Anti-Corruption Drive Continues", *South China Morning Post*, 27 Jun 2026, accessed 16 Mar 2026, https://www.scmp.com/news/china/politics/article/3358586/china-removes-6-generals-legislature-military-anti-corruption-drive-continues

5 Reuters, "China's Xi Taps New Military Anti-Graft Chief, Promotes Two Generals", 04 Jul 2026, accessed 16 Mar 2026, https://www.reuters.com/world/asia-pacific/china-promotes-two-military-officers-full-generals-rank-2026-07-03/

6 Becker Friedman Institute, University of Chicago, "The Anatomy of the Great Terror: A Quantitative Analysis of the 1937–38 Purges in the Red Army", BFI Working Paper no. 2024-154, Dec 2024, accessed 16 Mar 2026, https://bfi.uchicago.edu/wp-content/uploads/2024/12/BFI_WP_2024-154.pdf

7 BBC, "China's Xi Allowed to Remain 'President for Life' as Term Limits Removed", 18 Mar, 2018, accessed 16 Mar 2026, https://www.bbc.com/news/world-asia-china-43361276

8 Brookings Institution, "Purges, Personnel, and Policy: A Primer on China's Fourth Plenum", 13 Oct 2025, accessed 17 Mar 2026, https://www.brookings.edu/articles/purges-personnel-and-policy-a-primer-on-chinas-fourth-plenum/.

9 Growing Cracks in Xi's Military Control as CCP Plenum Exposes Deep Turmoil in PLA", *The Tribune*, 28 Oct 2025, accessed 17 Mar 2026, https://www.tribuneindia.com/news/world/growing-cracks-in-xis-military-control-as-ccp-plenum-exposes-deep-turmoil-in-pla/

10 Howard Wang and Brett Zakheim, *China's Lessons from the Russia-Ukraine War*, RR-A3141-4 (Santa Monica, CA: RAND Corporation, n.d.).

11 Kareem Korayem, "Why Xi's Search for Loyalty Is Strangling the PLA's Effectiveness," *Small Wars Journal*, 05 May 2026.

12 U.S.-China Economic and Security Review Commission, *CCP Decision-Making and the 20th Party Congress: Hearing before the U.S.-China Economic and Security Review Commission*, 117th Cong., 2nd sess., 27 Jan 2022, https://www.uscc.gov/sites/default/files/2022-01/January_27_2022_Hearing_Transcript.pdf

13 Two Former Chinese Defence Ministers Handed Suspended Death Sentences", *South China Morning Post*, 08 May 2026, accessed 17 Mar 2026, https://www.scmp.com/news/china/military/article/3352764/2-former-chinese-defence-ministers-given-death-sentence-reprieve

14 Xiao X., "The Swift Removal of He Weidong, the Desire to Eliminate Zhang Youxia, and Zhang Shengmin Being Forced onto Liangshan by Xi," *People News Today*, 13 Nov 2025, https://www.peoplenewstoday.com/news/en/2025/11/13/1124524.html.The-Swift-Removal-of-He-Weidong-the-Desire-to-Eliminate-Zhang-Youxia-and-Zhang-Shengmin-Being-Forced-Onto-Liangshan-by-Xi.html

15 "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force"*, Jamestown Foundation, Apr 2024.*

16 "Xi Purges Six More PLA Generals", Jamestown Foundation, Jul 2026; "The Chinese Military's New Information Support Force", *CNA,* Aug 2024.

17 Liang Xiuqiong, He Tao, and Wang Yue, “An Army Unit Strictly Regulates the ‘Social Circles’ of Its Leading Cadres”, *PLA Daily*, China Military Online, 23 May 2026, accessed 18 Mar 2026, http://www.81.cn/yw_208727/16462867.html

18 David M. Glantz, *Stumbling Colossus: The Red Army on the Eve of World War* (Lawrence: University Press of Kansas, 1998), 27–31.

19 Ibid.

20 “Who Are the Officers Filling the Big Shoes Left Behind in PLA Anti-Corruption Drive?”, *South China Morning Post*, 07 Aug 2026.

21 Suyash Desai, “Operational Continuity on the China-India Border Despite Purge”, in *Assessing Xi’s Unprecedented Purges of China’s Military*, Center for Strategic and International Studies, Feb 2026, https://www.csis.org/analysis/assessing-xis-unprecedented-purges-chinas-military-key-developments-and-potential

22 Bonny Lin et al., “The Purges Within China’s Military Are Even Deeper Than You Think”, ChinaPower, Center for Strategic and International Studies, 2026, accessed 18 Mar 2026, https://chinapower.csis.org/china-pla-military-purges/

23 “Who Are the Officers Filling the Big Shoes Left Behind in PLA Anti-Corruption Drive?”, *South China Morning Post*, 07 Aug 2026.

24 “Chinese HQ-9B, HQ-16 Air Defences and PL-15 Missiles Failed to Counter Indian Aerial Onslaught in Pakistan during Operation Sindoor: Report,” *Swarajya*, 18 May 2025, accessed 19 Mar 2026, https://swarajyamag.com/news-brief/chinese-hq-9b-hq-16-air-defences-and-pl-15-missiles-failed-to-counter-indian-aerial-onslaught-in-pakistan-during-operation-sindoor-report

25 “China’s Air Defence System HQ-9B Explained: How US-Israel Strikes Breached Iran’s Shield”, *India TV*, 01 Mar 2026, accessed 19 Mar 2026, https://www.indiatvnews.com/explainers/iran-air-defence-system-hq9b-explained-us-israel-strikes-2026-03-01-1032184

26 “Operation Absolute Resolve and the Future of Warfare: Military Lessons for India”, Manohar Parrikar Institute for Defence Studies and Analyses, 16 Jan 2026, accessed 20 Mar 2026, https://idsa.in/publisher/issuebrief/operation-absolute-resolve-and-the-future-of-warfare-military-lessons-for-india

27 China’s ICBM Test a Sign PLA Rocket Force Stands Ready Despite Corruption Scandals”, *South China Morning Post*, 26 Sep 2024, https://www.scmp.com/news/china/military/article/3280097/chinas-icbm-test-sign-pla-rocket-force-stands-ready-despite-corruption-scandals

28 "China's SLBM Test Underscores the Importance of a Ballistic Missile Launch Notification Agreement", Center for Strategic and International Studies, Jul 2026, accessed 20 Mar 2026, https://www.csis.org/analysis/chinas-slbm-test-underscores-importance-ballistic-missile-launch-notification-agreement

29 Timothy R. Heath, *The Chinese Military's Doubtful Combat Readiness* (Santa Monica, CA: RAND Corporation, 2023), accessed 20 Mar 2026, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA800/PEA830-1/RAND_PEA830-1.pdf

30 "Xi's Second Purge of China's Military", *MERICS*, Jan 2025; "Who Are the Officers Filling the Big Shoes Left Behind in PLA Anti-Corruption Drive?," *South China Morning Post*, 07 Aug 2026.

31 "PLA Navy Shifts Training Focus from Near-Shore to Blue-Water Operations", Jamestown Foundation, 26 Jul 2025.

The Three-Body Problem Trilogy: A Reflection of New China under Communism

Group Captain Sunny Vyas[@]

Abstract

This article uses Liu Cixin's Three-Body Problem trilogy and other contemporary literature on China as a lens to understand Chinese strategic culture under the Chinese Communist Party (CCP) and its implications for India's evolving security environment. It examines the philosophical and practical dimensions of this strategic culture and suggests ways to address the resulting threats. The analysis identifies several strategic concepts mirrored in both the trilogy and Chinese foreign policy, including the dark forest theory, surveillance and control, patience and deception, existential deterrence, and collective behaviour and mob mentality. From an Indian perspective, the article recommends analysing CCP behaviour as an expression of strategic culture, building institutional memory, developing credible military, economic, and technological deterrence, and recognising that security is 'Never Enough' and is an ongoing process requiring resilience, redundancy, and strategic depth across multiple domains.

[@]**Group Captain Sunny Vyas** was commissioned into the Aeronautical Engineering (Mechanical) branch of the Indian Air Force in Jan 2004. He is trained on IL-76/78 aircraft, has received Original Equipment Manufacturer training for the C-130J fleet, and is an alumnus of the Technical Staff Officers Course. He has held staff appointments at Air Headquarters and played a key role in concluding sustainment contracts for the C-130J and C-17 fleets.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

Introduction

India's rise over the last two to three decades has fundamentally altered its strategic environment and the focus of its anxieties. Earlier, public discourse often framed India's problems—terrorism, social unrest, political instability—as the work of an 'External Hand', usually shorthand for Pakistan. Today, while Pakistan remains a concern, the primary axis of competition has clearly shifted toward China, a far more complex and powerful challenger whose ambitions, methods, and worldview demand a more nuanced approach.

The China that India confronts under Chinese Communist Party (CCP) rule is not only a neighbour and rival but also a civilisational state that has reinterpreted Marxism as 'Socialism with Chinese characteristics'. This philosophy combines one-party rule with state-led capitalism and long-term strategic planning. Writers such as Vijay Gokhale and others in the Indian strategic community have highlighted how Beijing plays a 'Long Game', blending economic leverage, military modernisation, and psychological signalling to shape its environment over decades.

Yet the Indo–China relationship is not only about present-day rivalry. Historically, India has exercised a deep cultural influence on China—through Buddhism, ideas, trade routes, and intellectual exchange—as richly described by William Dalrymple in *The Golden Road*, his account of the subcontinent's connections with East Asia.[1] Modern Chinese nationalists, however, often downplay or recast such shared heritage, preferring narratives that centre China's uniqueness and continuity.

Against this backdrop, Liu Cixin's trilogy (*The Three-Body Problem*, *The Dark Forest* and *Death's End*)[2] becomes a useful lens to analyse Chinese strategic culture. It is not just a work of speculative fiction but a Chinese imagining—shaped by the traumas and ambitions of the People's Republic—of survival, power, and fear at a civilisational scale. When read alongside Sun Tzu's *The Art of War* and modern analyses of Chinese strategy, the trilogy offers Indian readers a way to grasp how 'New China under communism'

might think about the world, enemies and allies, and the cold calculations required in a universe it perceives as a 'Dark Forest'.

Introduction to The Three-Body Problem

The Three-Body Problem (TBP) is a landmark science fiction trilogy by Chinese author Liu Cixin, which won the Hugo Award for Best Novel in 2015[3], first Asian book to achieve the feat, and has a critically acclaimed series of the same name. It has been widely praised for blending rigorous science with large-scale political and philosophical questions. Although the author's relationship with the CCP is contested–in fact some portion of the book and series of the same name generated controversy in China for being critical of the CCP[4]–the trilogy is a useful lens through which to explore how the country's outlook has been shaped under CCP rule.

The story begins amid the upheaval of China's Cultural Revolution, then expands into a cosmic drama in which humanity confronts the Trisolarans, an alien civilisation. The Trisolarans come from a chaotic three-sun system whose unstable environment repeatedly brings them to the brink of extinction. The trilogy explores themes of civilisational survival, ideological struggle, technological acceleration, and interstellar conflict, making it one of the most influential sci-fi works of the 21st Century and a key window into contemporary Chinese speculative thought.

Historical and Ideological Foundations in TBP

The first book opens during the Cultural Revolution, when radicalised Red Guards publicly persecute scientists and intellectuals. This background highlights how ideological extremism, political purges, and suspicion of experts shaped modern China's governing mentality. The trauma of that era—fear, chaos, and the privileging of political loyalty over truth—reverberates throughout the trilogy in the form of distrust, tight control, and an overriding focus on regime and species survival.

The Trisolarans' looming threat and inescapable surveillance through a *Sophon* (a device) resonate with the Chinese leadership's sense of existing in a hostile environment, facing both external

pressures and internal instability, and the perceived need for pervasive surveillance to ensure regime survival. TBP thus transforms specific Chinese historical experiences into a universal story about how civilisations react when cornered. And the Sophon can be read as reflecting the pervasive surveillance that a dominant power may employ to suppress opposition. TBP also deals with the possibility of circumventing such surveillance–a 'Wallfacer' project[5] where strategies are made in the minds of the protagonist, the final domain beyond the reach of surveillance. These strategies are executed by a Swordholder.[6]

In *The Art of War,* Sun Tzu devotes an entire chapter, 'The Use of Spies',[7] to the idea that perfect information is the key to winning without fighting, urging rulers to cultivate multiple types of agents embedded everywhere, including among enemies and *their own people*.

The Dark Forest and the Chinese Worldview

In *The Dark Forest*, Liu introduces the 'Dark Forest' theory[8] - the universe is like a dark forest in which every civilization is a hunter who must hide because discovery may lead to annihilation. The concept echoes the Chinese diplomatic maxim of 'Hiding capabilities and biding time', especially during Deng Xiaoping's leadership, and reflects his cautious view of international politics: never assume others are benevolent, never fully reveal your capabilities, and always prepare for worst-case scenarios.

This also fits Sun Tzu's emphasis on obscuring one's intentions and strengths until the decisive moment.[9] This mindset explains the Chinese preference for ambiguity and indirectness in foreign policy—projecting moderation while quietly building power, avoiding unnecessary provocations, and assuming that other actors may harbour hostile intentions even when they speak of peace.

Patience, Deception, and Long-Term Timing

In TBP, the Trisolarans wait decades to move directly against Earth and use sophisticated deception to slow human progress, including distorting basic scientific research and spreading false theoretical 'Truths'. This long-term strategy of psychological warfare and

technological sabotage aligns with a broader Chinese tradition of strategic patience: accepting short-term constraints to create favourable conditions later.

A real-world parallel is the period leading up to the 1962 Sino-Indian war, when Chinese leaders projected a message of peace and coexistence even while preparing militarily. Beijing continued to speak the language of 'Peace' and 'Friendship' in diplomatic exchanges[10] and international forums even as it quietly massed forces, developed logistics infrastructure, and planned offensive operations across the Himalayas. Indian leaders, reassured by public Chinese statements and misreading the tempo of PLA movements, failed to grasp how far preparations had already advanced.

As later documented in accounts such as *Himalayan Blunder* by Brig JP Dalvi, Chinese forces had pre-constructed prisoner-of-war camps capable of holding thousands of Indian soldiers, redeployed large numbers of acclimatised troops, stockpiled ammunition along the frontier, recruited Tibetan porters, and even positioned interpreters proficient in multiple Indian languages months before hostilities began.[11] The combination of polite rhetoric and quiet preparation can be read as echoing the same pattern seen in TBP—surface calm masking deep planning.

In *Art of War*, Sun Tzu treats deception as the foundation of strategy, urging leaders to appear weak when strong, distant when near, and inactive when ready to strike, turning misperception itself into a weapon.[12] This logic fits closely with both CCP behaviour in episodes such as the 1962 war[13] and the Trisolarans' long campaign of misdirection and scientific sabotage in TBP, where open conflict is prepared under a cover of apparent calm and constraint.

Deterrence and Existential Will

TBP offers a radical model of deterrence. Facing destruction, Earth adopts a 'Dark Forest deterrence' posture, i.e., if attacked by Trisolaris, it will broadcast both civilizations' locations to the wider universe, inviting unknown, superior powers to destroy both of them. This is effectively a threat of mutual annihilation on a cosmic scale. Deterrence works only because both sides fear the consequences.[14]

This logic differs in an instructive way from early Mao-era nuclear doctrine, in which Chinese leaders publicly expressed willingness to accept enormous casualties rather than submit, thereby signalling that nuclear threats would not easily coerce them. In both TBP and Chinese strategic history, the credibility of deterrence comes from demonstrating a readiness to endure extreme sacrifice—deterring stronger adversaries by showing that the *cost of victory would be unbearable*.

History as Narrative and Validation

In *Death's End*, the narrative explains how people often use stories not to gain new strategic insight but to seek confirmation of what they already believe.[15] This tendency maps closely to how the CCP constructs and uses historical narrative: invoking the 'Century of Humiliation' and celebrating revolutionary victory and national rejuvenation as a way to legitimise current rule. TBP's observation that people prefer reaffirmation over uncomfortable truth can thus be read as a subtle reflection on the use of history in sustaining modern Chinese political identity.

In *Art of War*, Sun Tzu stresses the importance of unity between ruler, army and people, noting that a commander must ensure the troops 'are in accord with their ruler'[16] and that their morale is high before battle. In practice, this means telling a coherent story about why the war is necessary, just, and winnable. The CCP extends this logic into peacetime by using patriotic history, victimhood, and revival stories to align public sentiment with party goals.

Arrogance and Survival

A key idea of the trilogy is that weakness and ignorance are not fatal by themselves; arrogance is.[17] Civilisations can survive being technically backward or partially blind, as long as they remain cautious, adaptable, and self-aware. The truly deadly mistake is overestimating oneself and underestimating others.

This aligns with Sun Tzu's insistence that knowing oneself and the enemy is the foundation of victory and that overconfidence leads to ruin.[18] For a rising China, the implied lesson is the need for modesty in posture, realistic self-assessment and constant re-

evaluation. TBP thereby reinforces a core theme of Chinese strategic culture: the greatest danger is overconfidence.

Evolving Enemies and Transactional Alliances

Across the trilogy, the relationship between humans and Trisolarans shifts from uncompromising hostility to conditional collaboration when confronted with higher-level cosmic forces. Alliances are depicted as situational tools rather than permanent, value-based commitments.

This resonates with the CCP's pragmatic foreign policy. China's support for Pakistan against India, despite Pakistan's participation in anti-communist alliances like CENTO and SEATO during the Cold War[19], shows how Beijing can sidestep ideological contradictions when pursuing strategic goals. In this sense, TBP's flexible alignment logic matches a real-world Chinese pattern: 'Friend' and 'Enemy' are variables, not constants.

Mob Mentality, People's War, and Collective Transformation[20]

TBP also explores how collective behaviour can transform human morality. The opening Cultural Revolution scenes show mobs of students and citizens, inflamed by ideology, persecuting and even killing intellectuals. Individual conscience dissolves into collective fervour, and a group of people becomes a distinct, often more ruthless actor than any single person. This offers a more nuanced depiction of mob mentality.

This theme recurs in *The Dark Forest* and *Death's End* through the behaviour of isolated starship communities.[21] In *The Dark Forest*, crews aboard 'Escapist' or wandering ships, cut off from Earth and faced with limited resources, collectively decide to attack or destroy other human ships to secure their own survival. The decisions made by vote create a chilling picture of democracy under existential fear.[22]

In *Death's End*, a human 'Vagabond' ship that chose to abandon Earth in a previous crisis is later lured back under false pretences, and its crew is tried for crimes against humanity.[23] Here, both the original escape and the later deception and judgement[24] reveal how 'Collectives' redefine loyalty and treason, and how

majorities can recast survival choices as moral crimes once circumstances change.

These episodes show that when groups act under stress, they can become something qualitatively different—colder, more calculating, more willing to sacrifice outsiders or dissenters for collective survival. The trilogy thus dramatises the psychological and moral mechanics of mob and mass behaviour.

This directly connects to communist notions of 'People's War',[25] in which political and military struggles are waged by mobilising the masses as the primary force in protracted warfare. In Maoist practice, mass campaigns—whether against class enemies, during the Cultural Revolution, or in other movements—channelled collective energy to reshape society's direction. TBP suggests both the power and danger of such mobilisation: once activated, a crowd or a polity can endorse extreme measures, from purges to betrayal, that individuals might resist on their own.

How this analysis can help in International Relations with China

Strategic Culture

A useful way forward for engaged with the CCP in international relations is to treat its behaviour as the product of a strategic culture, much as C Christine Fair does for Pakistan in *Fighting to the End.*[26] In that book, she argues that Pakistan's military elite—and through them, much of the state and civilian strategic discourse—operate within a worldview in which resisting India's dominance is itself 'Victory', regardless of material cost. This *strategic culture* shapes not only the army's war-fighting choices but also the narratives that are internalised by large segments of the civilian population and political class, who repeatedly return to confrontational policies even when they are economically or diplomatically damaging.

By analogy, any serious strategy toward China must start from an understanding of the *CCP's strategic culture* rather than assuming it will behave like a typical status quo power i.e. a realist or an idealist. China's strategic culture draws on communist ideology, the 'Middle Kingdom'[27] civilisational narrative, Confucian moralism, a siege mentality about encirclement, and a strong realpolitik instinct.

Liu Cixin's TBP universe, when read together with this behaviour, suggests a CCP strategic culture with certain especially important features relevant to foreign policy:

- **Centrality and phases of interaction**. Communist China sees itself—as in both traditional 'Middle Kingdom' ideology and TBP's civilisational logic—as a central actor whose primary task is to survive, endure, and eventually shape the environment around it.[28]

- **Patience and timing**. TBP's Trisolarans, and Earth's later Dark Forest strategy, embody extreme patience and careful sequencing; they wait for the right 'Window' before acting decisively.[29] Modern Chinese doctrines like *tao guang yang hui*[30] (hide capabilities, bide time) and later 'Peaceful Rise' rhetoric resonate with the same phased, timing-sensitive approach. If this is correct, then the key to dealing with the CCP is not to expect linear, transparent behaviour, but to 'Catch China in the right phase of interaction'. Vijay Gokhale in his book *The Long Game,* painstakingly explains in detail the frustrating nature of Chinese negotiators.[31] He emphasise the need to build institutional memory of Chinese interactions and understanding long-term strategy, and cautions against interpreting short-term silence as acceptance of India's position.

In military terms, this may mean a sustained buildup of capability and intelligence with a forward-looking strategic mindset. Studying Chinese philosophy and communist ideology separately is important to understand which strand of Chinese strategic thinking is being addressed. The opponent has shown a tendency to alternate between the roles of a champion of people's war and a defender of an ancient civilisation. Recognising the distinction between these approaches and responding appropriately to each would be a significant step.

Deterrence

Deterrence emerges as another crucial thread linking TBP and CCP practice. In the trilogy, deterrence is not just about possessing destructive capability but about how credibly a side signals its willingness to use it and accept the consequences; Earth's Dark Forest deterrent works because it convinces Trisolaris that humanity will risk mutual annihilation rather than submit.[32] Mao's approach to nuclear deterrence followed a related but distinct psychological logic: publicly dismissing fear of nuclear strikes by insisting that people's war would continue even after the loss of major cities, while at the same time relentlessly pursuing China's own nuclear capability to ensure it could not be coerced or ignored.[33]

In recent years, China has experimented with new forms of economic coercion beyond military power, notably signalling potential leverage over rare earth supplies in disputes with advanced economies, including the United States[34] and Japan.[35] These episodes illustrate that Beijing views critical economic and technological chokepoints as tools for shaping adversary behaviour, much like strategic weapons. For other states, especially India, the TBP lens suggests two imperatives: first, to identify what forms of deterrence can be credibly brought to bear on China—whether military, economic or technological—and second, to anticipate how the CCP's strategic culture will interpret and respond to those deterrent signals. Understanding both sides of that equation through game theory, is essential to avoid miscalculation in a real-world 'Dark Forest' where misread deterrence can trigger the very escalation it aims to prevent.

When Enough is Enough

Security in the TBP universe, as in real geopolitics, has no end state; it is an open-ended pursuit where 'Enough' is never truly enough. In *The Dark Forest*, Earth's most advanced space defences and deterrent systems are destroyed in moments once a superior force decides to act[36], underscoring how quickly painstaking security architectures can be rendered obsolete by qualitative shifts in capability or intent.

Taken together, these examples highlight a hard truth that TBP dramatises on a cosmic scale: security requirements expand with context, threat perception, and technological change, and cannot be 'Completed' in any stable, permanent sense. There is always another layer of vulnerability, another dependency, another domain—space, cyber, critical minerals, sea lanes—where a state can be surprised or coerced. The bottom line is that security is an ongoing process of adaptation and prioritisation rather than a fixed end state; accepting that it is 'Never Enough' is not a counsel of despair but a reminder to build resilience, redundancy, and strategic depth into any long-term defence.

Conclusion

This article attempts to show that in international affairs, Chinese realism is a sharp reflection of the Dark Forest theory. The historical aspect of people's war, and existential aspect of 'Socialism with Chinese Character',[37] is a veil that needs to be kept in mind while dealing with the CCP. The Three Body Problem trilogy is a seminal work which is a reflection of these characteristic and a code breaker of how to deal with such a problem. The reader is left to consider how such patience and concealment might be interpreted and countered.[38]

Endnotes

1 William Dalrymple, *The Golden Road* (Bloomsbury, 2024), 151–56.

2 Liu Cixin, *The Three-Body Problem*, trans. Ken Liu (Tor Books, 2014).

3 Hugo Awards, "The 2015 Hugo Awards", accessed 18 Mar 2026, https://awardshelf.com/award/hugo-award/2015/.

4 "Netflix's 3 Body Problem Faces Controversy in China", CBR, https://www.cbr.com/netflixs-3-body-problem-faces-controversy-in-china/

5 Liu Cixin, *The Dark Forest*, trans. Joel Martinsen (Tor Books, 2015), 96.

6 Liu Cixin, *Death's End*, trans. Ken Liu (Tor Books, 2016), 118.

7 Sun Tzu, *The Art of War*, trans. Lionel Giles (1910), chap. 13, "The Use of Spies".

8 Liu, *The Dark Forest*, 487.

9 Sun Tzu, *The Art of War*, chap. 5, “Energy”.

10 J. P. Dalvi, *Himalayan Blunder* (Thacker & Company, 1969), 53–54, 76.

11 Dalvi, *Himalayan Blunde*r, 152–54.

12 Sun Tzu, *The Art of War*, chap. 1, “Laying Plans”.

13 Dalvi, *Himalayan Blunder*, 147.

14 Liu Cixin, *Death’s End*, 169.

15 Liu, *Death’s End*, 326. “All of these groups tried to interpret the stories according to their own political aims and self-interest, and disseminate propaganda”.

16 Sun Tzu, *The Art of War*, chap. 1, “Laying Plans”.

17 Liu Cixin, *Death’s End*, 450.

18 Sun Tzu, *The Art of War*, chap. 3, “Attack by Stratagem”.

19 *“Foundational Basics of Pak-China Strategic Relations”, Pakistan Today, 27* Oct 2019, *accessed 18 Mar 2026, https://www.pakistantoday.com.pk/2019/10/27/foundational-basics-of-pak-china-strategic-relations.*

20 Liu Cixin, *The Dark Forest*, 455–60. “The birth of a new civilization is the formation of a new morality”.

21 Liu Cixin, *The Dark Forest*, 461. “The new space humans had passed through their infancy”.

22 Liu Cixin, *The Dark Forest*, 101.

23 Liu Cixin, *The Dark Forest*, 98.

24 Liu Cixin, *The Dark Forest*, 101.

25 “People’s War,” ProleWiki, accessed 19 Mar 2026, https://en.prolewiki.org/wiki/People%27s_war

26 C. Christine Fair, *Fighting to the End* (Oxford University Press, 2014), 279–81.

27 Henry Kissinger, *On China* (Penguin Press, 2011), 27.

28 Kissinger, *On China*, 20.

29 Liu Cixin, *Death’s End*, 168–69.

30 “Deng Xiaoping’s ‘24-Character Strategy’”, GlobalSecurity.org, accessed 19 Mar 2026, https://www.globalsecurity.org/military/world/china/24-character.htm

31 Vijay Gokhale, *The Long Game* (Penguin Random House, 2021), 131–60.

32 Liu Cixin, *The Dark Forest*, 505.

33 Kissinger, *On China*, 108.

34 "Rare Earths, Trade and Pressure Tactics: How China Holds a Powerful Card against Trump," Moneycontrol, accessed 20 Mar 2026, https://www.moneycontrol.com/world/rare-earths-trade-and-pressure-tactics-how-china-holds-a-powerful-card-against-trump-explained-article-13918158.html

35 "China Cuts Japan off from Some Materials amid Diplomatic Spat", *Mining Weekly,* accessed 20 Mar 2026, https://www.miningweekly.com/article/china-cuts-japan-off-from-some-materials-amid-diplomatic-spat.

36 Liu Cixin, *The Dark Forest*, 433.

37 "Adapting Marxism to the Chinese Context: A Glorious Chapter in CPC's Hundred-Year History", *Qiushi Journal, 08* Sep 2021, accessed 20 Mar 2026, https://en.qstheory.cn/2021-09/08/c_657826.htm

38 "Deciphering Xiaokang Along the India-China Border", Indian Council of World Affairs, accessed 20 Mar 2026, https://www.icwa.in/show_content.php?lang=1&level=1&ls_id=10993&lid=6989

Artificial Intelligence in the Defence Sector: A Comparative Analysis of the United States, China, and India

Dr Salam Binodkumar Singh[@]

Abstract

This article examines how Artificial Intelligence (AI) is rapidly transforming the defence sector by reshaping military operations, decision-making, intelligence, surveillance, autonomous systems, logistics, cyber warfare, and training. It compares the development and adoption of AI in the defence sectors of the United States (US), China, and India, with particular emphasis on their technological capabilities, investment patterns, institutional frameworks, and strategic approaches. The study also examines the technical, operational, ethical, legal, and institutional challenges of military AI, including algorithmic bias, data security, accountability, human oversight, interoperability, and compliance with International Humanitarian Law. It argues that India's strategic response should focus on indigenous Research and Development, public-private partnerships, secure defence datasets, high-performance computing, edge AI, autonomous systems, skilled human resources, and trustworthy AI frameworks. The article concludes that India can narrow its capability gap not by replicating the scale of the US and China, but by pursuing a focused,

[@]**Dr Salam Binodkumar Singh** scholar is a guest faculty member in the Department of National Security Studies at Manipur University, Manipur. After completing his PhD in 2012 from the Department of Defence and National Security Studies at Punjab University, Chandigarh, the scholar joined the Institute for Conflict Management, New Delhi, and worked as a research associate until Apr 2022. Over the past 14 years, the scholar has published ten articles in refereed journals and ten chapters in edited books and presented eight papers at national and international conferences.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

self-reliant, and human-centred AI strategy aligned with its specific defence requirements and national security priorities.

Introduction

Artificial Intelligence (AI) is a major force behind the current technological revolution in defence. As AI increasingly transforms modern warfare, global powers are increasing investments in Research and Development (R&D) than ever before. AI's considerable potential is transforming military planning, operations, and decision-making. The future battlefield is likely to be shaped as much by computing power and algorithms as by conventional weapon systems.[1] AI is becoming a key part of next-generation military capabilities, as warfare moves toward greater accuracy, speed, and automation. AI's true strength is in changing how people make decisions, how aware they are of their surroundings, and how much control they have over the systems.[2]

The application of AI in defence is expanding across the tactical, operational and strategic levels.[3] One such application is real-time analysis of intelligence gathered by drones, satellites, and ground sensors, providing commanders with enhanced situational awareness in complex operational environments. AI is also used extensively in cyber-defence and Electronic Warfare (EW) to detect anomalies, prevent intrusions, and adapt communication protocols. At the same time, AI-supported training simulations and other user-behaviour-based scenarios are helping prepare forces for combat situations.[4]

Notably, the global military AI market reached USD 9.82 bn in 2025 and is expected to reach USD 41.58 bn by 2035.[5] Indeed, militaries are racing to adopt AI to gain military advantage over competitors. Nevertheless, little is understood about AI's long-term impact on warfare. As militaries continue to pursue AI, leaders should be aware of the significant risks that could come with its adoption.[6] At the same time, AI-enabled systems—drones, autonomous platforms, and lethal autonomous weapons—are raising complex legal questions about the application of existing international humanitarian law and the

need for additional rules governing autonomous weapon systems. Therefore, identifying the legal consequences of AI's swift adoption and examining existing rules of international law through the lens of this technology is crucial.[7]

In this context, this article examines how AI is changing military operations to boost efficiency, enhance decision-making, and improve personnel safety and effectiveness. The paper's primary contribution is a comparative overview of AI trajectories in the defence sectors of the United States (US), China, and India, highlighting their major defence AI projects. It also discusses operational, ethical, legal, and institutional impediments to military AI adoption. Lastly, the paper outlines strategic directions to strengthen AI in India's defence sector.

Military Application of Artificial Intelligence

AI is applied in a wide spectrum of military tasks—from operational planning to medical response—improving efficiency and potentially reducing some forms of human error. For this analysis, military applications of AI are grouped into eight broad categories: command and control; intelligence, surveillance and reconnaissance; simulation and training; automated target recognition; autonomous systems and vehicles; information operations and EW; predictive maintenance and logistics; and medical applications.[8]

In sum, AI is reshaping military operations by improving efficiency, decision-making, personnel safety, and mission effectiveness. It augments human capabilities, helping armed forces adapt more swiftly to evolving threats. To conceptualise AI's role, there is a need to separate its impact on warfighting from its role in preparing for war. Warfighting comprises active combat—dynamic and unpredictable, marked by friction and the fog of war—where adaptability is essential.[9]

By contrast, preparing for war includes force development, technological innovation, production, and logistics. AI could influence preparation by improving production efficiency and enabling the design of novel military capabilities.[10] Meanwhile, Integrating AI into autonomous systems can improve performance in specified tasks,

provided the systems are adequately tested and remain reliable under operational conditions. The central debates about autonomy and Machine Learning (ML) in weapons concern definitions and implications. 'Autonomy' typically refers to a machine's capacity to carry out intended tasks without human intervention, using sensors and software. 'ML' is an approach in which models learn patterns from data to perform specified tasks through various methods.[11] Both fall under the AI umbrella and are often used together.

Michael C Horowitz, a leading expert on AI, defence policy, and international security, views AI as a general-purpose technology comparable to electricity or the combustion engine, meaning its ultimate impact on warfare is shaped by organisational use and human-machine teaming rather than software capabilities alone. In his work on strategic stability, such as *Artificial Intelligence and the Future of Strategic Stability*, he highlights risks from machine-speed conflict, automation bias, and integrating AI into sensitive domains like nuclear command and control.[12]

Comparative Analysis of United States, China and India

According to Stanford University's 2025 AI Vibrancy Index, India ranked third, behind the US and China, in Stanford Human-Centred Artificial Intelligence's 2025 Global AI Vibrancy Tool.[13] India's position stems from a strong talent base, a growing start-up ecosystem, and rising AI research and patent activity. However, despite its strengths in talent, start-ups, and R&D, India remains a 'Distant Third,' substantially trailing the top two in areas such as infrastructure and investment. The gap between India and major military powers is stark. The defence sectors of the US, China, and India are experiencing a rapid surge in AI spending as part of a global, algorithm-driven military revolution. The US leads in investment, focusing on autonomous systems and AI models free from vendor-imposed ethical restrictions. China is aggressively advancing through 'Military-civil Fusion', while India is rapidly accelerating its domestic defence AI ecosystem, focusing on surveillance and autonomous systems.[14]

United States

- The US has pursued a measured and incremental strategy in integrating AI into its defence architecture, with an emphasis on human oversight and ensuring interoperability within existing military systems. This cautious approach has largely stemmed from its historical dominance in technological innovation and leadership. However, amid an evolving geopolitical environment, particularly amid strategic competition with China, the US faces significant challenges in sustaining its leadership in the military application of AI. In light of these developments, the US faces a critical policy dilemma: whether to maintain its trajectory or adopt a more assertive posture toward the militarisation of AI to preserve its strategic advantage.[15]

- Consequently, the US Department of Defence (DoD) continued to prioritise AI and autonomous systems in its Financial Year 2026-27 spending plans, earmarking approximately USD 13.4 bn, alongside broader investments in information technology, cybersecurity, advanced weapons and defence modernisation. The Pentagon is prioritising AI, autonomous technology, and cybersecurity in its 2026 budget, aiming for rapid experimentation and deployment. The DoD's total information technology budget in 2026 is projected to increase by USD 1.8 bn over 2025 levels.[16] The US continues to shift toward AI-enabled warfare to maintain a technological advantage over competitors. Moreover, a 2026 directive encourages AI models without 'Vendor-imposed ethical guardrails', signalling an acceleration toward rapid, unconstrained deployment.[17]

- In Jan 2026, US President Donald Trump proposed increasing military expenditure to USD 1.5 tn in 2027 as part of his vision for a 'Dream Military', stating "It is an especially troubled and dangerous time".[18] It would result in a 50 per cent increase in the nation's military budget as a result of growing concerns within the Pentagon about China's advances in the field of AI. In the US-China competition to develop new technologies, AI has increasingly been used as a weapon in itself.[19]

China

- China is strategically leveraging AI as a central element of its Military-Civil Fusion strategy, aiming to achieve dominance in autonomous systems, cyber warfare, and surveillance technologies, among others. In contrast to the US, where AI innovation is predominantly driven by private sector enterprises, China adopts a more state-directed approach that integrates civilian AI research with military applications over a prolonged time period. This integration fosters more cohesive and rapid development of AI technologies for defence purposes, giving China a potentially significant advantage in emerging domains of warfare.[20] The People's Liberation Army seeks not only to equal but also to overtake the US military by seizing the initiative in the ongoing Revolution in Military Affairs.

- The Chinese government allocated CYN 1.78 tn (USD 245.2 bn) to its military budget for 2025, making China the world's second-largest military spender, after the US as the world's second-highest military spender.[21] For 2026, China plans to allocate CNY 1.94 tn (USD 282 bn), up 6.9 per cent from the previous year, continuing 11 straight years of single-digit growth to modernise technology like AI.[22] While the total budget grows, China's 2025 AI-specific capital expenditure is expected to reach up to USD 98 bn, with significant investment aimed at military AI, biotechnology, and autonomous systems to counter the US.[23]

- Chinese military leaders believe the form of warfare is changing from today's 'Informatised' warfare to future 'Intelligentised' warfare.[24] China is rapidly expanding its military technology through major investments in 6th generation fighters, stealth drones, and 500-ton stealth drone ships.[25] On 05 Mar 2026, China unveiled major development targets in its five-year plan for 2026-2030. The country aims to seize the commanding heights of science and technological development and achieve decisive breakthroughs in key core technologies.[26] Notably, in order to gain technological

dominance by 2035, Chinese President Xi Jinping, on 08 Jul 2026, asked Chinese scientists and engineers to make the country a leading power in science and technology by 2035 to achieve high-level self-reliance.[27]

India

- India initiated its defence AI efforts in Feb 2018 by forming a Task Force on AI under the Ministry of Defence (MoD). In Feb 2019, based on the recommendations of the task force, the Defence Artificial Intelligence Council and the Defence AI Project Agency were established.[28] In Aug 2019, an AI roadmap for Defence Public Sector Undertakings (DPSUs) was released. The MoD showcased AI adoption at the 'AI in Defence' symposium and exhibition in 2022. At the event, Defence Minister Shri Rajnath Singh unveiled 75 products that were made with the help of DPSUs, private companies, universities and research organisations.[29] Later, in Oct 2024, the Defence Research and Development Organisation (DRDO) launched the Evaluating Trustworthy AI Framework, a risk-based assessment model designed to integrate safe, secure, and reliable AI into critical defence operations.[30]

- India has allocated a record INR 7.85 lakh cr (USD 93.5 bn) to the MoD for the fiscal year 2026–27, marking a 15.19 per cent increase from the previous year.[31] While AI does not yet feature as a separate budget head in India, reports estimate roughly INR 100 crore per year earmarked explicitly for military AI projects, supplemented by broader national allocations like the INR 1,000 cr India AI Mission.[32] DRDO laboratories such as the Centre for Artificial Intelligence and Robotics (CAIR) are working on AI-enabled unmanned aerial vehicles, humanoid robots, and secure indigenous defence software for secure battlefield communication and information management systems.[33] A notable CAIR accomplishment is the AI techniques for net centric operations project, a modified technology group for knowledge-based creation, semantic information handling, inference reasoning, and event correlation.[34] Other notable CAIR projects are the multi-agent

robotics framework, such as the 'Wall Climber' robots and 'Snake Robots'.[35]

- Indeed, India is accelerating AI adoption in defence to boost operational efficiency, surveillance, decision-making, and self-reliance in future warfare. In Sep 2025, India released a 15-year defence roadmap (2025–2040) focused on AI, hypersonic technologies and capabilities for future warfare, charting a major modernisation path to address emerging challenges over the coming decades.[36] By Feb 2026, the MoD had signed 548 contracts under the Innovations for Defence Excellence (iDEX) initiative covering AI, autonomy, and other advanced technologies, engaging more than 676 startups, micro, small, and medium enterprises and individual innovators.[37] A total of 106 AI-based projects have been recognised, while 40 AI-based tools have entered defence operations.[38] India is pursuing a multi-layered security approach, prioritising 75 projects centred on AI, drone swarms, and cybersecurity, emphasising indigenisation as part of the *Atmanirbhar Bharat* (Self-Reliant India) drive.[39]

In comparison, the US, China, and India differ significantly in their military AI capabilities, budget scale, and strategic doctrines. The US has a long history of integrating AI into its defence strategy and maintains a massive computational and financial advantage. China has achieved parity or near-parity with the US in specific domains, supported by substantial state funding. India currently lags behind the US and China in raw computational power and operates with a significantly smaller defence AI budget. However, India manages its military AI shortcomings through a phased capability roadmap, institutional oversight, and a push for domestic technological self-reliance.

Challenges in the Use of Artificial Intelligence in Defence

Implementing AI in defence offers significant benefits, but it also presents challenges across technical, ethical, legal and operational domains. Technical challenges include ensuring data security, addressing algorithmic bias, meeting heavy computational demands,

and maintaining system reliability in unpredictable combat environments.[40] Ethical challenges include the potential erosion of human oversight and accountability in lethal decisions, biased targeting outcomes, and difficulties in assigning responsibility for potential war crimes.[41] The legal challenges include accountability for autonomous actions, adherence to International Humanitarian Law, and biases embedded in algorithms.[42] Operational challenges include limited transparency, scarcity of labelled training data, algorithmic bias, and integration issues with legacy systems.[43]

Indeed, India's aspirations to become a leading centre for AI and deep technology face several systemic barriers. Institutional fragmentation within India's AI landscape creates significant gaps in funding, compute infrastructure, and regulatory uncertainty. Competition among government bodies, fragmented regulatory jurisdictions, and hardware dependence disperse resources, create unequal regional deployment, and hinder scaling indigenous AI technologies.[44] On the other hand, India's dependence on imported AI semiconductors and limited domestic manufacturing capacity create severe supply chain and geopolitical vulnerabilities as dependency on foreign manufacturers undermines the strategic independence of India and the safety of its digital infrastructure.[45]

Moreover, despite its vast digital public infrastructure (DPI), much of its unique data remains unutilised, disconnected, and largely untapped by local startups.[46] Additionally, in India, bureaucratic hurdles and inter-service rivalries slow down the process of incorporating AI into defence. The core problem appears to be bringing civilian scientific capacity together with armed forces organisations.[47] Another problem is the retention of AI talent in India. 2025 'Global AI Vibrancy Ranking', India leads the globe in relative AI skill penetration. Nevertheless, the country continues to experience an outflow of AI talent, as professionals seek better opportunities abroad.[48]

Strategies to Strengthen Artificial Intelligence in Indian Defence

Strengthening AI capabilities within India's defence sector requires greater indigenous R&D, stronger public-private partnerships, and robust data and digital infrastructure to create secure, dependable, and intelligent systems.

The key strategies to improve AI in Indian Defence are as follows:

- **Foster Indigenous Innovation and Partnerships**. Bridge gaps between DRDO, DPSUs, and private tech firms to enable agile development. Scale up startup funding via iDEX to accelerate solutions in AI, sensor systems, and autonomous unmanned platforms.[49]

- **Strengthen Data and Digital Infrastructure**. Build a secure national repository of labelled, defence-relevant data to train algorithms while ensuring data sovereignty. Invest in domestic high-performance computing centres and consider indigenously designed semiconductors for sensitive defence workloads.[50]

- **Focus Areas for Deployment**. Deploy AI-based image-analytics systems (e.g., Agni-D) for real-time border monitoring and threat detection. Develop AI-enabled swarm drones for collaborative surveillance and target identification.[51]

- **Institutional and Human Resource Development**. Empower Defence AI Project Agency to set AI development standards, standard operating procedures, and intellectual property rights policies. Introduce specialised AI courses across defence training institutions.[52]

- **Ethical AI Frameworks**. Maintain human-in-the-loop architectures for critical life-or-death decisions. Through initiatives such as Moral and Ethical Systems, Accountable Governance, National Sovereignty, Accessible and Inclusive, and Valid and Legitimate (MANAV), India aims to promote an AI trajectory that advances both technology and human welfare.[53]

- **Strategic Initiatives**. Strengthen military decision-making with wargaming and simulation at centres such as the Wargame Research and Development Centre, recognising wargaming's growing role in operational planning, leadership development, and doctrinal innovation for multi-domain operations.[54]

Given India's current limitations in matching the scale of datasets available to the US and China, its defence sector and deep tech startups are pivoting towards smaller language models and edge AI to create smarter battlefield systems. India's long-term strategy should emphasise indigenous AI models tailored to domestic defence datasets and operational requirements. India can improve AI in its defence sector by accelerating R&D, building a sovereign military data cloud, and fostering industry-academia collaboration. Sarvam AI is a notable example selected under the the IndiaAI Mission's IndiaAI Innovation Centre pillar to build foundational models for Indian languages and public services for start-ups, academia, research institutions, and industry.[55]

Conclusion

AI has emerged as a transformative force in the defence sector, reshaping military operations, decision-making, intelligence, surveillance, logistics, cyber operations, and autonomous systems. The comparative analysis of the US, China, and India demonstrates that AI is increasingly becoming an important component of military power and strategic competition. However, the trajectory of AI adoption differs significantly among the three countries because of differences in technological capacity, financial resources, institutional structures, and strategic priorities.

For India, the central challenge is not merely to replicate the AI capabilities of the US or China, but to develop an indigenous, context-specific defence AI ecosystem. This requires greater investment in domestic R&D, high-performance computing, secure defence datasets, semiconductor capabilities, and AI talent. Stronger cooperation among DRDO, the armed forces, DPSUs, universities, start-ups, and established technology companies is equally

necessary. Institutional mechanisms should also be strengthened to establish common standards, testing procedures, accountability mechanisms, and responsible AI principles across defence applications.

Endnotes

1 "Artificial Intelligence (AI) in Defence", *European Commission*, Dec 2025, accessed 15 Mar 2026, https://defence-industry-space.ec.europa.eu/system/files/2025-12/Factsheet%20AI%20in%20Defence.pdf

2 Denise Garcia, "AI in military decision-making", *Global Catastrophic Risks 2026*, accessed 17 Mar 2026, https://globalchallenges.org//app/uploads/2025/12/GCF-Risk-report-2026-Risk-4-.pdf

3 Roberto Poli, ed., *Handbook of Futures Studies* (Cheltenham, UK: Edward Elgar Publishing, 2024), 432

4 *KPMG*, "Artificial Intelligence (AI) in Defence Modernisation", 23 Jun 2025, accessed 20 Mar 2026, https://kpmg.com/in/en/blogs/2025/06/artificial-intelligence-in-defence-modernisation.html

5 Sai Teja Thota, "Military AI Market Size, Share, Growth, Trends and Forecast 2026–2035", *DataM Intelligence*, 13 Aug 2026, accessed 25 Aug 2026, https://www.datamintelligence.com/research-report/military-ai-market

6 Paul Scharre, "The Militarization of Artificial Intelligence", *Texas National Security Review*, roundtable, 02 Jun 2020, 35–43.

7 Jaemin Lee, *Artificial Intelligence and International Law* (Singapore: Springer, 2022), 2.

8 Kurtis H Simpson et al., "Militarizing AI: How to Catch the Digital Dragon?", *Centre for International Governance Innovation*, 26 Feb 2025, accessed 25 Aug 2026, https://www.cigionline.org/articles/militarizing-ai-how-to-catch-the-digital-dragon/

9 Soumya Awasthi, "Artificial Intelligence and India's National Security", *Raisina Debates*, ORF, 28 Mar 2026, accessed 29 Mar 2026, https://www.orfonline.org/expert-speak/artificial-intelligence-and-india-s-national-security

10 Zachary Burdette, et. al., “How Artificial Intelligence Could Reshape Four Essential Competitions in Future Warfare”, *RAND*, 22 Jan 2026, accessed 30 Mar 2026, https://www.rand.org/pubs/research_reports/RRA4316-1.html

11 Vincent Boulanin and Maaike Verbruggen, “Mapping the Development of Autonomy in Weapon Systems”, *SIPRI*, Nov 2017, accessed 03 Apr 2026, https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf

12 Michael C Horowitz, “Artificial Intelligence and the Future of Strategic Stability”, *Texas National Security Review*, Vol. 9, Issue 2, 09 Mar 2026. pp. 66–83.

13 IANS, “India Ranks 3rd in AI Competitiveness after US and China”, *NDTV*, 14 Dec 2025, accessed 05 Apr 2026, https://www.ndtv.com/world-news/india-ranks-3rd-in-ai-competitiveness-after-us-and-china-stanford-university-report-9806521

14 Ajay Vaishnav, “Military power is shifting from weapons to algorithms, says defence research paper on India’s AI doctrine”, *CNBC TV18*, 19 Feb 2026, accessed 10 Apr 2026, https://www.cnbctv18.com/technology/military-power-is-shifting-from-weapons-to-algorithms-says-defence-research-paper-on-indias-ai-doctrine-19854066.htm

15 Arpan Chakravarty, “ilitary Application of Artificial Intelligence: A Case Study of Ecosystem in United States, China, and India”, *India Foundation*, Jun 2025. P.10.

16 Chris Borges and Yutong Deng, “Innovation Lightbulb: Federal R&D Funding Matters for U.S. AI Leadership”, *Center for Strategic and International Studies*, 22 Oct 2025, accessed 13 Apr 2026, https://www.csis.org/blogs/innovation-lightbulb-federal-rd-funding-matters-us-ai-leadership#:~:text=As%20stated%20in%20the%20White%20House's%20AI,progress%20in%20AI%2C%20including%20investments%20in%20R&D.

17 David Jeans and Deepa Seetharaman, “Pentagon pushing AI companies to expand on classified networks, sources say”, *Reuters*, 12 Feb 2026, accessed 15 Apr 2026, https://www.reuters.com/business/pentagon-pushing-ai-companies-expand-classified-networks-sources-say-2026-02-12/

18 Osmond Chia, “Trump calls for US military spending to rise more than 50% to $1.5tn”, *BBC*, 08 Jan 2026, accessed 17 Apr 2026, https://www.bbc.com/news/articles/cy59kxl2xwzo

19 Lucy Quaggin, “The AI race: US and China defence sectors emerge as key battlegrounds”, *South China Morning Post*, 05 Feb 2026, accessed 19 Apr 2026, https://www.scmp.com/news/us/diplomacy/article/3342412/us-and-china-defence-sectors-emerge-key-battlegrounds-race-ai

20 Chakravarty, “Military Application of Artificial Intelligence”, 14.

21 *Quaggin,* ‘The AI race.’

22 Reuters, “China lifts military budget to modernize weapons, defence technology”, *Reuters*, 10 Mar 2026, accessed 25 Apr 2026, https://www.reuters.com/world/asia-pacific/china-lifts-military-budget-modernize-weapons-defence-technology-2026-03-10/

23 Annual Report to Congress: “Military and Security Developments Involving the People’s Republic of China 2025”, *U.S. Department of Defence*, accessed 26 Apr 2026, https://media.defense.gov/2025/dec/23/2003849070/-1/-1/1/annual-report-to-congress-military-and-security-developments-involving-the-peoples-republic-of-china-2025.pdf

24 Elsa B Kania, ‘Artificial Intelligence in China’s Revolution in Military Affairs’, *Journal of Strategic Studies*, Vol. 44, No. 4, 2021. pp. 515–542.

25 William Zheng, “China unveils ‘Killer Whale’ stealth drone ship”, *South China Morning Post*, 10 Nov 2024, accessed 26 Aug 2026, https://www.scmp.com/news/china/military/article/3285955/china-unveils-killer-whale-stealth-drone-ship

26 Laurie Chen and Eduardo Baptista, “China's new five-year plan calls for AI throughout its economy, tech breakthroughs”, *Reuters*, 05 Mar 2026, accessed 27 Apr 2026, https://www.reuters.com/world/asia-pacific/china-vows-accelerate-technological-self-reliance-ai-push-2026-03-05/

27 PTI, “Make China leading power in sci-tech by 2035: Xi tells scientists”, *The Hindu*, 08 Jul 2026, accessed 26 Aug 2026, https://www.thehindu.com/news/international/make-china-leading-power-in-sci-tech-by-2035-xi-tells-scientists/article71198311.ece

28 PIB, “Task Force for Implementation of AI”, *Ministry of Defence*, Government of India, 28 Mar 2022, accessed 29 Apr 2026, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1810442&reg=3&lang=2

29 Manoj Joshi, “AI in Modern Warfare: India’s Strategic Challenges and Opportunities”, *Raisina Debates,* ORF, 27 Feb 2026, accessed 01 May 2026, https://www.orfonline.org/expert-speak/ai-in-modern-warfare-india-s-strategic-challenges-and-opportunities

30 PIB, “Framework & Guidelines to integrate Trustworthy AI into critical defence operations unveiled”, *Ministry of Defence*, Government of India, 17 Oct 2024, accessed 07 May 2026, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2065847&reg=3&lang=2

31 J Paul Zachariah, "Analysing India’s Defence Allocation in Budget 2026-27: Modernisation in the Shadow of Operation Sindoor”, *Centre for Public Policy Research*, 03 Feb 2026, accessed 26 Aug 2026, https://www.cppr.in/archives/analysing-india-defence-budget-2026-27-post-operation-sindoor

32 Anand Singha, “Budget 2026: Not just big guns, the real test of Bharat's defence will be dictated by its modern muscle”, *The Economic Times*, 21 Jan 2026, accessed 26 Aug 2026, https://economictimes.indiatimes.com/news/defence/budget-2026-defence-allocations-artificial-intelligence-ai-not-just-bug-guns-but-real-indias-modern-muscle-on-focus/articleshow/126929053.cms?from=mdr

33 “Centre for Artificial Intelligence and Robotics (CAIR)”, Indian Science, Technology, and Innovation Portal, *Department of Science and Technology*, Government of India, accessed 11 May 2026, https://www.indiascienceandtechnology.gov.in/organisations/ministry-and-departments/defence-research-and-development-organisation-drdo-govt-india/centre-artificial-intelligence-robotics-cair

34 P. K. Chakravorty, “Artificial intelligence and its impact on the Indian armed forces”, *Indian Defence Review*, 05 May 2017, accessed 13 May 2026, https://indiandefencereview.com/artificial-intelligence-and-its-impact-on-the-indian-armed-forces/

35 Petr Topychkanov, “The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk”, *SIPRI*, Apr 2020, accessed 14 May 2026, https://www.sipri.org/sites/default/files/2020-04/impact_of_ai_on_strategic_stability_and_nuclear_risk_vol_iii_topychkanov_1.pdf

36 Shivani Sharma, “India unveils 15-year defence plan”, *India Today*, 05 Sep 2025, accessed 16 May 2026, https://www.indiatoday.in/india/story/india-15-year-defence-plan-ai-hypersonic-next-generation-warfare-2782430-2025-09-05

37 PIB, “India must become global hub of drone manufacturing in next few years amid current geopolitical instability: Raksha Mantri at National Defence Industries Conclave 2026”, *Ministry of Defence*, Government of India, 19 Mar 2026, accessed 17 May 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2242398&reg=3&lang=2

38 Mohd Asif, “India is Developing AI in National Security and Defence”, *Impact and Policy Research Institute*, 02 Mar 2025, accessed 21 May 2026, https://www.impriindia.com/insights/india-ai-security-defence/

39 Antoine Levesques, “Early steps in India’s use of AI for defence”, *IISS*, 18 Jan 2024, accessed 04 Jun 2026, https://www.iiss.org/online-analysis/online-analysis/2024/01/early-steps-in-indias-use-of-ai-for-defence/

40 Pooja Awasthi, “Artificial Intelligence in Future Defense Systems: Opportunities, Risks, and Ethical Challenges”, *Journal of Applied Bioanalysis*, Vol. 11, No. 11, Dec 2025. pp. 1079-1087.

41 Mariarosaria Taddeo and David Sutcliffe, “The Ethics of Artificial Intelligence in Defence”, *Oxford Internet Institute,* University of Oxford, 03 Feb 2025, accessed 26 Aug 2026, https://www.oii.ox.ac.uk/the-ethics-of-artificial-intelligence-in-defence/

42 Amir Rabet, “Artificial Intelligence and International Law: Challenges and Opportunities”, *Legal Studies in Digital Age*, Vol. 5, Issue 1, Jan 2026. pp. 1-15.

43 John Cerulli, “Challenges Facing the Military's Use of AI at the Tactical Edge”, *Forbes*, 12 Nov 2024, accessed 26 Aug 2026, https://www.forbes.com/councils/forbesbusinesscouncil/2024/11/12/challenges-facing-the-militarys-use-of-ai-at-the-tactical-edge/

44 Sejal Gupta, “India’s AI Regulation at the Crossroads: A Comprehensive Law or a Sectoral Mosaic?”, *Journal of Development Policy and Practice*, Vol. 11, No. 1, Jan 2026. pp. 120-132.

45 Gourav Yadav, “India’s Semiconductor Push: Defence Implications”, Issue Brief, *IDSA*, 20 Nov 2025, accessed 26 Aug 2026, https://idsa.in/publisher/issuebrief/indias-semiconductor-push-defence-implications

46 Preeti Raghunath, “Data in India’s Digital Public Infrastructure (DPI): A Deliberative Policy Ecology Approach”, *International Journal of Communication*, Vol. 20, 2026. pp. 417–434.

47 Anit Mukherjee, “Towards control and effectiveness: The Ministry of Defence and civil-military relations in India”, *Journal of Strategic Studies*, Vol. 45, Nos. 6–7, 2022. pp. 820–842.

48 Sha Sajadieh et al., “Artificial Intelligence Index Report 2026”, *Institute for Human-Centered AI*, Stanford University, Apr 2026, accessed 26 Aug 2026, https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf

49 Sudhish Kumar Jaini and Navin Varma, “Indian defence manufacturing landscape-DRDO, public & private sector”, *International Journal of Applied Research*, Vol. 11, No. 10, 2025. pp. 179-197.

50 Tejas Bharadwaj, “Mapping India’s Cybersecurity Administration in 2025”, *Carnegie Endowment for International Peace*, 01 Sep 2025, accessed 08 Jun 2026, https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025

51 Mohammed Abbad Mohiuddin, “AI-Driven Tools in the Indian Defence Sector”, *India AI*, 30 Sep 2024, accessed 10 Jun 2026, https://indiaai.gov.in/article/ai-driven-tools-in-the-indian-defense-sector

52 Pardeep Bhardwaj, “Use of Artificial Intelligence for Improving Operational Efficiency in the Armed Forces”, *Air Power Journal*, Vol. 19, No. 4, Winter 2024 (Oct-Dec). pp. 1-23.

53 PIB, “M.A.N.A.V.: PM Narendra Modi’s Human-Centric AI Odyssey”, *PIB Headquarters*, Government of India, 19 Feb 2026, accessed 12 Jun 2026, https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=157492&ModuleId=2&reg=6&lang=1

54 PIB, Indian Army Hosts National Seminar on “Enhancing Military Decision-Making Through Wargaming and Simulation” and “Releases Indigenous Decision-Support Applications”, *Ministry of Defence*, Government of India, 20 Feb 2026, accessed 14 Jun 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2230790&reg=3&lang=1

55 PIB, “Sarvam AI Powering a Made-in-India AI Revolution”, *PIB Headquarters*, Government of India, 21 Feb 2026, accessed 16 Jun 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2231169&reg=3&lang=1

Geopolitical Antecedents and Strategic Implications of the 2026 Iran–United States Military Confrontation: A Critical Assessment

B Srinivasan[@]

Abstract

The 2026 military confrontation between Iran and the United States represents one of the most consequential escalations in the history of post-1979 US–Iran relations. Although the confrontation emerged from decades of strategic rivalry, sanctions, nuclear disputes, proxy warfare, maritime competition, and regional alliance polarisation, its transformation into sustained direct warfare in 2026 reflected a breakdown of deterrence and diplomacy. This article critically examines the conflict's geopolitical antecedents and strategic implications, with particular attention to developments from Jan 2025 through Jul 2026 and to the Persian Gulf theatre. The primary objective is to identify the political, nuclear, military, and proxy-related drivers that transformed prolonged strategic competition into direct armed confrontation. It also evaluates the immediate military consequences and the wider effects on Middle Eastern security, international alliances, maritime commerce, nuclear non-proliferation, and global energy markets. The study adopts a qualitative analytical approach based on United Nations documents, International Atomic Energy Agency materials, strategic assessments, policy

[@]**B Srinivasan,** Assistant Professor and Head, Department of Defence and Strategic Studies, Dr MGR Educational Research Institute (Deemed to be University). Part-Time Research Scholar, PG & Research Department of Historical Studies, Pachaiyappas College, Chennai, Tamil Nadu.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

reports, and relevant scholarly literature. The analysis finds that the conflict cannot be attributed to a single triggering event. Rather, it resulted from the interaction of nuclear uncertainty, eroding diplomatic trust, US coercive pressure, Iranian deterrence strategies, Israeli security calculations, proxy conflict, maritime competition, and reciprocal perceptions of existential threat. The war subsequently transformed the Strait of Hormuz from a strategic chokepoint into a central theatre of military and economic contestation. The article argues that the conflict has weakened traditional deterrence assumptions, intensified regional polarisation, increased nuclear security risks, and exposed global energy systems' vulnerability to geopolitical disruption. It concludes that durable de-escalation requires a new regional security framework combining nuclear verification, maritime confidence-building, sanctions diplomacy, proxy de-escalation, and multilateral guarantees.

Introduction

The 2026 Iran–United States (US) military confrontation marks a major turning point in contemporary Middle Eastern geopolitics. Since the Iranian Revolution of 1979, relations between Tehran and Washington have been characterised by ideological antagonism, economic sanctions, diplomatic rupture, competing regional strategies, and periodic military crises. Yet for much of this period, both sides generally attempted to prevent their rivalry from developing into sustained direct interstate war. The 2026 confrontation represents a profound departure from that pattern.

The conflict must not be understood simply as an isolated military crisis beginning in Feb 2026. Its antecedents extend through the collapse of confidence surrounding the Joint Comprehensive Plan of Action (JCPOA), the US withdrawal from the agreement and subsequent ‘Maximum Pressure’ campaign, Iran's expansion of its nuclear capabilities, repeated attacks involving Iranian-aligned armed groups, Israeli-Iranian military exchanges, and the increasing strategic

importance of the Persian Gulf and Strait of Hormuz. The Jun 2025 attacks on Iranian nuclear facilities further weakened the distinction between nuclear diplomacy and military coercion. The International Atomic Energy Agency (IAEA) reported that military attacks on Iranian nuclear facilities in Jun 2025 led to the suspension of verification activities and the withdrawal of inspectors for safety reasons.[1]

The temporal scope extends from Jan 2025 to Jul 2026, while the geographical emphasis is the Persian Gulf and its immediate strategic environment. The analysis therefore considers the wider Middle Eastern consequences only where they directly affect the US–Iran confrontation.

This article critically examines the geopolitical drivers and strategic consequences of the 2026 Iran–US military confrontation, exploring how prolonged deterrence gave way to direct conflict. It treats the confrontation as a multidimensional security crisis involving the US, Iran, Israel, Gulf states, Iranian-aligned groups, international shipping companies and external powers such as China and Russia. Using a qualitative approach informed by United Nations (UN) documents, IAEA reports, strategic assessments and contemporary reporting, it integrates nuclear strategy, proxy warfare, maritime competition, alliance politics and economic coercion. It assesses the conflict's military and geopolitical consequences, its implications for energy security and maritime commerce, and policy options for preventing renewed escalation, while considering competing interpretations of its origins and legality.

Historical and Geopolitical Antecedents

The Structural Legacy of US–Iran Rivalry

- The confrontation's foundations lie in the transformation of US–Iran relations after 1979. The Iranian Revolution fundamentally altered the regional balance of power by replacing the pro-Western monarchy with an Islamic Republic committed to political independence from US influence. The hostage crisis, subsequent sanctions, the Iran–Iraq War, and continuing ideological antagonism institutionalised mutual distrust.

- From Washington's perspective, Iran became a state challenging US interests and allied governments in the Middle East. From Tehran's perspective, US military deployments, sanctions, alliances with Israel and Gulf monarchies, and support for adversarial regional actors represented a continuing strategy of containment. This reciprocal threat perception became a self-reinforcing security dilemma.

- Realist international relations theory helps explain this process. When states cannot be certain of adversaries' intentions, they may interpret defensive measures as offensive preparations.[2] Iranian missile development, naval capabilities, regional partnerships, and nuclear infrastructure were therefore interpreted in Washington as components of a strategy for regional coercion. Conversely, Tehran interpreted US military deployments and sanctions as evidence that Washington sought regime change or strategic subordination.

The Nuclear Dispute and Collapse of Strategic Trust

- The nuclear issue became the most important institutional mechanism for managing the rivalry after the JCPOA was concluded in 2015. The agreement restricted Iran's nuclear activities in return for sanctions relief and international verification.[3] For several years, the agreement represented an example of how adversarial states could transform strategic mistrust into verifiable limitations.

- The US withdrawal from the JCPOA in 2018, however, fundamentally altered this framework. Washington reintroduced extensive sanctions, while Iran gradually reduced compliance with nuclear restrictions. The resulting cycle produced a strategic paradox: coercive pressure was meant to compel Iran to accept stricter limitations, but it also weakened incentives for Tehran to remain within the original nuclear framework.

- The central problem became one of credibility. Iran increasingly questioned whether agreements with Washington could survive political changes in the US, while the US

questioned whether Iranian nuclear commitments would remain verifiable over the long term.

- The Jun 2025 military attacks on Iranian nuclear facilities represented another critical rupture. The IAEA recorded attacks affecting several Iranian nuclear-related sites, including Natanz, Fordow, and other facilities, and stated that attacks against nuclear facilities have serious implications for nuclear safety, security, safeguards, and international peace.[4]

- The 2026 conflict consequently inherited a nuclear dispute in which diplomacy had already suffered substantial institutional damage.

The Nuclear Factor in the 2026 Confrontation

- Nuclear strategy was central to the escalation because Iran's nuclear programme became inseparable from broader questions of regime security.

- Iran has consistently maintained that its nuclear programme is intended for peaceful purposes, while the US, Israel, and several regional actors have expressed concern about Iran's capacity to rapidly develop a nuclear weapons capability. The problem is therefore not merely whether Iran possessed an operational nuclear weapon but whether it had developed a sufficiently advanced nuclear infrastructure to create a latent nuclear deterrent.

- This distinction is strategically important. A state does not necessarily require an assembled nuclear weapon to alter regional calculations. A large enrichment capability, advanced centrifuges, technical expertise, and reduced international monitoring may create what strategic analysts describe as nuclear latency.[5]

- The deterioration of IAEA access after the 2025 attacks further complicated verification. Once inspectors could no longer conduct normal verification activities, uncertainty increased. Uncertainty, in turn, encouraged worst-case assumptions.

- This generated a dangerous escalation cycle: Nuclear uncertainty → intelligence alarm → military pressure → Iranian dispersal and concealment incentives → reduced verification → greater uncertainty → further military pressure.
- This cycle is particularly dangerous because each actor can see its actions as defensive while interpreting the adversary's actions as preparation for aggression.
- The attacks on Iranian nuclear-related infrastructure in 2026 consequently had consequences beyond immediate physical damage. They potentially weakened the international non-proliferation regime by demonstrating that nuclear facilities can become direct targets during interstate confrontation.

Proxy Warfare and the Expansion of the Security Dilemma

A second major antecedent was the shift from US–Iran competition to a networked regional conflict.

Iran's relationships with Hezbollah, Iraqi armed groups, the Houthis, and other regional partners have historically provided Tehran with strategic depth. These relationships allow Iran to exert influence beyond its national territory while complicating adversaries' ability to retaliate directly against Iran.

The US, Israel, and Gulf states have consequently viewed Iran's regional network as a mechanism for projecting military power without conventional confrontation. Iran, however, has viewed many of these relationships as part of a broader deterrence strategy designed to prevent encirclement.

This creates what can be described as distributed deterrence. Instead of relying exclusively on Iranian national military forces, Tehran can impose costs across multiple geographical theatres.

The weakness of distributed deterrence is that it creates escalation ambiguity. When an armed group attacks US personnel or shipping, Washington must determine whether the group acted independently, with Iranian assistance, or under direct Iranian instruction. Tehran, meanwhile, may deny direct responsibility while benefiting strategically from the attack.

The US's Mar 2026 communication to the UN Security Council explicitly linked its military operations to attacks and threats from Iran and Iranian proxies and argued that US actions were intended to protect American personnel, regional allies, and maritime commerce.[6]

Thus, proxy warfare became a principal mechanism through which regional competition crossed the threshold into interstate confrontation.

The Immediate Escalation into Direct War

The decisive transformation occurred in Feb 2026, when the US and Israel initiated major attacks against Iran. The conflict subsequently developed into sustained exchanges of missiles, drones, air strikes, and attacks against military and strategic infrastructure.

The US presented its military campaign primarily through the language of self-defence, protection of American forces and allies, and preservation of freedom of navigation. Iran characterised the attacks as aggression against its sovereignty and asserted its right to self-defence under Article 51 of the UN Charter.[7]

These competing legal narratives demonstrate a broader problem in international security: once military action begins, each side tends to construct a retrospective justification based upon its own interpretation of preceding threats.

The conflict therefore cannot be reduced analytically to which individual attack constituted the first act of aggression. Its deeper significance lies in the cumulative erosion of barriers against direct military action.

The critical strategic failure was deterrence without effective communication. Deterrence requires an adversary to understand both one's capabilities and one's red lines. In the US–Iran relationship, however, red lines increasingly became ambiguous.

Iran sought to demonstrate that attacks against it would generate regional costs. Washington sought to demonstrate that Iranian attacks or nuclear advances would trigger increasingly severe military responses. Each side consequently attempted to restore

deterrence by increasing pressure. Instead, the accumulation of pressure contributed to war.

The Strait of Hormuz as the Central Strategic Theatre

The Strait of Hormuz became the most consequential geographical dimension of the conflict.

Approximately one-fifth of global petroleum liquids consumption has historically moved through the Strait, making it one of the world's most important energy chokepoints.[8] The waterway is therefore not simply a regional maritime route; disruption can affect inflation, transportation costs, industrial production, food prices, and economic stability worldwide.

The conflict transformed Hormuz from a strategic vulnerability into an active military bargaining instrument. Iran's geographical position gives it considerable capacity to threaten shipping through mines, missiles, drones, small boats, and other asymmetric means. By contrast, the US has superior naval capabilities and seeks to preserve freedom of navigation.

The US–Iran memorandum of understanding of 17 Jun 2026 temporarily reduced military operations and included arrangements intended to facilitate commercial passage through the Strait.[9] Yet the arrangement proved fragile.

By Jul, fighting had resumed, and the Strait again became a principal theatre of confrontation. Reports indicated attacks on commercial vessels and renewed US military operations.[10]

Hormuz's strategic importance lies in the asymmetry between the actors. The US can dominate conventional maritime operations, but Iran does not need to permanently close the Strait to impose enormous costs. Even uncertainty about safe passage can increase insurance premiums, discourage shipping, reduce traffic, and produce speculative price increases.

Thus, perceived risk can be almost as economically significant as actual physical closure.

Military Consequences

The immediate military consequences of the confrontation were extensive.

- First, the war demonstrated the vulnerability of fixed military infrastructure in the Gulf. US bases in regional partner states became potential targets, thereby forcing Gulf governments to reconsider the security costs of hosting American forces.

- Second, Iran demonstrated the strategic utility of ballistic missiles, drones, maritime attacks, and asymmetric operations. Although the US retained overwhelming conventional superiority, Iran's ability to impose costs across multiple theatres complicated Washington's military calculations.

- Third, the conflict accelerated the militarisation of the Persian Gulf. Naval forces, air-defence systems, missile-defence platforms, surveillance assets, and unmanned systems became increasingly important.

- Fourth, the war exposed the limits of technological superiority. Precision strike and missile defence can reduce damage but cannot eliminate strategic uncertainty. A technologically superior power may still face substantial economic and political costs from relatively inexpensive asymmetric attacks.

The conflict therefore reinforces an important principle of contemporary warfare: strategic effectiveness is not identical to battlefield superiority.

A weaker state can remain strategically consequential if it possesses geographical advantages, asymmetric capabilities, political resilience, and the ability to impose costs on economically sensitive infrastructure.

Humanitarian and Civilian Consequences

Military confrontation also generated significant humanitarian consequences. Air strikes, missile attacks, infrastructure destruction, displacement, disruptions to electricity and fuel supplies, and damage to civilian facilities intensified pressure on Iranian society and populations elsewhere in the region.

The protection of nuclear installations represented a particularly serious humanitarian issue. The IAEA documented incidents involving Iranian nuclear facilities during the fighting and repeatedly emphasised the need to protect nuclear installations from military action. In Mar 2026, projectiles struck the Bushehr Nuclear Power Plant, although the IAEA reported no damage to the facility, no injuries, and no radiological release.[11]

The possibility of radiological contamination adds a unique dimension to warfare around nuclear facilities. Even without a release, attacks can spark panic, disrupt monitoring systems, and complicate emergency preparedness.

The humanitarian dimension therefore cannot be treated as secondary to military strategy. Civilian vulnerability can drive political instability, refugee movements, economic disruption, and international diplomatic pressure.

Energy Security and Global Economic Consequences

The war's most immediate global economic consequence was the disruption of energy markets.

The global petroleum market is highly interconnected. Even countries that do not import oil directly from the Persian Gulf can experience price increases because crude oil is traded internationally. As Brookings has noted, the US itself remains exposed to global oil-price shocks despite being a major oil producer because petroleum is a globally traded commodity.[12]

The conflict consequently produced three interconnected effects:

- **Supply Disruption**. Reduced Gulf exports directly constrained available petroleum.
- **Risk Premium**. The possibility of further disruption increased market prices even when physical shortages were limited.
- **Macroeconomic Transmission**. Higher energy prices increased transportation and production costs, contributing to inflation.

The Jul 2026 situation showed the global economy's strategic vulnerability to maritime disruption. Analysts reported that Gulf oil flows remained significantly below pre-war levels and warned that continued disruption would place additional pressure on oil, refined products, and LNG markets.[13]

The implications extend beyond oil. Gulf disruption affects LNG shipping, petrochemicals, maritime insurance, global freight costs, and industrial supply chains.

The war therefore illustrates that energy security is not merely a question of resource availability. It is also a question of **transport security**.

Transformation of Middle Eastern Alliances

The confrontation also altered regional alliance structures.

For decades, many Gulf States relied heavily upon the US for external security while simultaneously attempting to maintain working relationships with Iran. The 2026 war challenged this balancing strategy.

Hosting US military facilities could increase the risk of Iranian retaliation. Yet distancing themselves from Washington could weaken their deterrence against other regional threats.

This dilemma is particularly significant for Bahrain, Qatar, Kuwait, Saudi Arabia, and the United Arab Emirates. Their strategic challenge is no longer simply choosing between the US and Iran. Instead, they must develop mechanisms that allow security

cooperation with Washington without automatically becoming participants in US–Iran escalation.

The war therefore strengthened the logic of strategic hedging among regional powers.

At the same time, the conflict increased opportunities for China and Russia to expand diplomatic influence. Neither power can easily replace the US as the principal regional military actor, but both can benefit from the perception that US-led security arrangements cannot guarantee stability.

China's dependence on Gulf energy supplies gives Beijing strong incentives to promote diplomatic de-escalation. Russia, meanwhile, can benefit geopolitically from increased pressure on Western economies and from the diversion of US strategic attention toward the Middle East.

Consequences for International Order

The conflict has wider implications for the international order.

- First, it demonstrates the weakening ability of international institutions to prevent interstate escalation when major powers disagree over the interpretation of international law.
- Second, it challenges the credibility of nuclear non-proliferation mechanisms. If nuclear facilities become targets during military conflict, states may conclude that nuclear ambiguity or even nuclear deterrence is necessary for survival.
- Third, it raises difficult questions concerning the law of self-defence, proportionality, necessity, maritime blockades, and attacks against infrastructure.

The US’s official justification emphasised self-defence and protection of maritime commerce, whereas Iran's official communications characterised the initial attacks as aggression and invoked Article 51 of the UN Charter.[14]

The significance of these competing interpretations extends beyond Iran. Other states may use the precedent to justify preventive military action against perceived nuclear or missile threats.

The long-term consequence could therefore be a more permissive international environment for military strikes against strategic infrastructure.

Strategic Miscalculation as a Central Cause

The most persuasive explanation of the conflict is not that either side deliberately sought an unlimited war from the beginning. Rather, the conflict can be understood as the product of strategic miscalculation.

Washington may have calculated that overwhelming military pressure would compel Tehran to make rapid concessions. Tehran may have calculated that asymmetric retaliation would raise the costs of US intervention without provoking an unlimited response. Israel may have calculated that degrading Iranian military and nuclear capabilities would improve long-term security. Each calculation contained a rational element. The problem was that these calculations interacted.

Military pressure increased Iranian incentives to retaliate. Iranian retaliation strengthened the US case for further military action. Israeli involvement intensified Iranian perceptions of encirclement. Attacks on shipping expanded the conflict into the global economy. Economic pressure increased Iran's domestic vulnerability while also reducing Tehran's willingness to concede under coercion.

This is a classic security dilemma in which measures intended to increase security collectively produce greater insecurity.

The Failure of Nuclear Diplomacy

The breakdown of nuclear diplomacy was perhaps the most important structural cause.

Diplomacy requires three forms of confidence:

- Confidence that agreements will be honoured;

- Confidence that verification mechanisms will function; and
- Confidence that concessions will not be exploited by the opposing side.

By 2026, all three had deteriorated.

Iran questioned the durability of American commitments. The US questioned the reliability of Iranian nuclear restrictions. The IAEA faced severe constraints on verification following military attacks and changes in Iranian cooperation.

The result was an environment in which intelligence uncertainty replaced verified knowledge.

This is strategically dangerous because military decision-makers tend to plan against worst-case scenarios. Once verification declines, worst-case planning becomes easier to justify politically.

Consequently, the nuclear issue became a catalyst rather than merely a subject of negotiation.

The Conflict as a Crisis of Deterrence

The 2026 confrontation also challenges conventional understandings of deterrence.

Traditional deterrence assumes that rational actors will avoid actions that could produce unacceptable costs. However, deterrence becomes unstable when actors disagree about what constitutes an unacceptable cost.

For Iran, national sovereignty and regime survival may justify significant economic and military sacrifices. For the US, unrestricted nuclear proliferation and threats to maritime commerce may be considered unacceptable. For Israel, the possibility of an Iranian nuclear capability may be interpreted as an existential threat.

These different definitions of unacceptable risk make mutual deterrence extremely difficult.

The central lesson is that deterrence without credible diplomatic off-ramps can become escalation management rather than conflict prevention.

Strategic Implications for India and the Global South

Although the conflict is geographically concentrated in West Asia, its consequences matter especially for India and other energy-importing developing countries.

India has extensive economic and strategic interests in the Gulf. Many Indian citizens work in Gulf States, and India's energy security depends substantially on stable maritime supply routes. Disruption in the Strait of Hormuz therefore directly affects India's import costs, inflation, shipping insurance, and diaspora security.

The conflict also reinforces India's longstanding preference for strategic autonomy and diversified energy partnerships.

For developing countries, the confrontation demonstrates how geopolitical instability can rapidly become a development crisis. Higher oil prices can increase fiscal pressure, inflation, transport costs, and current-account deficits.

The Global South therefore has a strong interest in strengthening international mechanisms for maritime security, energy diversification, and diplomatic conflict prevention.

Policy Implications and Pathways to De-escalation

The first policy requirement is to restore nuclear verification. The IAEA must regain sufficient access to Iranian nuclear facilities to establish reliable information concerning nuclear materials and activities.

Second, the US and Iran require a durable diplomatic channel insulated from immediate military crises. Secret backchannels may help initiate negotiations, but a sustainable settlement requires institutionalised communication.

Third, States concerned with security in the Strait of Hormuz should establish maritime confidence-building measures. These could include advance-notification mechanisms, incident-at-sea

protocols, emergency communication channels, and mutually accepted rules for commercial shipping.

Fourth, regional states should establish a Gulf security dialogue involving Iran, Saudi Arabia, the United Arab Emirates, Iraq, Oman, Qatar, Kuwait, Bahrain, and external stakeholders. The objective should not initially be to create a comprehensive security organisation but to gradually develop crisis-management mechanisms.

Fifth, any settlement should include proxy de-escalation. A bilateral US–Iran agreement that ignores attacks by allied and partner armed groups would remain vulnerable.

Sixth, sanctions diplomacy should replace an exclusively coercive approach. Sanctions relief can be linked to measurable nuclear verification and regional security commitments.

Finally, nuclear facilities must be treated as protected infrastructure. The risks associated with attacks near operating reactors and nuclear material make the targeting of nuclear facilities particularly dangerous.

Conclusion

The 2026 Iran–US military confrontation cannot be adequately explained by a single event, leader, policy decision, or military operation. It was the cumulative product of decades of geopolitical rivalry, institutionalised mistrust, nuclear uncertainty, proxy warfare, economic coercion, regional alliance polarisation, and competing concepts of deterrence.

The period from Jan 2025 to Jul 2026 demonstrates how rapidly these accumulated pressures can interact. The 2025 attacks on Iranian nuclear infrastructure weakened the already fragile architecture of nuclear verification. The subsequent deterioration of trust contributed to a strategic environment in which military solutions became increasingly attractive. The Feb 2026 escalation transformed indirect confrontation into direct war. The conflict subsequently expanded into the maritime and economic domains, particularly through the struggle over the Strait of Hormuz.

The most important strategic consequence is therefore not simply the destruction of military infrastructure. It is the transformation of the regional security architecture.

The Gulf states now face heightened uncertainty concerning the reliability and costs of external security guarantees. Iran has demonstrated that asymmetric capabilities can generate consequences far beyond the battlefield. The US has demonstrated overwhelming conventional superiority but also encountered the limitations of military coercion against a geographically resilient adversary. Israel's security strategy has become even more intertwined with broader US–Iran competition. Meanwhile, China and Russia have acquired greater opportunities to challenge Western influence diplomatically.

The conflict has also exposed the fragility of global energy security. The Strait of Hormuz remains a powerful reminder that a geographically narrow waterway can affect global inflation, trade, and strategic stability. Reports during Jul 2026 showed that the confrontation continued to disrupt shipping and energy flows, while the temporary Jun arrangement failed to establish a durable settlement.[15]

Ultimately, the central lesson of the 2026 confrontation is that military superiority cannot substitute for a sustainable regional security order. A durable settlement requires simultaneous progress on the nuclear question, maritime security, sanctions, proxy warfare, and regional confidence-building.

The challenge is therefore not merely to negotiate another ceasefire. It is to create a political and institutional framework in which Iran, the US, Israel, and the Gulf states possess credible alternatives to escalation. Without such a framework, the strategic conditions that produced the 2026 confrontation will remain intact, making another crisis—and potentially another war—highly probable.

Endnotes

1 International Atomic Energy Agency, *Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015)*, GOV/2025/50 (Sep 2025), 3–4, accessed 18 Mar 2026, https://www.iaea.org/sites/default/files/documents/gov2025-50.pdf.

2 Robert Jervis, “Cooperation under the Security Dilemma”, *World Politics* 30, no. 2 (Jan 1978): 167–214, accessed 18 Mar 2026, https://doi.org/10.2307/2009958

3 Trita Parsi, *Losing an Enemy: Obama, Iran, and the Triumph of Diplomacy* (New Haven, CT: Yale University Press, 2017).

4 International Atomic Energy Agency, *Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015)*, GOV/2025/50 (03 Sep 2025), accessed 18 Mar 2026, https://www.iaea.org/sites/default/files/documents/gov2025-50.pdf

5 Nuclear Threat Initiative, “Iran”, nuclear overview, accessed 04 Oct 2026, accessed 18 Mar 2026, https://www.nti.org/countries/iran/

6 United Nations Security Council, *Letter Dated 10 Mar 2026 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council*, S/2026/161 (11 Mar 2026), accessed 18 Mar 2026, https://docs.un.org/en/S/2026/161

7 United Nations Security Council, *Letter Dated 28 Feb 2026 from the Permanent Representative of the Islamic Republic of Iran to the United Nations Addressed to the Secretary-General and the President of the Security Council*, S/2026/106 (02 Mar 2026), https://docs.un.org/en/S/2026/106; accessed 19 Mar 2026, United Nations Security Council, *Letter Dated 10 Mar 2026 from the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council*, S/2026/161 (11 Mar 2026), accessed 19 Mar 2026, https://docs.un.org/en/S/2026/161

8 Congressional Research Service, *The Strait of Hormuz: Security Developments and Impacts on Oil, Gas, and Other Commodities*, R45281 (07 Aug 2026), accessed 19 Mar 2026, https://www.congress.gov/crs-product/R45281

9 Ibid.

10 Jana Choukeir et al., “US and Iran Target Infrastructure as Strait Shipping Comes under Further Attack”, *Reuters,* 17 Jul, 2026*,* accessed 19 Mar 2026,*https://www.reuters.com/world/middle-east/iran-launches-fresh-attacks-after-sixth-day-us-strikes-2026-07-17/*

11 *International Atomic Energy Agency,* "A Projectile Struck the Premises of the Bushehr Nuclear Power Plant", 17 Mar 2026*,* accessed 19 Mar 2026, https://www-news.iaea.org/ErfView.aspx?mId=e7543f73-ef49-47d9-9e27-71b0048e0cca

12 Samantha Gross and Ryan Beane, "From Chokepoint to Crisis: The Strait of Hormuz and Global Oil Markets", Brookings Institution, 08 Jun 2026, accessed 19 Mar 2026, https://www.brookings.edu/articles/from-chokepoint-to-crisis-the-strait-of-hormuz-and-global-oil-markets/

13 Eamonn Brennan, "Energy Markets Face Coming Stress If No New US-Iran Deal Reached: Analysts", S&P Global Energy, 16 Jul 2026, accessed 20 Mar 2026, https://www.spglobal.com/energy/en/news-research/latest-news/crude-oil/071626-energy-markets-face-coming-stress-if-no-new-us-iran-deal-reached-analysts

14 United Nations Security Council, S/2026/106 (02 Mar 2026), accessed 20 Mar 2026, https://docs.un.org/en/S/2026/106; S/2026/161 (11 Mar 2026), https://docs.un.org/en/S/2026/161

15 Raad Alkadiri et al., "What a Fragile U.S.-Iran Ceasefire Means for Energy and Beyond", Center for Strategic and International Studies, 01 Jul 2026, accessed 20 Mar 2026, https://www.csis.org/analysis/what-fragile-us-iran-ceasefire-means-energy-and-beyond; Eamonn Brennan, "Energy Markets Face Coming Stress If No New US-Iran Deal Reached: Analysts", S&P Global Energy, 16 Jul 2026, accessed 20 Mar 2026, https://www.spglobal.com/energy/en/news-research/latest-news/crude-oil/071626-energy-markets-face-coming-stress-if-no-new-us-iran-deal-reached-analysts

The Algorithmic Age of Warfare: Lessons from Contemporary Conflicts and a Techno-Legal Framework for Autonomous Defensive Response in India

Commander Ravi Shankar NRK (Retd)[@]

Abstract

The fusion of Artificial Intelligence (AI) with drones, missiles, cyber capabilities and Intelligence, Surveillance and Reconnaissance is compressing modern warfare to machine speed. The Middle East has exposed the perils of algorithmic targeting outpacing human review; the Russia–Ukraine war has shown that combat AI must function at the tactical edge, unaided by cloud connectivity; and India's Operation Sindoor, read against China's 'Intelligentised Warfare' doctrine, shows Indo-Pacific decision cycles compressing to single-digit seconds. Together, these expose a 'Speed Versus Control' paradox that conventional 'Human-in-the-loop' doctrine cannot resolve once the engagement window narrows below the time a human needs to process a binary choice. This article does not propose a general AI-regulation framework; its scope is narrower — how India should govern AI's use in weapons and defensive-response systems built to counter machine-speed

[@]**Commander Ravi Shankar NRK (Retd)** is an independent researcher and the author of The Digital Armada (2026). A veteran of the Indian Navy with over 35 years of service across submarines, frontline warships, and major defence establishments, he has held senior leadership and program-management appointments overseeing the induction of combat systems, fleet logistics and mission-critical networks. His current research focuses on autonomous systems, algorithmic sovereignty, and artificial intelligence governance in the maritime domain.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

threats. It proposes a four-pillar techno-legal framework — Pre-Authorised Autonomous Defensive Response (PAADR), edge-first resilience with federated learning, a Joint Maritime Domain Awareness Data Architecture, and ring-fenced agile procurement — to reconcile algorithmic velocity with democratic accountability and India's obligations under international humanitarian law.

Introduction

The character of warfare has shifted structurally over the past decade. The battlefield no longer sits within the physical domains of land, sea, and air alone; it runs through the electromagnetic spectrum, data networks, space, and the cognitive domain. Military superiority increasingly depends on data dominance, network integration, and the speed of decision-making, with Artificial Intelligence (AI) serving as the cognitive spine linking Intelligence, Surveillance And Reconnaissance (ISR), cyber operations, space assets, and precision strike.

States embedding AI into their national security architectures are not merely enhancing existing capabilities; they are redefining what strategic advantage means, and that redefinition brings a governance problem that cannot be deferred: reconciling the lethal speed of these technologies with the legal requirement of meaningful human control.[1] This article confines itself to that narrower problem rather than to the broader debate over regulating AI development in India, which is already under way through the India AI Mission and related fora.[2] Its subject is AI's employment specifically within weapons and defensive-response systems. The Defence Research and Development Organisation's (DRDO) 2024 Evaluating Trustworthy AI (ETAI) Framework and India's own submission to the United Nations' (UN) Secretary-General already establish safety, transparency, fairness, and human oversight as governing principles in the military domain.

In the military domain, safety, transparency, fairness, and human oversight are already established as governing principles.[3], [4] The question is operational, not declaratory: how those principles

survive an engagement window that has collapsed to single-digit seconds.

The analysis that follows draws on a structured comparison of three theatres—the Middle East, Russia–Ukraine, and the Indo-Pacific, including Operation Sindoor—chosen because each isolates a distinct variable bearing on weapons-employment governance: human oversight under high-tempo targeting, resilience under sustained electronic warfare, and the compressed decision cycles of a two-front, nuclear-armed threat environment, respectively. Evidence is drawn from open-source operational reporting cross-checked across independent accounts, India's primary governance documents, and comparative defence-budget data. Where a single-source claim could not be independently corroborated, it has been qualified in the text rather than treated as settled.

Review of Literature

Existing scholarship falls into three strands that, read separately, leave the question of weapons employment unanswered. The first, on 'Meaningful Human Control' (MHC), is analytically rich but operationally thin: Williams's critique of the MHC debate argues that the 'Meaningful Human' at its centre reflects a narrow, Western conception of agency that says little about what happens once the physics of an engagement make real-time deliberation impossible.[5] Indian commentary has tended toward the cautious end of this debate—writing from the Centre for Land Warfare Studies argues that algorithms cannot substitute for human judgement of context and consequence, and that the 'Decide' function of the Observe–Orient–Decide–Act loop should stay with humans[6]—without engaging the empirical reality that a strict human-in-the-loop requirement is already being overtaken by combat tempo. The second strand is institutional: Saini's assessment for the Council for Strategic and Defence Research documents India's fragmented AI funding and the absence of a unified inter-service data architecture in granular detail, but is oriented toward capability-building rather than the governance of weapons employment.[7] The third is doctrinal — the ETAI Framework and India's UN Secretary-General submission state principles of safety, oversight and International Humanitarian Law

(IHL) compliance without an engineering specification for how those principles hold once the decision window collapses.[8] Read together, the gap is precise: ethics and law theorise control without confronting engagement physics; institutional analysis documents capability gaps without addressing employment governance; and doctrine states principles without architecture. This article sits at the intersection of the three, using the operational record below to derive design constraints for a bounded architecture rather than a general governance principle.

Trends and Dynamics in Contemporary Conflicts

The Middle East: ISR, Missiles and the Erosion of Human Oversight. In Gaza and Lebanon, Israeli forces are reported to have used AI decision-support systems such as 'Lavender' and 'The Gospel' to generate targeting recommendations at a pace producing a reported 45-fold increase in operational tempo.[9] That speed produced 'Automation Bias': operators reportedly spent only about 20 seconds verifying AI-generated targets before authorising strikes, reducing human review to a rubber stamp while the ethical guardrails distinguishing combatants from civilians progressively gave way.[10] Israel's Operation Rising Lion and the United States' (US) strike codenamed Midnight Hammer confirmed that AI-integrated air power can project long-range strikes across considerable distances,[11] while Houthi drone and missile attacks in the Red Sea have forced coalition navies into sustained air defence with engagement windows measured in tens of seconds—a preview of what platform-centric the Indian Ocean area defence will struggle to match.[12]

The Russia–Ukraine Theatre: Drone Swarms and Edge-AI Resilience. Ukraine has shown that centralised cloud dependence is a critical vulnerability under sustained electronic warfare. During Operation Spider Web, drones whose remote links were severed completed strikes autonomously using onboard visual-recognition algorithms; platforms such as the Saker Scout now navigate without global positioning system or cloud connectivity.[13] Persistent wiper-malware and disinformation campaigns aimed at logistics and command networks, run from the war's opening hours, reinforce the

same lesson: any system India fields must degrade gracefully, not catastrophically, the moment connectivity is denied.[14]

The Indo-Pacific and South Asia: Operation Sindoor and Intelligentised Warfare. Operation Sindoor in May 2025 offers India's own evidence. Over a 4-day window, 23 AI applications were reportedly unified for a common battlefield picture, and the Electronic Intelligence Collation and Analysis System, trained on 26 years of archival data, achieved roughly 94 per cent accuracy in identifying hostile radar and missile units.[15] Separately, the Army's Akashteer air-defence network—built by Bharat Electronics with DRDO and Indian Space Research Organisation, fusing tactical radars, low-level radars and the Akash weapon system into one operating picture — was credited with directing interceptions along the western front. It is worth being precise here: contemporaneous reporting described this as 'Automated operations for faster response' and 'Decentralised engagement authority' at forward nodes, rather than a fully autonomous killweb; the more expansive 'AI-driven' description appears mainly in later trade commentary.[16] The verifiable claim is narrower but still significant—Akashteer compressed detection-to-engagement time by pushing authority to automated forward nodes, the design principle this article's first pillar seeks to generalise.

AI-Enabled Military Threats. China's 'Intelligentised Warfare' doctrine, backed by a military–civil fusion strategy that transfers commercial AI advances into battlefield deployment with little friction, has produced platforms such as the JARI-USV-A 'Orca' unmanned surface vessel, a stealth platform reportedly capable of ranges beyond 4,000 nautical miles and vertical missile launches.[17] Pakistan is separately pursuing AI-enabled drone-swarm programmes and an expanding inventory of cruise missiles such as the Harbah, raising the prospect of a future crisis combining both threat streams.[18] Along the Line of Actual Control, both India and China have fielded long-endurance drones and AI-assisted change detection, compressing the warning time on which conventional crisis signalling and restraint have traditionally relied.[19]

Lessons Learnt: The Speed Versus Control Paradox

Taken together, these theatres expose a tension that India's own ETAI doctrine, resting on a strict human-in-the-loop mandate, does not resolve.[20] Against a hypersonic missile or a saturation drone swarm, the engagement window from detection to impact can compress to 25 to 40 seconds, while human decision-making under stress requires 8 to 12 seconds simply to process a binary choice.[21] At that timescale, an operator cannot fuse sensor data, classify a threat and authorise a response; forcing the attempt converts a commander into a liability shield rather than an agent of genuine moral control—a distinction with legal as well as ethical weight, since a decision made without room for deliberation cannot straightforwardly satisfy the accountability human-in-the-loop doctrine is meant to guarantee. Adversaries operating under less restrictive doctrines—the US' 'AI-First' posture and China's intelligentised warfare—are engineering autonomous engagement precisely to exploit that latency.[22] A related consequence is doctrinal: deterrence in South Asia has rested on the threat of punishment, which presumes an adversary has time to receive a signal and revise intent; algorithmic warfare compresses every stage of that sequence, favouring deterrence-by-denial and demonstrably resilient defensive autonomy over speculative retaliation.

Strategic Implications for India: A Techno-Legal Framework for Autonomous Defensive Response

Resolving this paradox requires an engineered architecture, not a restated commitment to oversight that the record above shows has already been overtaken. The ETAI Framework and India's UN Security General submission supply the governing principles; what follows operationalises them.[23]

Pillar One: Resolving the Speed Paradox Through Pre-Authorised Autonomous Defensive Response (PAADR). The armed forces should institute a PAADR framework, legally and technically pre-authorising bounded, autonomous terminal-defence actions—activating close-in weapon systems, releasing decoys—before an engagement occurs rather than during it. Activation would

require simultaneous hardware-encoded conditions: an active hostile radar or terminal-guidance signature, independent sensor corroboration, and a computed impact probability above a pre-authorised, operationally and legally validated threshold—85 per cent is used here only as an illustrative figure, not a proposed Indian standard; the actual value is a calibration question for the weapons-review process described below, not one this article can settle in the abstract. PAADR would be confined to terminal self-defence, excluding offensive tasking, with the commanding officer retaining standing authority to deactivate it. Crucially, human decision-making is relocated rather than removed: it is exercised prospectively, in designing trigger conditions and in a mandatory Article 36-style weapons review, rather than in real time, where it cannot meaningfully be exercised at all.[24] The argument is not that prospective authorisation by itself constitutes meaningful human control; rather, it is that control must be distributed across system design, weapons review, operational constraints, standing command authority and the ability to intervene or deactivate, of which prospective authorisation is one component among several. Understood that way, the architecture is designed to operationalise the cardinal IHL principles in a manner that real-time human review under hypervelocity conditions cannot easily match: distinction is supported through the narrowness of the trigger set itself, since only objects exhibiting a verified attack signature can activate the system; proportionality is supported by confining permissible action to defensive, terminal-phase responses with pre-set collateral limits; and precaution is supported through the mandatory review—though actual compliance in any given engagement remains a facts-and-circumstances question the architecture cannot guarantee in advance. The benefit is concrete, not rhetorical—it converts a commander's choice between a legally fraught snap decision and a fatal delay into an auditable, improvable, peacetime one, and it is that relocation of judgement, not the removal of it, that makes PAADR defensible.

Pillar Two: Edge-First Resilience and Federated Learning. AI systems must be deployed through hardware-isolated, air-gapped modules that can function at the tactical edge without internet or

satellite connectivity, treating jamming and denial as baseline design conditions. This must also address a specifically Indian problem: a model trained on Rajasthan's desert terrain can fail outright in Ladakh's high-altitude conditions, where lighting, thermal signature and atmosphere differ fundamentally.[25] ETAI-mandated uncertainty estimation, which hands control back to a human when confidence drops, must be built in from the outset so unfamiliar conditions default to caution rather than false confidence—and air-gapped deployment simultaneously narrows the attack surface for adversarial data poisoning. For cross-domain ISR, federated learning allows models to train locally on platforms such as P-8I aircraft or Kalvari-class submarines, sharing only encrypted model updates rather than sensitive raw data such as submarine acoustic signatures—preserving both data sovereignty and bandwidth discipline.[26]

Pillar Three: Breaking Institutional Silos for ISR Integration. India's three services operate largely distinct legacy systems reflecting decades of separate modernisation, a fragmentation that is doctrinal before it is technical: without a shared operational picture, PAADR-style prospective authorisation cannot scale beyond single-platform defence to a genuinely joint defensive network. The framework calls for a Joint Maritime Domain Awareness Data Architecture—a unified defence data cloud paralleling the 'Directorate of AI' and data-cloud already recommended independently within the Integrated Defence Staff — standardising formats across the Defence Intelligence Agency, service intelligence wings and civilian space agencies, and fusing satellite, coastal radar and drone inputs through platforms such as TRIDENT-SAMUDRA to automate detection of 'Dark Vessels' and grey-zone maritime militia, the category of threat hardest to counter precisely because it sits below the threshold that triggers a conventional platform-centric response.[27, 28]

Pillar Four: Agile Procurement and Ring-Fenced Budgeting. India has no single dedicated military-AI budget line; funding is drawn from annual service-specific earmarks of roughly INR 100 cr from each of the Army, Navy and Air Force plus a further INR 100 cr from the Defence AI Project Agency—about INR 400 cr (USD 46 mn) a year in total, under three per cent of estimated Chinese military AI

spending and dwarfed by the US Department of War's FY2026 request of USD 13.4 bn in standalone autonomy funding.[29] India's civilian India AI Mission budget was itself halved, from INR 2,000 cr to INR 1,000 cr, in the same cycle.[30] Three-to-five-year hardware acquisition cycles are structurally incompatible with software-defined AI, which needs continuous retraining against evolving threats and adversarial poisoning. India should ring-fence one per cent of the capital defence budget for AI software, R&D and edge computing infrastructure—roughly a fivefold increase over current dedicated spending—and decouple procurement from hardware timelines through agile framework contracts and deeper engagement with the domestic start-up ecosystem through initiatives such as iDEX, which has already shown, through contracts such as the roughly INR 100 cr award to the counter-drone start-up Indrajaal, that faster-cycle procurement is administratively possible within existing law. Money alone will not close the gap: the two-to-three-year officer rotation policy that serves broad command experience is directly at odds with the multi-year specialisation AI stewardship requires, moving personnel out just as they accumulate the depth needed to supervise these systems critically rather than defer to them. A specialised AI cadre, complemented by lateral recruitment of civilian data scientists on competitive terms, would address that retention problem directly.[31]

Conclusion

AI's fusion with drones, missiles, cyber capabilities and ISR is an operating reality, not a future one. The Middle East, Ukraine and South Asia show algorithmic speed as a genuine force multiplier and equally show the risks of deploying it without engineered governance—automation bias, unaccountable escalation, and acute vulnerability to electronic and cyber warfare. This article has deliberately not proposed a general AI regulation framework; it has argued that the narrower problem of weapons employment governance requires its own architecture, built on the recognition that meaningful human control, once an engagement window shrinks to single-digit seconds, must be exercised prospectively rather than in real time. Pre-Authorised Autonomous Defensive Response, edge-first hardware built for India's own terrain diversity, a unified ISR data

architecture, and procurement and talent reform matched to software-defined tempo together constitute a defensible answer to the speed-versus-control paradox—one designed to keep India's defensive posture within its IHL obligations through explicit constraints, review and accountability.

Translating this into practice will require the Ministry of Defence, DRDO, the three services, the domestic start-up ecosystem and the diplomatic community—which will need to explain India's approach in forums such as the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems—to move in step, which they do not customarily do. Three concrete steps would begin that process: piloting PAADR's trigger logic and legal-review procedure in the next major tri-service exercise cycle; publishing an Indian doctrinal statement on prospective human control, consistent with but distinct from the ETAI Framework, that other states could examine and, if they choose, adopt; and instituting an annual, parliamentary-facing review of the ring-fenced AI allocation proposed above, so the commitment is tracked rather than merely announced. The conflicts of this decade leave little room for gradualism; they will reward states that decide, deliberately and in peacetime, what algorithmic power they are prepared to wield and under what constraints, rather than states that let the battlespace decide for them.

Endnotes

1 Defence Research and Development Organisation, *Evaluating Trustworthy AI (ETAI) Framework: Version 1.0* (New Delhi: Scientific Analysis Group, Oct 2024).

2 Anita Bhatt, “Artificial Intelligence and India’s Emerging Role in Global Digital Governance”, *International Journal for Multidisciplinary Research* 8, no. 2 (2026), accessed 18 Mar 2026, https://www.ijfmr.com/research-paper.php?id=70753

3 DRDO, *ETAI Framework*, op. cit.

4 Permanent Mission of India to the United Nations, “AI in the Military Domain and Its Implications for International Peace and Security”, national submission pursuant to United Nations General Assembly Resolution 79/239, updated version (2025), Accessed 18 Mar 2026, https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_%282025%29/79-239-India-rev-EN.pdf

5 John Williams, “Locating LAWS: Lethal Autonomous Weapons, Epistemic Space, and ‘Meaningful Human’ Control”, *Journal of Global Security Studies* 6, no. 4 (Dec 2021): ogab015, accessed 19 Mar 2026, https://doi.org/10.1093/jogss/ogab015

6 Meya Kelkar, “Artificial Intelligence in Military Decision Making—A Case for the Human to Stay in the OODA Loop”, Centre for Land Warfare Studies, 06 Jan 2024, accessed 19 Mar 2026, https://claws.co.in/artificial-intelligence-in-military-decision-making-a-case-for-the-human-to-stay-in-the-ooda-loop/

7 Gaurav Saini, *India’s Approach to Military AI: Strategy, Governance, and Challenges* (New Delhi: Council for Strategic and Defense Research, Feb 2026), accessed 20 Mar 2026, https://csdronline.com/indias-approach-to-military-ai-strategy-governance-and-challenges/

8 DRDO, *ETAI Framework*, op. cit.; Permanent Mission of India, UNSG submission, op. cit.

9 Ehab Khalifa, “Blind Technology: Israel’s AI Deployment in Gaza and Lebanon Wars”, Future for Advanced Research and Studies, 07 Oct 2024, accessed 20 Mar 2026, https://futureuae.com/en-US/Mainpage/Item/9735/blind-technology-israels-ai-deployment-in-gaza-and-lebanon-wars

10 Khalifa, op. cit.

11 Michael N. Schmitt, "Israel's Operation Rising Lion and the Right of Self-Defense", *Lieber Institute West Point*, 16 Jun 2025, accessed 21 Mar 2026, https://lieber.westpoint.edu/israels-operation-rising-lion-right-of-self-defense/

12 Wolf-Christian Paes, Edward Beales, Fabian Hinz, and Albert Vidal, *Navigating Troubled Waters: The Houthis’ Campaign in the Red Sea and the Gulf of Aden* (London: International Institute for Strategic Studies, Dec 2024), accessed 21 Mar 2026, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/12/navigating-troubled-waters.pdf

13 Katja Bego, “Ukraine’s Operation Spider’s Web Is a Game-Changer for Modern Drone Warfare. NATO Should Pay Attention”, Chatham House, 06 Jun 2025, updated 17 Jul 2025, accessed 21 Mar 2026, https://www.chathamhouse.org/2025/06/ukraines-operation-spiders-web-game-changer-modern-drone-warfare-nato-should-pay-attention

14 Microsoft Threat Intelligence, *An Overview of Russia’s Cyberattack Activity in Ukraine* (Redmond, WA: Microsoft, 27 Apr 2022), accessed 21 Mar 2026, https://www.microsoft.com/en-us/security/security-insider/threat-landscape/special-report-ukraine; European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024* (Heraklion: ENISA, 2024), accessed 21 Mar 2026, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

15 D. P. Pandey, “Operation Sindoor: Air Power as Enforcer of National Will”, *Journal of the United Service Institution of India* 155, no. 642 (Oct-Dec 2025): 586–96, accessed 22 Mar 2026, https://usiofindia.org/pdf/USI_Journal_2025_Oct-De_4.pdf; Lieutenant General Rajiv Kumar Sahni, quoted in Snehesh Alex Philip, “Op Sindoor Is India’s First AI-Enabled Operation. How ‘Heavy Use’ of Modern Tech by Army Played Out”, *ThePrint*, 07 Oct 2025, accessed 22 Mar 2026, https://theprint.in/defence/op-sindoor-is-indias-first-ai-enabled-operation-how-heavy-use-of-modern-tech-by-army-played-out/2758797/

16 Operation Sindoor: Akashteer Leads AI-Driven Strikes on Terror Launch Pads”, *News on Air*, 16 May 2025, accessed 22 Mar 2026, https://www.newsonair.gov.in/operation-sindoor-akashteer-leads-ai-driven-strikes-on-terror-launch-pads/, Kalyan Ray, “Operation Sindoor: Indian Army’s Home-Grown Akashteer Air Defence Systems Block Pakistan’s Air Adventure”, *Deccan Herald*, 14 May 2025, https://www.deccanherald.com/india/operation-sindoor-indian-armys-home-grown-akashteer-air-defence-systems-block-pakistans-air-adventure-3540833; cf. Tapanjana Rudra, “Operation Sindoor: How AI-Powered Air Defence System Akashteer Shielded India,” *Inc42*, 17 May 2025, accessed 02 Mar 2026, https://inc42.com/features/operation-sindoor-how-ai-powered-air-defence-system-akashteer-shielded-india/

17 Lora Saalman, *AI in Chinese, Indian and US Nuclear Postures, Norms and Systems* (Stockholm: Stockholm International Peace Research Institute, Feb 2026), 20–21, accessed 23 Mar 2026, https://www.sipri.org/sites/default/files/2026-02/2602_ai_integration.pdf; “China’s JARI USV A Orca Unmanned Vessel with VLS Revealed at Zhuhai”, *Army Recognition*, 12 Nov 2024, https://www.armyrecognition.com/archives/archives-naval-defense/2024/chinas-jari-usv-a-orca-unmanned-vessel-with-vls-revealed-at-zhuhai

18 Quwa Team, “GIDS Harbah NG Anti-Ship Cruise Missile (ASCM)”, *Quwa*, 27 Nov 2024, accessed Aug 2026, accessed 23 Mar 2026, https://quwa.org/pakistan/munitions/gids-harbah-ng-anti-ship-missile/;

19 Saalman, op. cit., 25–28

20 20. DRDO, ETAI Framework, op. cit., 4–8.

21 Richard H. Speier, “Hypersonic Missiles: A New Proliferation Challenge”, RAND, 29 Mar 2018, accessed 23 Mar 2026, https://www.rand.org/pubs/commentary/2018/03/hypersonic-missiles-a-new-proliferation-challenge.html

22 U.S. Department of War, *Artificial Intelligence Strategy for the Department of War: Accelerating America’s Military AI Dominance* (Washington, DC: Department of War, 09 Jan 2026), accessed 23 Mar 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF

23 DRDO, ETAI Framework, op. cit.; Permanent Mission of India, UNSG submission, op. cit.

24 Protocol Additional to the Geneva Conventions of 12 Aug 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 08 Jun 1977, art. 36, accessed 24 Mar 2026, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36.

25 Saini, op. cit., 11.

26 Shankar, The Digital Armada, op. cit., chap. 12.

27 Saini, op. cit., 3, 15–16.

28 Saini, op. cit., 12–14.

29 Saini, op. cit., 14.

30 Saini, op. cit., 12–13, 15–16.

Operation X in Naval Warfare History: An Early Example of Indian Maritime Hybrid Warfare

Monika Choudhary[@]

Abstract

This article examines Operation X as an early example of maritime hybrid warfare during the Bangladesh Liberation War. While existing literature on the 1971 conflict has largely emphasised land operations, the Mukti Bahini, and conventional military engagements, the maritime dimension—particularly India's clandestine naval operations in East Pakistan—deserves greater attention. Operation X involved the Indian Navy's training and deployment of Mukti Bahini naval commandos to conduct underwater sabotage against shipping, ports, and inland waterways. This study examines the operation through the complementary concepts of asymmetric and hybrid warfare and argues that its significance lay not merely in the use of irregular maritime tactics but in their integration with India's wider conventional naval strategy. Attacks on key logistical hubs, including Chittagong, Mongla, and Narayanganj, disrupted shipping and supply networks and imposed military and economic costs on Pakistani forces. The article further examines the relationship between

---

[@]**Monika Choudhary** is a Research Assistant at the Centre for Military History and Conflict Studies, United Service Institution of India. She is working on Gallantry Award Portal project for the Ministry of Defence and serves as a Consultant to the Ministry of Defence on the Veer Gatha 4.0 and 5.0 projects. Her research primarily focuses on post-independence wars, with special expertise in non-traditional security threats in the Western Indian Ocean region. Monika holds a Master's degree in National Security Studies from the Central University of Jammu and has prior experience at the National Maritime Foundation, where she deepened her knowledge of maritime security and strategic studies.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

Operation X and conventional naval operations such as Operation Trident and Operation Python. It argues that Operation X offers an important historical case for understanding how conventional naval power, irregular forces, covert action, local intelligence, and attacks on maritime logistics can combine to produce strategic effects. The retrospective application of the contemporary concept of hybrid warfare is acknowledged as a conceptual limitation.

Introduction

The Bangladesh Liberation War of 1971 is frequently characterised by the decisive land campaigns and the rapid defeat of Pakistani forces in East Pakistan. However, the maritime dimension of the conflict was also important to Pakistan's ability to sustain military operations in the eastern theatre. The genocide perpetrated by the Pakistan Armed Forces and the resulting refugee crisis placed India under increasing political, humanitarian, and security pressure. By Apr 1971, the possibility of war in the eastern sector was becoming evident.

East Pakistan's geographical isolation meant Pakistani forces depended heavily on maritime and riverine routes to move troops, equipment, fuel, and other supplies. Control of sea lines of communication and disruption of these logistical networks could therefore influence the outcome of the conflict. The Indian Navy's response extended beyond conventional fleet operations to include covert and irregular maritime activity. Operation X emerged within this wider strategy and involved training and deploying Mukti Bahini naval commandos to sabotage shipping and port infrastructure.[1]

The central argument of this article is that Operation X should be understood not simply as a covert naval or commando operation but as an important early case of integrating asymmetric maritime tactics with conventional naval power. The operation used irregular personnel, local networks, covert infiltration, underwater sabotage, and attacks on maritime logistics while forming part of a broader Indian strategy that also included overt naval operations. The article

therefore asks how Operation X combined conventional and unconventional means, what strategic effects this combination produced, and to what extent the operation can be interpreted through the contemporary concept of maritime hybrid warfare.

The study first examines the existing literature and research gap. It then considers the strategic and maritime context of the 1971 war, the planning and organisation of Operation X, its execution and effects, and finally its significance as an early example of maritime hybrid warfare.

Literature Review

Existing literature on the Bangladesh Liberation War has focused extensively on the political crisis, military operations on land, the Mukti Bahini, and the conventional campaigns of the Indian and Pakistani armed forces. The maritime dimension, particularly India's clandestine naval activity in East Pakistan, has received comparatively less attention.

Operation X: The Untold Story of India's Covert Naval War in East Pakistan (2019), by Captain M N R Samant and Sandeep Unnithan, is an important source for understanding the planning, organisation, training, and execution of the naval commando campaign. G M Hiranandani's *Transition to Triumph: History of the Indian Navy 1965–1975* provides a broader naval and operational context.[2] Secondary sources and contemporary narratives also describe attacks at Chittagong, Mongla, and Narayanganj.

The principal gap identified in this literature is conceptual. Operation X is generally presented as a covert naval, commando, or sabotage operation rather than examined through a hybrid maritime warfare framework. This distinction is important because the operation involved more than irregular action by local personnel. Its significance also derived from the interaction between irregular forces, covert action, local intelligence, maritime sabotage, and conventional Indian naval power.

For this study, asymmetric warfare refers to exploiting capability differences through unconventional methods, while hybrid warfare refers to the coordinated employment of conventional and irregular approaches within a broader strategy.[3] The article does not claim that Indian planners in 1971 used the contemporary term 'Hybrid Warfare'. Instead, it applies the concept retrospectively as an analytical framework and examines whether Operation X's characteristics support that interpretation.

Research Methodology

This study adopts a qualitative historical case-study approach. It examines Operation X through a descriptive and analytical reconstruction of its strategic context, planning, organisation, execution, and effects. The principal sources identified in the article include published memoirs, historical accounts, operational narratives, and secondary literature, particularly the works of M N R Samant, Sandeep Unnithan, and G M Hiranandani.

The analytical framework combines asymmetric warfare and hybrid warfare. The former assesses the operational methods employed by the naval commandos, while the latter examines the relationship between irregular maritime action and conventional naval operations. The study focuses on the interaction between means, actors, and strategic effects rather than the label alone.

The study has two principal limitations. First, the limited availability of declassified primary material concerning the planning and command structure of Operation X means that the analysis relies substantially on published memoirs and secondary accounts. Second, applying a contemporary concept such as hybrid warfare retrospectively to a 1971 operation creates a conceptual limitation. The article therefore treats Hybrid Maritime Warfare' as an analytical interpretation rather than a historical description used by the actors themselves.

Strategic and Maritime Context of the 1971 War

The political crisis following the 1970 general elections and the subsequent military crackdown created widespread violence against the Bengali population, a large refugee movement into India, and eventually the Bangladesh Liberation War. During the conflict, the Mukti Bahini emerged as the principal resistance force in East Pakistan and targeted communication networks, infrastructure, and supply routes.

East Pakistan's geography shaped the conflict's maritime dimension. The region's separation from West Pakistan made maritime and riverine transportation essential for sustaining Pakistani forces. Chittagong, Mongla, and Narayanganj served as key logistical hubs connected to an extensive inland waterway network.[4] Disrupting these routes could therefore have effects beyond the immediate destruction of individual vessels. It could disrupt the movement of supplies, restrict access to ports, and force Pakistan to divert resources to protect vulnerable maritime infrastructure.

This strategic vulnerability created an operational rationale for covert maritime sabotage. Operation X sought to exploit Pakistani forces' dependence on shipping, ports, and inland waterways while avoiding direct naval confrontation in every target area.



Image 1: Mukti Bahini Fighters

Planning and Organisation of Operation X

Operation X, officially designated Naval Commando Operations (X), was a covert maritime campaign approved by Prime Minister Indira Gandhi and executed by the Indian Navy to disrupt Pakistan's logistical network in East Pakistan. Admiral S M Nanda supervised the operation, and Captain Mihir Kumar Roy, Director of Naval Intelligence, coordinated it and developed the 'Water Rat' concept to train about 600 Bengali naval commandos for underwater sabotage missions.[5]

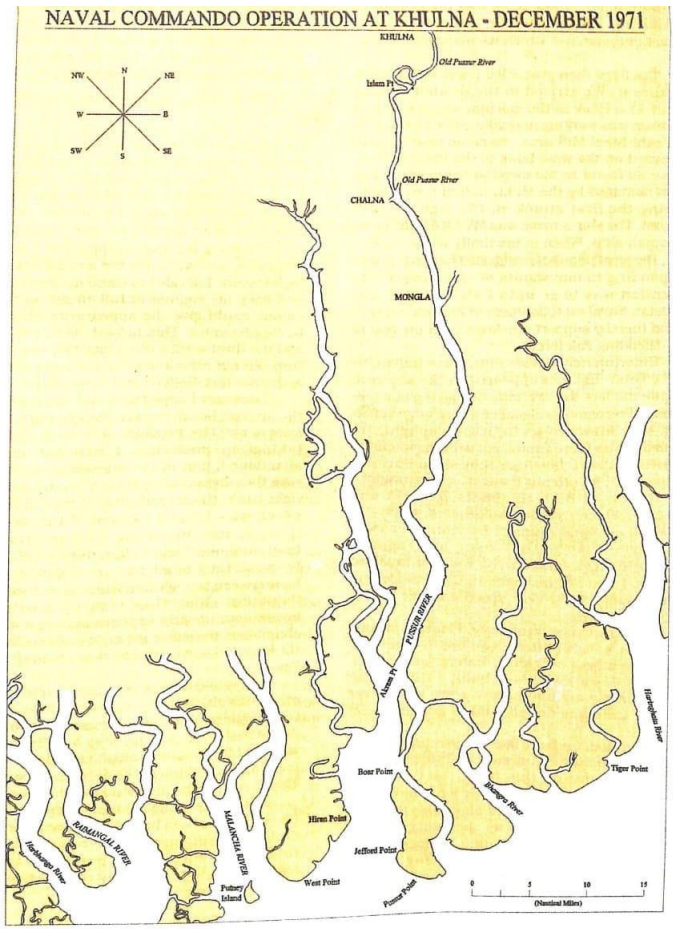
The 'Mangro Eight', a group of Bengali submariners who had defected from the Pakistan Navy, supported recruitment and local intelligence. Commander M N R Samant oversaw field operations and coordinated between Naval Headquarters and the Army's Eastern Command.[6]

A secret facility at Plassey, codenamed Camp 2 Plassey (C2P), was established to train the recruits in endurance swimming, weapons handling, and the use of limpet mines under the supervision of Indian Navy clearance divers.[7]

The operational plan was executed in three phases:

- Phase One: Fifty teams focused on ports and harbours, launching coordinated attacks on Chalna/ Khulna and Mongla to sink ships, barges, and steamers, blocking harbour access.
- Phase Two: One hundred teams moved inland to disrupt the riverine network by sinking vessels, obstructing channels, removing navigational aids, and destroying ferries and pontoons.
- Phase Three: Two hundred teams conducted large-scale operations to paralyse ports, communications, and inland waterways.[8]

Specially designed limpet mines enabled underwater sabotage, and coded All India Radio broadcasts coordinated simultaneous attacks across multiple locations.[9]



Map 1: Operation X

Source: Hiranandani, G M, *Transition to Triumph History of the Indian Navy 1965-1975*

Execution of Maritime Sabotage Operations

Infiltration Techniques

Commandos infiltrated East Pakistan through secret border points such as Hasnabad, Taki, and Agartala using methods designed to maintain secrecy.[10] Small teams of three to five commandos moved through local villages in civilian clothing, often guided by Mukti Bahini networks. They travelled mainly at night and used village safe houses during the day. For the final stage of an approach, commandos

entered the water upstream of their targets and used river currents to move towards anchored vessels while reducing the risk of detection. Camouflage methods included swimming on their backs or diagonally and using floating vegetation or bamboo reeds to remain concealed.[11]

Underwater Sabotage and Limpet Mines

Locally developed limpet mines were used to attack steel-hulled vessels. The mines were designed to attach magnetically to ships and used a delayed-fuse mechanism.[12] Commandos also adapted the mechanism to account for the time required to reach their targets. Once the commandos reached a vessel, they fixed the mines below the waterline, usually near the engine room or propeller shafts, to maximise damage.[13]

Strategic Sabotage of Key Ports

The first large-scale coordinated attacks occurred on the night of 14–15 Aug 1971 under the codename Operation Jackpot.[14] Naval commandos attacked strategic ports in East Pakistan. At Chittagong, commandos infiltrated the harbour and destroyed cargo vessels carrying military supplies. At Mongla, sabotage operations damaged foreign and Pakistani merchant ships anchored in the Pussur River, disrupting shipping and export activity. At Narayanganj, commandos targeted river steamers and inland transport facilities.[15]

These operational methods show the asymmetric character of Operation X. Small teams, local knowledge, concealment, and underwater sabotage let the commandos attack a larger logistical system without engaging Pakistani forces in conventional naval combat.



মুক্তিযুদ্ধে বাংলাদেশ নৌ–কমান্ডোদের আক্রমণের পূর্ব মুহূর্তের একটি দৃশ্য। কমান্ডোদের সবার বুকে মাইন। ছবিটি চাঁদপুর এলাকায় তোলা।

Image 2: Bangladesh Navy Commandos before at attack in Chandpur during Liberation War[16]



Oil Tanker Sunk as Government Reports Sharp Rise in Guerrilla Activity in East Pakistan

Chittagong Port Blocked
Eight Ships Sunk In A Day By Guerrillas

Freedom fighters sink 7 Pak ships

British ship holed in Pakistan port by East Bengal frogmen

Valiant struggle of the Bangla Desh freedom fighters

by PRABHAT DAS GUPTA

Image 3: Media coverage of Operation Jackpot[17]

Strategic Impact of Operation X

The attacks had effects at several levels.

Military and Logistical Effects

The destruction and damage inflicted on shipping disrupted Pakistan's maritime logistics. More than 100,000 tons of shipping were reported as sunk or damaged over the course of the operation. Sunken vessels obstructed shipping channels and reduced access to berths. The threat of further sabotage also reduced foreign shipping companies' willingness to use East Pakistani ports. The Pakistani military consequently had to divert resources to protect ports and waterways, reducing resources available for counter-insurgency operations.

Economic Effects

The attacks affected commercial shipping, port activity, and military logistics. The increased risk at East Pakistani ports further disrupted maritime trade and shipping. Thus, the operation produced effects beyond the immediate physical destruction of vessels.

Psychological and Strategic Effects

The vulnerability of ports and waterways imposed psychological pressure on the Pakistan Navy and military authorities. The need to protect maritime infrastructure and shipping complicated military operations. By constraining the movement of supplies and contributing to the disruption of maritime communications, Operation X supported the broader strategy of isolating Pakistani forces in East Pakistan.

The significance of these effects lies in the relationship between relatively small-scale tactical actions and wider strategic consequences. Operation X did not seek to defeat Pakistani naval forces through fleet engagement. Instead, it exploited vulnerabilities in the logistical system those forces depended on.



Image 4: Navy commandos attack the US ship SS Lightning in Mongla on 15 Aug 1971[18]

Operation X as Maritime Hybrid Warfare

The strongest basis for interpreting Operation X as an early example of maritime hybrid warfare lies in how different forms of military power interacted. The operation did not consist exclusively of irregular action, nor was it an independent commando campaign detached from India's wider military strategy.

First, the operation employed irregular forces. Bengali naval commandos drawn from the Mukti Bahini provided local knowledge and operated in an environment in which conventional Indian naval forces faced significant access and concealment challenges.

Second, it relied on covert and asymmetric methods. Small teams infiltrated through local networks, approached targets clandestinely, and used underwater sabotage rather than direct naval engagement. This enabled relatively small forces to impose costs on a much larger logistical system.

Third, Operation X involved intelligence and local networks. Recruiting Bengali submariners, using local intelligence, supporting

the Mukti Bahini, and coordinating with Indian naval and military authorities connected the tactical missions to a wider operational framework.

Fourth, the operation generated multiple strategic effects. The immediate effects were physical damage to shipping and port infrastructure, but these actions also disrupted logistics, affected commercial shipping, imposed security costs, and contributed to the isolation of Pakistani forces.

Finally, Operation X existed alongside conventional Indian naval power. Operation Trident and Operation Python demonstrated India's ability to conduct overt naval strikes, while Operation X provided a complementary way to attack maritime vulnerabilities through covert and irregular means. The significance therefore lies not in the existence of irregular tactics alone but in their relationship to conventional naval operations and wider strategic objectives.

On this basis, Operation X can reasonably be interpreted as an early example of maritime hybrid warfare. The term should nevertheless be applied cautiously. The operation predated the contemporary theoretical development of hybrid warfare, and the available evidence does not establish that Indian planners conceived of it in those terms. The argument is therefore analytical and retrospective: Operation X displayed several characteristics that are now associated with hybrid approaches to warfare.

Integration with Conventional Naval Operations

Operation X is best understood within the Indian Navy's broader maritime strategy during the Bangladesh Liberation War. While the naval commandos conducted covert sabotage in East Pakistan, the Indian Navy later employed conventional naval power during the war. Operation Trident and Operation Python represented overt naval strikes against Pakistani naval and logistical assets, particularly at Karachi.[19]

The contrast between these operations is analytically important. Conventional naval operations relied on naval vessels, missile systems, and direct attacks, whereas Operation X relied on irregular personnel, concealment, local networks, and underwater

sabotage. The two approaches therefore addressed different vulnerabilities and operated at different levels.

Together, they expanded India's maritime options. Conventional forces could impose direct military pressure, while covert commando operations could disrupt shipping and infrastructure in areas where conventional naval action was less suitable. Operation X should consequently be viewed as complementary to, rather than a substitute for, conventional naval power.

This integration provides the strongest basis for the article's hybrid-warfare argument: different forms of maritime power were employed against interconnected military and logistical vulnerabilities to pursue wider strategic objectives.

Operation X in the Evolution of Naval Warfare

Operation X demonstrates how maritime warfare can extend beyond traditional fleet engagements, blockades, and attacks on enemy warships. Its use of local personnel, covert infiltration, underwater sabotage, and attacks on logistical infrastructure illustrated the potential of targeting an adversary's maritime support system rather than focusing solely on its combat fleet.

The operation also demonstrated the value of local knowledge and irregular forces in complex maritime environments. Bengali commandos familiar with the waterways and local terrain could operate in areas that were difficult for conventional naval forces to access covertly. This expanded the operational reach of India's maritime campaign.

Its historical significance therefore lies less in suggesting that hybrid warfare began in 1971 and more in demonstrating an early form of the operational logic later associated with hybrid conflict: combining different actors, methods, domains, and effects to achieve strategic objectives.

Limitations

The study is constrained by the limited availability of declassified primary sources concerning the planning and command structure of Operation X. Consequently, the analysis relies substantially on published memoirs, historical accounts, and secondary sources. Applying the contemporary concept of hybrid warfare retrospectively to a 1971 operation also has conceptual limitations. The article therefore treats hybrid maritime warfare as an analytical framework rather than a term the actors themselves used.

Contemporary Relevance

The character of warfare has evolved considerably since 1971, with cyber operations, information warfare, electronic warfare, artificial intelligence, and network-centric capabilities becoming increasingly important. Contemporary conflicts also show the continued vulnerability of maritime trade, ports, energy infrastructure, and shipping to covert and irregular disruption.

Operation X remains relevant because it illustrates a principle that extends beyond its historical setting: strategic effects can be achieved by combining conventional military power with irregular capabilities and by attacking the logistical systems that sustain an adversary's military capacity. The technological environment has changed, but the importance of intelligence, concealment, local networks, operational coordination, and protecting maritime infrastructure remains.

Conclusion

Operation X was an important component of India's maritime strategy during the Bangladesh Liberation War of 1971. By training and employing Mukti Bahini naval commandos for covert underwater sabotage, India was able to attack shipping, ports, and inland waterways that were essential to Pakistan's ability to sustain military operations in East Pakistan.

The operation's significance, however, extends beyond the physical destruction of vessels. Its strategic value arose from the combination of irregular forces, covert action, local intelligence,

maritime sabotage, and conventional Indian naval power. Operation X therefore provides a strong historical case for examining the interaction between asymmetric and conventional maritime warfare.

Although the contemporary concept of hybrid warfare must be applied retrospectively and with caution, Operation X displayed several characteristics now associated with hybrid approaches: the use of multiple actors and methods, exploitation of logistical vulnerabilities, covert action, and the integration of irregular activity with conventional military operations. Its historical legacy consequently lies in demonstrating how relatively small-scale maritime actions can generate wider military, economic, psychological, and strategic effects.

Endnotes

1 M N R Samant and Sandeep Unnithan, *Operation X: The Untold Story of India's Covert Naval War in East Pakistan* (HarperCollins Publishers India, 2019)

2 Samant and Unnithan, *Operation X*; G. H. Hiranandani, *Transition to Triumph: History of the Indian Navy, 1965–1975* (New Delhi: Lancer Publishers, 2000).

3 Rank G Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018): 30–47, accessed 15 Apr 2026, https://ndupress.ndu.edu/Media/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

4 G H Hiranandani, *Transition to Triumph: History of the Indian Navy, 1965–1975* (New Delhi: Lancer Publishers, 2000), 99–103.

5 M N R Samant and Sandeep Unnithan, *Operation X: The Untold Story of India's Covert Naval War in East Pakistan* (HarperCollins Publishers India, 2019), 44.

6 M N R Samant and Sandeep Unnithan, ibid.

7 Ibid.

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 “Choking Pakistan’s Artery: Naval Commando Story”, The *Business Standard*, accessed 16 Apr 2026, https://www.tbsnews.net/bangladesh/50-years-freedom/choking-pakistans-artery-naval-commando-story-222142

17 Ibid

18 Ibid

19 Ibid.

Cognitive Warfare: India's Approach to Influencing Perception and Behaviour

Wing Commander Maxmillan GG[@]

"क्रोधाद्भवति सम्मोह: सम्मोहात्स्मृतिविभ्रम: |

स्मृतिभ्रंशाद् बुद्धिनाशो बुद्धिनाशात्प्रणश्यति ||"

"Anger leads to clouding of judgment, which results in bewilderment of memory. When memory is bewildered, the intellect gets destroyed; and when the intellect is destroyed, one is ruined".

— Chapter 2, Verse 63 - Bhagavad Gita

Abstract

This essay examines cognitive warfare as a critical and evolving domain in modern conflict, focused on influencing human minds. Tracing the fundamentals of Cognitive Warfare (CW) strategies, the essay establishes its reach beyond traditional psychological and information warfare. It further assesses global strategic threats, focusing on international players, state and non-state actors. This essay proposes a comprehensive National Cognitive Warfare Strategy for India, blending traditional wisdom with today's security needs. It identifies key pillars for building global ecosystem engagement, defensive

---

[@]**Wing Commander Maxmillan GG** is an Indian Air Force officer with 18 years of service and extensive experience as a Weapon System Operator on Su-30 MKI aircraft. He specialises in aerial warfare, war planning, electronic warfare, multi-domain operations and imagery intelligence. A qualified Psychologist Assessor, he has experience in inter-service operations, policy formulation and humanitarian assistance and disaster relief. He holds postgraduate degrees in Aviation Law and Air Transport Management and Psychology.

Journal of the United Service Institution of India, Vol CLVI, No. 645, July-September 2026.

resilience and offensive capabilities, while addressing institutional challenges, legal reforms and future technological trends. Ultimately, it lays out a vision for moving forward that focuses on merging different sectors, updating laws, using innovative and balanced strategies, developing talent, fostering innovation, and expanding into new areas. The essay underscores CW's pivotal role as a sixth domain of warfare in shaping India's advance as a global leader.

Introduction

In modern warfare, the functionality of human cognitive components—perceptions, attitudes, and behaviour—is a critical determinant of outcomes. Historical strategists like Sun Tzu, Clausewitz, and Kautilya discussed altering cognition in conflict, though Cognitive Warfare (CW) was not formally recognised as a distinct domain. Traditionally, CW manifested through psychological and information warfare methods such as perception management, information control, deception, decoys, concealment, or economic strangulation to gain advantage with minimal physical confrontation. In the 21st Century, technological progress has radically expanded the scale and speed of information and mis/disinformation dissemination. Internet of Things, social networks, and mobile technologies propel this hyper-connectivity.[1] Intra- or inter-connected homophilic societies make distances and boundaries almost non-existent. The world is at a crossroads where opinion-driven narratives overshadow facts, and human mind polarisation is the new norm. This paradigm shift elevates CW beyond traditional warfare mechanics as a quintessential method clasping its tentacles around the originator and progressors of war–the 'Human Mind'.[2]

Diverging from prevailing Indian commentary, this essay examines CW as an interconnected, penetrating method of warfare that extends beyond information and psychological warfare. It will first explain CW. Secondly, it will examine the strategic threat landscape. Thirdly, it will propose a national cognitive warfare strategy for India. Fourthly, it will identify key pillars of India's cognitive warfare approach.

And fifthly, it will analyse challenges to institutionalising CW and recommend a domain-specific path for India.

Understanding Cognitive Warfare

Cognitive Science. A foundational understanding reveals cognitive science as an interdisciplinary field.[3] It transcends the spectral boundaries of science, social science and allied arts. It includes subjects like psychology, anthropology, computer modelling, and Artificial Intelligence (AI),[4] philosophy, political science, sociology, and neuroscience. The North Atlantic Treaty Organisation (NATO) describes it as the convergence of cyber-psychology, the weaponisation of neuroscience, and cyber-influence.[5] CW is the superset of coordinated information, psychological and cyber operations.[6]

Defining CW. A useful definition: 'Cognitive Warfare is a strategy that focuses on altering how a target population thinks and, through that, how it acts'.[7] It alters natural cognitive processing of how others think, feel or act. By shaping the 'Who' (Communicator), 'What' (Message), 'Which' (Medium), 'Whom' (Receiver), 'When' (State) and 'How' (Effect) of communication[8]. It is deemed to exist when the end game of altered behaviour is achieved through shaped perceptions, influenced attitudes or hindered memory processing.

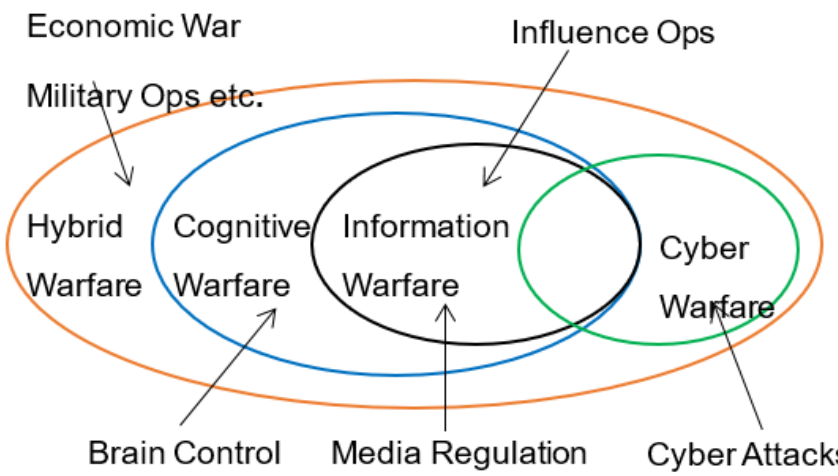


Figure 1: Relationship among Cognitive Warfare and Other Types of Warfare

Source: Journal of Global Security Studies[9]

Segments of CW. For effective application, CW involves influence, information, psychological, cyber, space, and neuroscience operations, with a legal watch for ethical regulation. It penetrates deeper into neurological, socio-cultural and behavioural systems, disrupting social unity and undermining group resolve to impact society's collective cognition. Unlike traditional warfare, it steers individuals or societies overtly or covertly to achieve victory without a battle. It permeates all existing domains—land, sea, air, space, and cyberspace—emerging as the sixth domain of warfare.[10]

The Strategic Threat Landscape

NATO Perspective. Having understood the significance of CW, it is essential to grasp its evolving strategic threat landscape. The NATO Warfighting Capstone Concept already recognises a CW strategy.[11] The inaugural NATO scientific meeting on CW was held at Bordeaux in France on 21 Jun 2021.[12] NATO Allied Command Transformation in Norfolk, United States (US), emphasises the militarisation of Nanotechnology, Biotechnology, Information Technology, and Cognitive Science technologies. Like the Modelling and Simulation Group, their teams focus on research and development.[13]

Adversarial CW. The West depicts Russia as a key CW actor and a model for China, Iran, and North Korea.[14] They claim that Russian tactics, rooted in the Soviet concept of reflexive control,[15] are used to challenge democratic processes in the US,[16] Baltic states and France.[17] The Chinese Communist Party's United Front is implicated in electoral interference in Canada, Australia, and New Zealand.[18] North Korea combines nuclear coercion with cognitive manipulation to influence decision-making,[19] while Iran spreads social and moral jihad propaganda against the US and Israel through universities and religious centres to foment internal dissent.[20]

China's Three Warfares. CW in the Indian neighbourhood is a significant and evolving challenge. China implements the '*San Zhong Zhanfa'* or Three Warfares strategy, which involves public opinion, psychological, and legal warfare.[21] It is a stratagem based on Sun Tzu's principle of subduing adversaries without direct conflict. These

strategies were evident during the Doklam standoff (2017) and the Galwan Valley clash (2020). China preferred non-kinetic tactics, using government information departments to shape perceptions and avoid direct military engagement with India.

Pakistan's CW. Pakistan's Inter-Services Public Relations abuses social media to invoke societal divisions and incite unrest.[22] During Operation Sindoor, Pakistan employed AI-generated deep fakes and disinformation targeting India's democracy, leadership, military and public sentiments.[23] India's Ministry of Information and Broadcasting, backed by the Army's Corps of Signals and the National Cyber Coordination Centre, stepped in to push back. Indian approach was centred on open updates, primarily through daily briefings from the Ministry of External Affairs. While the response was quick, it was reactive. It was neither coordinated nor built from any long-term system, relying more on exposing misinformation than being proactive.

Non-State CW. Beyond conventional conflict scenarios, proxies, non-state actors, and institutions adopt CW to manipulate perceptions, influence behaviour and destabilise societies. Terrorist and separatist groups in Jammu and Kashmir have exploited CW through social media to further their agendas, recruit youth and incite religious extremism to fuel unrest and undermine security forces.[24] The Havana Syndrome case, though unattributed, exemplifies CW infiltrating the physical domain and causing neurological damage.[25]

Classifications of CW Threats. An assessment of the threat landscape identifies three broad categories of CW targets based on scale: large groups sharing common characteristics (such as populations and ethnic or religious communities), smaller groups united by common objectives (such as companies, teams and armed forces), and critical individuals (such as decision-makers and leaders). These targets can be further classified by their degree of cognitive permeability into open societies (democracies), closed societies (dictatorships or autocratic regimes), and controlled societies, where stringent regulations or legal frameworks restrict information dissemination.

India's National Cognitive Warfare Strategy

Need for NCWS. The emerging strategic threat landscape highlights the vulnerabilities of this sixth dimension of warfare, emphasising the need to develop India's National Cognitive Warfare Strategy (NCWS). Kautilya's Arthashastra, our ancient treatise on statecraft, posits that 'A Well-reasoned Policy' serves as the fundamental thread that ensures the stability of the state.[26] Therefore, this formulation process must be elaborate, resolving asymmetric balances and questioning confusing dogmas focused purely on risk management and reduction.[27]

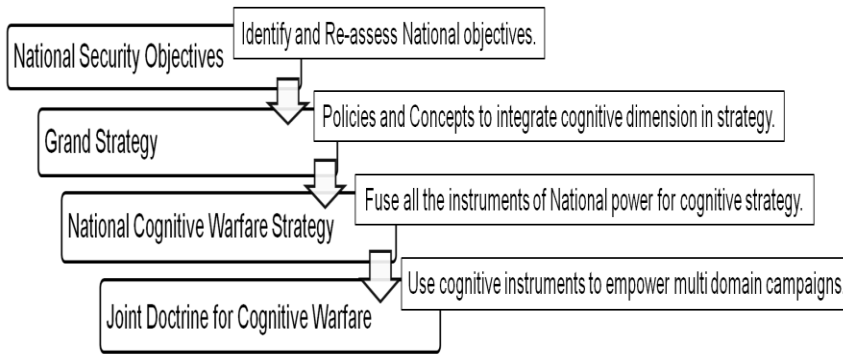


Figure 2: India's National Cognitive Warfare Strategy
Source: Compiled by the author

NCWS Framework. The NCWS must align with national security objectives and grand strategy, leverage contemporary strengths, and address gaps. A practical, pragmatic roadmap for the NCWS may be led by a high-level national security authority, such as the National Security Coordination Secretariat, which would act as a facilitator, advocate, and guardian. It should be a unified, specialised framework integrated across all instruments of national power, with grand strategy serving as the overarching mechanism synchronising military and non-military elements. Under its umbrella must exist the Joint National Cognitive Task Force, a purpose-driven, whole-of-nation team of government agencies, intelligence, armed forces, paramilitary, think tanks, academia, cyber institutions, industry, start-ups and society.

NCW Doctrine. A National Cognitive Warfare Doctrine (NCWD) must derive from the NCWS to establish actionable subordinate doctrines across all national power instruments at strategic, operational, and tactical levels. Respecting the sensitive nature of some elements, the NCWD can have public and classified versions.

Joint CW Doctrine. Drawing inspiration from the combined national approach, the military must weave its own Joint Doctrine for Cognitive Warfare (JDCW). This doctrine must be built on the existing Joint Doctrine for Multi-Domain Operations, Joint Doctrine for Perception Management and Psychological Operations, and the Joint Doctrine for Cyber Space Operations. This doctrine should form a flexible framework aligned with the grand strategy, coordinating all military CW capabilities through the Joint Planning Coordination Centre under the Chiefs of Staff Committee.[28] The JDCW should adopt a future-oriented, holistic outlook, emphasising strategic resource allocation and inter-agency coordination for seamless implementation. It should remain fundamentally stable, allowing only structural updates dictated by the doctrinal loop. It must establish clear strategic definitions to streamline operational planning and approvals across conflict levels.

Joint CW Team. Driven from a military vantage, a Joint Cognitive Warfare Team can execute goal-specific tactical cognitive operations. Because it is military-heavy, the team can also include embedded elements from all other segments of national power. Further, individual services should establish specialised teams to explore this domain without rigid boundaries hindering effectiveness.

Key pillars to India's Cognitive Warfare approach

India's CW approach should be based on the principle of 'One for All, All for One'. Based on this philosophy, the three pillars are the global ecosystem, defensive (domestic), and offensive (adversary), as shown in Figure 3. These pillars have co-functionality to prevent counter productivity, mandating existence in parallels and intersections.

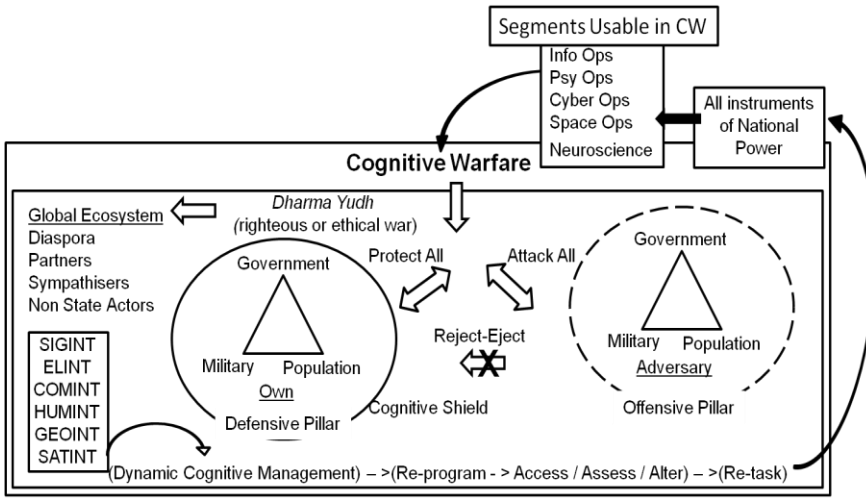


Figure 3: Pillars to India's Cognitive Warfare Approach
Source: Compiled by the author

The Global Ecosystem Pillar. India's CW strategy calls for unified global outreach that leverages soft power to shape international perceptions favourably. This includes engaging the diaspora, partners, non-state actors, and sympathisers through think tanks, media, sports, and cultural interfaces like yoga, arts, literature, cuisine, cinema, democratic traditions, and socio-economic exchanges.[29] Emphasising spirituality, socio-cultural values and democratic principles, India should spearhead multilateral cognitive organisations, convene summits and conduct cognitive gaming exercises to address security challenges collaboratively. Each kinetic military action should be paired with a cognitive initiative ensuring transparency and global support under the *Dharma Yuddha* (righteous or ethical war) principle. Platforms like the Raisina Dialogue and the Indian Ocean Conference aid coalition building, diplomatic isolation of adversaries and strategic communication.

Defensive Pillar: Safeguard One's Own Interests. Establishing cognitive safeguards to thwart adversarial attempts and secure India's national power instruments, including the population, government, and military, is essential. A cognitive shield must begin with a comprehensive risk assessment of the population-government-military trinity. Clear demarcation of cognitive

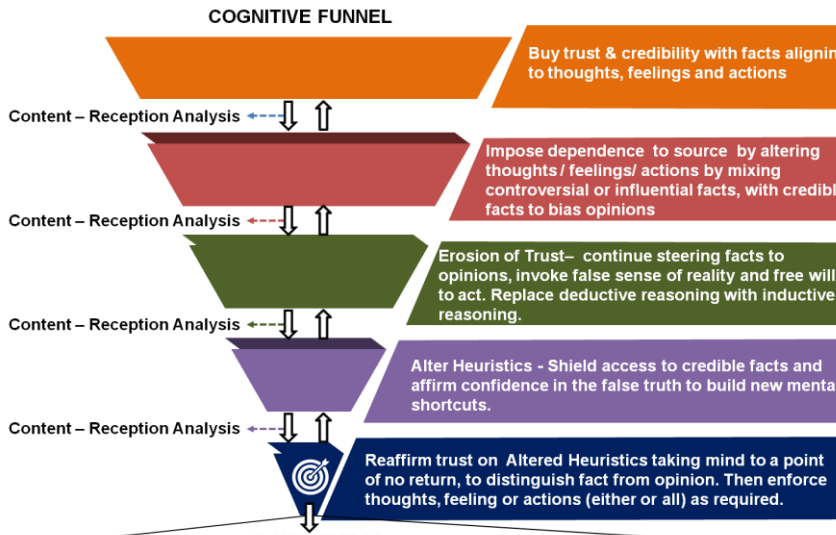
boundaries and management of functional overlaps is vital to create impenetrable defences. India's vast digital ecosystem, with over 700 million internet users, is a critical battleground. A layered resilience posture that incorporates these strategies can insulate the shield against foreign propaganda and targeted disinformation. Mass digital literacy is imperative to withstand shocks and prevent information operations and psychological tactics enhanced by AI and machine learning from eroding trust in democratic institutions.

Cognitive Resilience. An enhanced 'Observe, Orient, Decide, Act loop' for all decision-makers, built on unhindered access to factual data, will be the pillar's foundation. This involves redundancy in critical systems, supported by a culture of continuous learning. Allowing citizens to verify facts is vital to demystifying CW identification and data transparency. Such heightened awareness is essential for the stability and security of India's 1.46 billion citizens. Effective defence measures should serve as proactive deterrents, ensuring unhindered battlefield visibility through satellite surveillance and high-resolution imagery. Additionally, initiatives to condition hearts and reprogram minds are indispensable.

Offensive Pillar. Indian values of Ahimsa and Non-Alignment have kept Indians rooted in collective consciousness for peaceful co-existence. However, provocations necessitate defensive and offensive counterbalancing. Employing a hierarchical CW Matrix with escalation and de-escalation protocols maintains this equilibrium. Offence begins with eliminating attack detection and attribution errors, followed by clear rules for engagement, intrusion, neutralisation, extraction, and termination to ensure precision and control. The matrix should follow the principles of war and manoeuvre warfare at lower levels, unsettle the enemy's Centre of Gravity, and target vulnerabilities to fracture adversarial cohesion. Advanced phases must engage multi-spectral cognitive traps across all its segments to disrupt decision-making covertly. A Dynamic Cognitive Management Team can continuously adapt the response to match the progression of warfare.

Cognitive Trap. The author proposes exploring spiralling neural pathways through a cognitive funnel into a cognitive trap (shown in

Figure 4). This psychologically grounded strategy will be particularly effective for dominating CW. As shown, establishing a causal effects relationship shall permit deployment of harmful payloads to achieve cognitive supremacy. Such methods can be applied broadly within the Offensive Pillar. Other methods include unplug, corrupt, disorganise, diagnose and enhance.[30]



Likely Cause	Cognitive Dissonance, Distortion, Intrusive Thoughts	Apathy/Avolition, Cognitive overload, Thought blocking,	Counterfactual thinking, Overgeneralization, Faulty Emotional Regulation, Bandwagon effect	Precognition, Learned helplessness, Distorted Perception	Emotional override	Affect heuristic	
THINK	✓	✗	✗	✓	✓	✗	✗
FEEL	✗	✓	✗	✓	✗	✓	✗
ACT	✗	✗	✓	✗	✓	✓	✗
Likely Effect	Belief Bias, Emotional Numbing or Dissociation, Confirmation Bias, Loss Aversion, Counterfactual Thinking, Unconscious biases, Negativity bias	Availability Heuristic, Framing Effects, Hindsight Bias	Intention-Behavior Gap, Automaticity, Attention Bias, Foolhardiness, Fear (flee), Representativeness heuristic	Anchoring bias, Confirmation bias, Paralysis by Analysis, Status Quo Bias		,	Total Non - functionality
✓	Functioning of the specific component of Cognition, though not confirmed to be at desired level.						
✗	Non - functioning of the component of Cognition at desired level, though not confirmed to be purely non-functional.						

Figure 4: Suggested usage of Offensive Pillar
Source: Compiled by the author

Challenges to institutionalising CW

While India has seen how to build her CW strategy, one must understand certain challenges when employing it.

Intent to understand, appreciate, and employ it. CW is inherently disruptive and non-linear, and requires recognition of its dual nature as both a threat and an opportunity in hybrid and grey zone conflicts. Its distinction from cyber, information and psychological warfare must not be overlooked. Effective employment requires a pragmatic strengths, weaknesses, opportunities and threats analysis. Reluctance to formalise strategies stems from rigidity and fear of criticism, hindering effective risk management.

Barriers to Unified Integration and Collective Thinking. This domain rides upon advancing technological capabilities. Siloed research, insufficient interdisciplinary collaboration, and fragmented national efforts across government, military, intelligence, media, and information technology sectors exacerbate contradictory cognitive missions. Unaddressed fundamental gaps, a void of cohesion, integration and fusion- shake the foundations of the pillars of national cognitive strongholds.

Capability Building Measures in Human Resources and Infrastructure. A limited indigenous focus on AI, machine learning, and cloud infrastructure hinders capability building. Innovations fail to transition from academia to industry because research remains limited to theoretical or small-scale studies. Micro, small and medium enterprises face financial and regulatory barriers, resulting in low technology adoption and skill gaps.[31] Scalability requires enhanced infrastructure and streamlined processes.

Ethical and Human Rights Concerns. Current legal and regulatory frameworks lag behind technology, requiring a strong ethical and legal structure to isolate aberrant actors. CW operates in international legal grey areas and lacks explicit provisions under international humanitarian law or the UN Charter. Cognitive operations below armed conflict thresholds pose significant legal challenges. The capacity of *the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam of*

2023 to attribute cognitive activities as offences against the state, organised crime, and terrorism is ambiguous.[32]

Way forward

Advance from Integration to Fusion for Domain Capability. Capability development should commence with robust cognitive shielding and progressively evolve towards offensive cognitive capabilities. Strengthen population resilience through digital literacy, critical thinking, and metacognitive training to counter misinformation, disinformation, deep fakes, and engineered social media narratives. Long-term capacity-building should leverage advanced technologies, including artificial intelligence and data analytics, to maintain an up-to-date understanding of adversary information ecosystems and behavioural patterns. An integrated whole-of-nation approach that brings together government, military, academia, industry, and civil society is essential to bridge existing capability gaps and ensure inclusivity. A centralised national agency should provide strategic direction, standards, and oversight, supported by decentralised operational entities for effective implementation. Finally, sustained global engagement with leading research institutions and think tanks, coupled with the creation of autonomous, mission-oriented innovation teams, will foster indigenous expertise and accelerate the development of cognitive warfare capabilities within a robust national security framework.[33]

Legal Reforms and International Cooperation. Implement policy reforms and strengthen international cooperation. Expand the legal framework to regulate the misuse of the cognitive domain at both the domestic and international levels. Establish a legal tribunal within the national security architecture to oversee violations relating to cognitive warfare. Adopt adaptive cybersecurity laws and information-sharing models inspired by Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA), while safeguarding democratic freedoms and freedom of expression.

Develop Balance for CW Tactics. Cognitive tools can either exploit or enhance human cognition, making the offence-defence balance crucial for preserving force and optimising performance. This includes integrating counter-propaganda, strategic communication, and resilience training. Develop advanced AI-driven detection of disinformation and social engineering to mitigate echo chambers, biases, and targeted manipulation. The focus of offence must evolve from merely understanding adversaries' minds to actively shaping their actions.

Invest in Human Resources and Innovate Emerging Technologies. Invest in human resources and innovation through multidisciplinary convergence. Support talent development, public-private partnerships and advances in cognitive sciences, including generative AI, cyber forensics, machine learning, deep learning and quantum computing. Build infrastructure for related industries such as semiconductors, encrypted networks, satellite systems and sustainable energy. Promote initiatives like Innovations for Defence Excellence and Ran Samwad to drive cognitive war games and disruptive technology innovation.

Explore Novel Applications in the Domain. Exploring CW requires the intelligent application of smart power, blending soft and hard power strategies. Cultural influence must complement kinetic readiness. Future planning should anticipate advances in biometric targeting, neurotechnologies, and metaverse operations. Cognitive Warfare will increasingly involve neuromorphic systems, neural interfaces, advanced neuromodulation, and humanoids that integrate human and machine cognition. Having studied the challenges and the whole-of-nation approach required to implement CW, Table 1 presents a suggested practical way forward across various CW segments.

Segments Usable in CW	**Levels of CW**		
-	**Strategic**	**Operational**	**Tactical**
Influence Ops	Ministry of External Affairs, Tourism Ministry, Ministry of Finance	Embassies, United Nations, Intergovernmental organisations	Armed Forces, Paramilitary, Police, Journalists, Content Creators, Social Media Influencers, Veterans, Diaspora, Tourists, Legal cell, Defence Public Sector Undertakings (DPSUs), Public-Funded Research Institutions, large corporates, Small and Medium Enterprises (MSMEs), Start-ups, Academia, Think Tanks, Non-State Actors, Civil Society Groups, and Expats.
Information Ops	Information and Broadcast Ministry, Ministry of Home Affairs	All Intelligence Agencies, Own media in foreign vernacular, social media	
Psychological Ops	Ministry of Defence	Defence Institute of Psychological Research, Indian Psychological Association	
Cyber Ops	Ministry of Electronics and Information Technology, Ministry of Science and Technology	Computer Emergency Response Team, Defence Cyber Agency, Department of Scientific and Industrial Research	
Space Ops	Indian Space Research Organisation	Defence Space Agency	
Legal	Supreme Court of India	High Courts (CW Tribunal*)	

Segments Usable in CW	**Levels of CW**		
-	**Strategic**	**Operational**	**Tactical**
Neuro Science	Ministry of Health and Family Welfare	Central Drugs Standard Control Organisation (Directorate General of Health Services), National Institute of Mental Health and Neurosciences	
Note: All segments must operate with balanced independence and interdependence, employed in land, sea, air, cyber, and space domains synchronously through an integrated command and control, with tactical elements interoperable across segments. All three pillars of CW outlined in the essay must be addressed at every level. The military should have access to any segment as required, under the aegis of JDCW. (* is put for the organisations that need to be constituted from existing resources).			

Table 1: Way forward to use various segments of CW
Source: Compiled by the author

Conclusion

CW cannot be viewed only through the prevailing distinct prisms of psychological, information and cyber operations. Future war complexities will require multi-domain approaches, where CW arguably disrupts the other five domains of warfare. Harnessed effectively, it can drive India toward becoming a Vishwa Guru (global leader) on the *Viksit Bharat* (Developed India) pathway. Our philosophy of *Vasudhaiva Kutumbakam* (The world is one family) shall permit our cognitive expertise to safeguard both global interests and national aspirations. India's ethos supports a defensive cognitive shield promoting a free and transparent world order. Adversaries

resistant to global equality require innovative cognitive traps leveraging emerging technologies. The National Cognitive Warfare Strategy will guide a balanced defensive and offensive posture with clear red lines, enabling precise and calculated responses. Through the 'One for All, All for One, India for All' strategy, India seeks to foster a global collective consciousness for worldwide benefit.

Endnotes

1 "The Global State of Digital 2022: Top Takeaways", *Hootsuite, 2022,* accessed 15 Aug 2025, https://www.ttuhsc.edu/communications-marketing/documents/downloads/Hootsuite-Digital-2022.pdf

2 Christoph Deppe and Gary S. Schaal, "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept", *Frontiers in Big Data* 7 (2024), accessed 15 Aug 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/#B9

3 Paul Thagard, "Cognitive Science", *Stanford Encyclopedia of Philosophy*, substantive revision 31 Jan 2023, accessed 15 Aug 2025, https://plato.stanford.edu/entries/cognitive-science/

4 Robert Frodeman, ed., *The Oxford Handbook of Interdisciplinarity*, 2nd ed. (Oxford: Oxford University Press, 2017).

5 Bernard Claverie, Baptiste Prébot, Norbou Buchler, and François du Cluzel, eds., *Cognitive Warfare: The Future of Cognitive Dominance* (Neuilly-sur-Seine: NATO Collaboration Support Office, Mar 2022), ISBN 978-92-837-2392-9, accessed 16 Aug 2025, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf

6 Yvonne R. Masakowski, "Newport Lecture Series: 'Artificial Intelligence & Cognitive Warfare'", *Naval War College Foundation, YouTube video*, 11 Apr 2022, accessed Aug 2025, https://youtu.be/6Ev8eNR5k4w16

7 Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, "Fall 2020 Cognitive Warfare: An Attack on Truth and Thought" (*Baltimore, MD: NATO Innovation Hub and Johns Hopkins* University, 2020), accessed Aug 2025, https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

8 Fabio Ibrahim, Steffen Rhode, and Monika Daseking, “A Systematic Review of Cognitive and Psychological Warfare”, *The Defence Horizon Journal* (Dec 2023), DOI: 10.5281/zenodo.10205600, accessed 17 Aug 2025, https://doi.org/10.5281/zenodo.10205600

9 Tzu-Chieh Hung and Tzu-Wei Hung, “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” *Journal of Global Security Studies* 7, no. 4 (Dec 2022): ogac016, accessed 17 Aug 2025, https://doi.org/10.1093/jogss/ogac016

10 Sandra Pereira, “NATO Study on the ‘Weaponisation of Brain Sciences’ for the Purposes of ‘Cognitive Warfare’”, *European Parliament, Parliamentary Question* E-001093/2022, 16 Mar 2022, accessed 17 Aug 2025, https://www.europarl.europa.eu/doceo/document/E-9-2022-001093_EN.html

11 Rear Admiral John W Tammen, “NATO’s Warfighting Capstone Concept: Anticipating the Changing Character of War”, *NATO Review*, 09 Jul 2021, accessed 17 Aug 2025, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html

12 Ibid.

13 Ibid.

14 Nataliya Bugayova and Kateryna Stepanenko, “A Primer on Russian Cognitive Warfare”, *Institute for the Study of War*, 30 Jun 2025, accessed 17 Aug 2025, https://www.understandingwar.org/backgrounder/primer-russian-cognitive-warfare

15 John Merriam, “One Move Ahead—Diagnosing and Countering Russian Reflexive Control”, *The Journal of Slavic Military Studies* 36, no. 1 (2023): 1–27, DOI: 10.1080/13518046.2023.2201113, accessed 18 Aug 2025, https://doi.org/10.1080/13518046.2023.2201113

16 Andrew S Bowen, *Russian Military Intelligence: Background and Issues for Congress*, Congressional Research Service Report R46616, 24 Nov 2020, accessed 18 Aug 2025, https://www.congress.gov/crs_external_products/R/PDF/R46616/R46616.6.pdf

17 Oliver Backes and Andrew Swab, "Cognitive Warfare—The Russian Threat to Election Integrity in the Baltic States", Policy Analysis Exercise, Belfer Center for Science and International Affairs, Harvard Kennedy School, Nov 2019, accessed 18 Aug 2025, https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

18 Alexis von Sydow, "China's Foreign Election Interference: An Overview of Its Global Impact", *Swedish National China Centre Brief*, no. 4 (2024), accessed 18 Aug 2025, https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/chinas-foreign-election-interference-an-overview-of-its-global-impact.pdf

19 Hanbyeol Sohn and Changwoo Kang, "North Korea's Nuclear-Cognitive Warfare Strategy", *38 North*, 10 Apr 2025, accessed 19 Aug 2025, https://www.38north.org/2025/04/north-koreas-nuclear-cognitive-warfare-strategy/

20 Aviram Bellaishe, "Iran's 'Cognitive War' Is More Dangerous than Missiles and Killer Drones", *Jerusalem Center for Security and Foreign Affairs*, 26 May 2024, accessed 19 Aug 2025, https://jcfa.org/article/irans-cognitive-war-is-more-dangerous-than-missiles-and-killer-drones/

21 Paweł Behrendt, "San Zhong Zhanfa or Three Warfares: Chinese Hybrid Warfare", *Boym Institute*, 19 Apr 2022, accessed 19 Aug 2025, https://instytutboyma.org/en/san-zhong-zhanfa-or-three-warfares-chinese-hybrid-warfare/

22 Pradip R. Sagar, "Weapons of Mass Dissemination: The India-Pakistan Cyber Frontier", *India Today Insight*, 18 May 2025, accessed 19 Aug 2025, https://www.indiatoday.in/india-today-insight/story/weapons-of-mass-dissemination-the-india-pakistan-cyber-frontier-2726677-2025-05-18

23 "Pakistan Ran a Coordinated Anti-India Campaign During Op Sindoor, Forensic Analysis Finds", *The New Indian Express*, 08 Jul 2025, accessed 19 Aug 2025, https://www.newindianexpress.com/nation/2025/Jul/08/pakistan-ran-coordinated-anti-india-campaign-during-op-sindoor-forensic-analysis-finds

24 Sabrina Gabel, Lilian Reichert, and Christian Reuter, "Discussing Conflict in Social Media: The Use of Twitter in the Jammu and Kashmir Conflict", *Media, War & Conflict* 15, no. 4 (Dec 2022): 504–529, DOI: 10.1177/1750635220970997, accessed 19 Aug 2025, https://journals.sagepub.com/doi/pdf/10.1177/1750635220970997

25 Lewis Regenstein, “Havana Syndrome: The History Behind the Mystery”, *Foreign Policy Research Institute*, 01 Apr 2024, accessed 19 Aug 2025, https://www.fpri.org/article/2024/04/havana-syndrome-the-history-behind-the-mystery/

26 Dr. Punit Kumar, “Saam, Daam, Dand, Bheda: The Pillars of Indian Diplomacy from Arthashastra to Modern Times”, *Organiser*, 18 May 2025, accessed 19 Aug 2025, https://organiser.org/2025/05/18/291978/bharat/saam-daam-dand-bheda-the-pillars-of-indian-diplomacy-from-arthashastra-to-modern-times/

27 Col. Denis M. Drew and Dr. Donald M. Snow, *Making Strategy: An Introduction to National Security Processes and Problems* (Maxwell Air Force Base, AL: Air University Press, Aug 1988).

28 IAF Chief Proposes Joint Planning, Coordination Centre in Delhi, *The Hindu*, 27 Aug 2025, accessed 28 Aug 2025, https://www.thehindu.com/news/national/iaf-chief-proposes-joint-planning-coordination-centre-in-delhi/article69980913.ece

29 Committee on External Affairs, “India’s Soft Power and Cultural Diplomacy: Prospects & Limitations”, Sixteenth Report, Seventeenth Lok Sabha (New Delhi: Lok Sabha Secretariat, Dec 2022), accessed 20 Aug 2025, https://elibrary.sansad.in/server/api/core/bitstreams/b1effdb6-685d-4436-a5d5-f9fe331ad30f/view

30 Torvald F Ask, Ricardo G Lugo, Stefan Sütterlin, Matthew Canham, Daniel Hermansen, and Benjamin J Knox, “The UnCODE System: A Neurocentric Systems Approach for Classifying the Goals and Methods of Cognitive Warfare”, paper presented at the HFM-361 Symposium on *Mitigating and Responding to Cognitive Warfare*, Madrid, Spain, Nov 2023, accessed 20 Aug 2025, https://hal.science/hal-04945655/document

31 Protium, “Key Challenges for MSMEs: Compliance, Technology, and Skilling Gaps”, 20 Jun 2025, accessed 20 Aug 2025, https://protium.co.in/key-challenges-for-msmes-compliance-technology-and-skilling-gaps/

32 “The Bharatiya Nyaya Sanhita, 2023”, Act No. 45 of 2023 (New Delhi: Government of India, 2023), accessed 20 Aug 2025, https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nyaya_Sanhita,_2023.pdf

33 Regina E Dugan and Kaigham J Gabriel, “Special Forces” Innovation: How DARPA Attacks Problems,” *Harvard Business Review* 91, no. 10 (Oct

2013): 74–84, accessed 20 Aug 2025, https://hbr.org/2013/10/special-forces-innovation-how-darpa-attacks-problems

From the Archives

The Journal
OF THE
United Service Institution of India.
VOL. XXVIII 1898. NO. 131.

NOTES ON HILL WARFARE

BY LIEUTENANT COLONEL J A H POLLOCK, 1st SIKH INFANTRY.

There is a want in the Service of some work on Hill Warfare. The Infantry Drill Book scarcely mentions it, and I know of no work which has yet been written on the subject with reference to fighting with frontier tribes, who, most of them, are accustomed to fighting from their youth upwards; who are surrounded with enemies, and who are excellent shots and the finest material for light infantry in the world; whose knowledge of hill tactics is excellent, who see faults and know how to take advantage of them, and from whom we have much to learn.

Having spent over twenty years on the frontier, more or less in contact with these tribes, I think the following rough notes may be of interest to some readers, as showing the lines on which most of the frontier regiments are trained to meet these tribes.

Advance-guards. —This is probably the simplest part of frontier warfare. As a rule, attacks are not made on advance-guards, except when a very strong position is held in force, but on the baggage or rear-guard; still, with an enterprising hill enemy, it never does to be careless, and all work should be thoroughly and carefully done.

An advance-guard may be told off as on a plain, except that groups are better than an extended line, as they are more under control, and single men, in jungle or rough ground, are liable to be lost if wounded.

Flanking parties are always necessary, but in the hills cannot move along with the column, so have to remain where they are placed, fresh parties being sent up as the column advances.

With a brigade or larger force, the advance-guard and flankers might be given from different regiments, and I think should move off about an hour before the main body marches. This allows of the troops moving quicker, as the road is already piquetted for them, and also probably saves loss of lives; as, with careful piquetting, the line of march should be fairly out of range of the enemy. In enclosed country it is necessary to increase the number of connecting files; no party or file should lose touch of that behind it. It should continually look round and see if it is there, and, if not, halt till it appears again.

On arriving in camp, the advance-guard should at once place the day piquets, which should be far enough out to prevent the camp being fired into.

Flank piquets. —These, in the hills, are a most important detail, and are not, as a rule, thoroughly understood.

With an enterprising enemy the piquets must be strong, and also be in such positions that an enemy cannot approach the line of march without coming under their fire.

The ground beyond the piquets should be in view, so that the enemy can collect in numbers without their knowledge.

It is better, with a strong enemy, to leave supports along the line of march, especially at places like the mouths of nullahs; where they are likely to try and rush the convoy or rear-guard.

Piquet sentries should not stand up or walk about. Their object is to see the enemy, not to be seen by him.

On moving up hill to their places, piquets must not straggle; they should keep together and fix bayonets, or they may move up in extended order and close as they get near the top. It is better than to send one or two men forward to spy out the country. Don't march on to the skyline; it only gives the enemy a magnificent target just when the men are to out of breath too shoot straight. On the way up make a note

of the quickest and easiest way down, and, if possible, select one which will be under cover.

Piquets must be especially careful after the main body has passed. Frontier tribes don't want to fight a big force which they know can beat them, but they want rifles and loot, and these can be obtained from the baggage or rear guard.

The piquets must, on no account, come down till the rear of the rear-guard is level with them.

When they retire, they should leave a few active men to cover their retirement till they are well down the hill, when the party left should follow rapidly.

It is a common thing for the whole piquet to stand up and turn about in retiring, which at once shows the enemy what is happening, with the result that the position is occupied at once, and a heavy fire brought to bear on the rear or baggage.

Piquets should always withdraw as quickly as possible, when once they commence to do so.

The position of the companies who are to furnish the flank piquet should, on the line of march, be as near the head of the advance guard as possible.

The piquet should always leave one man facing the line of march, as, in case of anything happening in that direction, he can warn the piquet.

Always give piquets orders when to come down. Rear guards are frequently delayed by them. I recollect on one occasion when the piquets were asked why they had not joined, the answer given was that they had received no orders to come down.

The flank piquets and rear guard are generally given by different regiments, and it is often useful to send a non-commissioned officer or officer (especially in wooded country), who knows where they are posted, with the rear-guard.

Convoys. —May be sent in one of two ways, either with a strong escort which marches the whole way with the convoy, or else each post sends out half-way escorts, piquetting the hills half way, and giving also an escort to keep the convoy from straggling.

One thing is absolutely necessary, and that is, that the flanks of a long convoy must be protected by carefully placed piquets.

Hence, in starting, the advance-guard must be much stronger than the rear-guard, as the rear is gradually strengthened by the flank piquets joining it.

Foraging parties. —As a rule, these parties do not go out more than four or five miles from camp. The road should first of all be strongly piquetted, and these piquets should remain out till the rear-guard returns. They should when possible, be far enough out to stop the convoy being fired.

The animals should have a special escort and be told off to certain fields or villages. The remainder of the force be so placed that an attack on the convoy cannot take place without serious loss to the enemy. The advance-guard should throw out piquets well to the front, and connect on both sides with the flanking piquets. As a rule, the advance-guard returning to camp is not attacked, but the rear or flanks are the points chosen. It is, therefore, necessary to see that these are strong enough to resist an attack.

In retiring, successive positions should be taken up, and the rear-guard allowed to pass through and take up a fresh position, if necessary. All nullahs must be carefully watched, as it is down these an enemy generally creeps before he makes his sudden rush.

Forces searching or destroying the defences of villages work on the same principle.

Keep these out till everything has been finished, and the troops formed up to march home.

Any good position on the road home should be held by fresh troops and the rear-guard allowed to pass through.

Nothing disconcerts hill tribes so much as to find a body of men in an unexpected position.

A sudden surprise, or an ambuscade, makes them very wary of following up troops.

Never lose touch of your rear-guard; halt the main body when it halts, and always be ready to move quickly to its assistance: in fact, consider your whole force as one large rear-guard.

Attack—Before I commence this, I wish one point to be remembered, as it is a very important one, and that is, that men carrying seventy rounds, a day's rations, and a full water-bottle tire quickly if over-marched. It is distinctly the pace that kills with them, and many officers forget that they themselves are not so heavily weighted, and should therefore accommodate their pace to that of their men. Never force the pace unless there is some good reason for it. Officers riding seldom realise that horses walk faster than soldiers. If men are pressed beyond their ordinary pace, they straggle, and it was to the fact that the commanding officer led the leading regiment too fast at the Barara Tangi in the first Waziristan Expedition, and so made them straggle out that the successful attack of the swordsmen was due.

Another reason for not pressing the men is that the extra weight makes them perspire freely, with the result that they catch chills and become quickly unfit for service. The more you look after your men's comfort, the more men you will have fit for duty. When they get warm clothing, see they wear it. It is curious how careless they are about this themselves.

In hill warfare the supports and reserves can be brought up much closer to the firing line than in the plains, and the less distance they have to go to reinforce the less breath they lose. In a large number of steep hills there are positions from which men advancing can be, to a certain extent, saved from the fire of the enemy by the supports and reserves firing over their heads. As each position is taken, the support should move up to the firing line and the reserve to the position of the support. The firing line again moves on under cover of the fire of the support. If three or four spurs are worked like this, with a cross fire kept up on

sangars to right and left, and artillery helping at the same time, an enemy can be turned out of a very strong position; but one thing should be recollected, that whereas in a plain supports and reserves cannot fire over the heads of the firing line, in the hills they can frequently do so with impunity. The author only give the above as a specimen of a hill fight.

Tribesmen are wonderful shots and shoot very straight; but the author has often noticed that as firing becomes more accurate, theirs becomes less so, and then gradually ceases. Always, when possible, outflank your enemy; he will often leave a formidable position with little loss there, as he fears he will lose heavily in retiring if he holds on to it.

Rear-guards. —This, as in civilised warfare, is the most difficult task troops can be given to perform, and requires troops carefully trained to do it successfully in the face of an enterprising enemy.

But in order that a rear-guard may perform its duties properly, its flanks must be protected as it retires, as it will have quite enough to do to look after its front.

Whenever possible, successive positions should be taken up, and the rear-guard should move through and re-form to the rear.

No straggling must be allowed, as this is certain to lead to men being cut up.

All baggage guards and followers must remain with their own baggage; the latter are the worst offenders in straggling, and nothing but the fear of the cane will stop them doing so.

The rear-guard must always be alert; they have sharp eyes watching them for a chance of attack, and the slightest carelessness will be noted and made use of.

In retiring after a reconnaissance, never let the main body get out of touch with the rear-guard. It always wants a position to fall back on if hard pressed, and frequently may want to be reinforced; hence the main body should remain within recall. Touch should be kept up by connecting files or small parties, who can quickly pass on information.

Most officers, when retiring, expect the rear-guard to keep up connection with and regulate its pace by the main body; on the contrary, the main body should move in accordance with its rear-guard, which may frequently be delayed by piquets not coming down quickly, or other circumstances under which it is not at all uncommon for the main body to march clean away from its rear-guard.

Piquets Day.—The comfort and safety of the troops in camp depends on the position of the piquets. It is far better that a small portion of the troops should be disturbed than that the whole camp should be worried.

As arms of precision get into the hands of the frontier tribes, who are good judges of distance and excellent marksmen, it becomes necessary to place piquets further out from camp and in such positions that the men shall not be continually disturbed by sniping.

This point is not sufficiently recognised, and yet it is a very important one.

The further the piquets are out, the stronger they must be; but in a good sangar, with a ditch and abatis, a piquet of from twenty to fifty rifles can hold its own for a long time.

Night. —It is better, when possible, to hold the same piquets by night as by day. If this cannot be done, the night piquets should mount before the day ones come in, so that they can cover their retirement into camp.

All nullahs by which an enemy can approach should be watched. This is often done best by sending a strong party out after dark in order to surprise them coming down. This, if successful, has more effect than ordinary piquets have, as they are afraid other parties may be out watching for them, and one or two carefully worked "chapaos" often practically stop sniping at night.

Piquets must never pile arms, but men should keep their rifles by their side day and night; they are then ready for any attack.

In fact, except in camp, or when absolutely necessary, as at road-making, etc, I do not think rifles should ever be piled. When men fall out, they should keep their rifles in their hands.

Miscellaneous.

Never allow any strangers to sit down or mix with guards, escorts or piquets, or come near them on the march.

I have known cases when this has been done, and the whole guard killed, and the rifles, etc, made off with. All escorts should always send a point in front; it may save their lives.

In the Gomal, a few years ago, a whole escort was shot from a side nullah; this could not have happened if one or two men had been a hundred yards in front.

In advancing uphill in extended order against an enemy, who is given to charge downhill, it is generally best to close in to the centre nearing the crest, as the men are then in a better position to stand a charge.

Always go at a steady pace uphill, and stop now and then to reform the line: some men walk slower than others, and it is better to wait for these to come up than to attack in a straggling loose formation.

The action at the Barara Tangi in Waziristan is an instance of the harm done by the latter formation.

In 1881, after clearing some low hills at Shah Alam Kaghza, the 1st Sikhs advanced up a spur covered with oak jungle, so thick that it was difficult to see more than ten yards off. About half-way up they halted, and the two front companies were ordered to lie down, fix bayonets, and load. Suddenly a charge was made on them, the enemy appearing about ten yards off. The fire they received sent them back, but the officer, instead of allowing his men to get out of hand, pursued them steadily up the hill, halting to re-form every now and then. This was a wise precaution, as, if the men had got out of hand and rushed up the hill, a rush of Waziris might have swept through them. As it was at each halt the Waziris tried to rush the companies, but did not succeed. I was

then the junior subaltern in the regiment. After the charge we heard the General's bugler sounding our regimental call and the retire.

Colonel Rice, who was a very able officer and quite understood the situation, refused to obey the order, as he was aware that if we retired through that thick scrub before the Waziris were beaten, the result would have been a heavy loss in men, so, instead, he drove them over the range, and we halted for some time and then retired without a shot being fired at us. That was the last stand the Waziris made.

They had made up their minds to attack us that night, and they certainly had an excellent position to rush; but a piquet of thirty men, placed well to the front after dark, fired into them heavily, and this, taken with the beating they received during the day, had the effect of stopping the rush.

When retiring over unknown ground, especially in the hills, always send intelligent men back to find out the paths leading to the rear.

Some years ago, in retiring from the crest of the Kohat Pass, a body of men, not knowing the way, moved straight down the hill. The Afridis saw their mistake at once and pressed them back onto the precipice below them, and I think about forty men were shot or fell over it, I remember General McQueen telling us how the recollection of this had once helped him in a similar position.

It was in the Jowaki Expedition, in 1877, he was commanding the 5th Punjab Infantry, and was acting as rear-guard to the force as it retired off the heights above Ghariba. The hills were very precipitous, so he sent some intelligent men back and found out the different roads down. He then gradually moved the regiment down, and kept a few active men above till the bad ground was passed; he then took up another position, and the last men ran quickly down the hill under cover of the fire of the men posted below.

As far as possible, leave a position quietly, and, if possible, unobserved, take up a fresh position in rear, then at the last let the few men left clear out quickly. General Hammond's defence at the Asmai Heights in the last Afghan War, when left as rear-guard with I think only

a company of the Guides, is an excellent instance of how this should be done. He gradually sent all his men down till he had about twelve left, and they held the hill till the enemy were nearly on them, and then quickly retired. It was on this occasion that he gained his V.C. Always outflank your enemy, even if it is only with a few men. I recollect once an enemy, in a very strong position, stopping a frontal attack entirely, but leaving the position suddenly, because a naik and six sepoys managed to crawl up a steep place and from the top enfiladed them.

Never allow men or followers to straggle. When a man falls out for any purpose, always leave a comrade to look after him. At every halt put out small piquets. On one occasion the non-observance of this led to three men being knocked over from a nullah quite close to the force in the Jowaki Expedition in 1877.

An enterprising enemy is always on the look-out, and takes full advantage of any carelessness or mistake on your part.

Always fortify your camp and piquet posts, and have alarm posts told off. Even a wall two feet high is useful, as it shows men where to fall in, and gives a certain amount of cover, though it may not stop a rush. Always warn the men to fire low at night. If an attack on camp is expected, it is, I think, a good plan to strike tents at the first shot. There is then less mark for the enemy to fire at, and more room for the men to move about in. If you can afford tents for night piquets, and have those with dark lining, turn them inside out; they then are difficult to see at night.

Sir P. Palmer once gave me the following advice, the result, I believe, of a bad half hour in a fort in Burma: — "Allow no man to leave his alarm post without orders, even if other parts of your position are hard pressed, as the enemy can then enter at the place left unguarded. If the enemy get into the position, don't fire on them; you do more damage to your own men, besides demoralising them; turn them out with the bayonet."

An instance of how patient hillmen are when raiding once came under my notice at Kujari Kach in the Gumal. It was told by one of the party of Mahsud Waziris engaged in the attempt to steal the rifles of the

cavalry grass-cut piquet there. The cavalry grass-cuts used to go out daily under escort to cut grass. The escort used to furnish a piquet on some convenient spot, and it was the intention of the Waziris to rush this piquet if they could manage it.

They watched for three weeks, and at last saw what appeared to be their chance; the sentry was sitting down with his carbine across his knees, and apparently asleep. They got ready for their rush from a nullah they were in about eighty yards away, when the sentry raised his head. Then, in disgust, they gave it up and went back to their country: but men who have such patience are dangerous enemies, as they seldom attack rashly.

It is better, when possible, when you have to return to camp, not to go so far as to be obliged to return after dark. Your knowledge of the country is small compared with that of your enemies, and they know all the best places to ambuscade you at. If hardly pressed, it is often better to halt for the night in some strong position, and return to camp the next morning.

Learn, if you can, every path and road round your camp; they lead somewhere and may be useful to you later on. Never despise your enemy, and always be ready to learn something from him.

Take every opportunity of exercising your men in firing at unknown distances: nothing trains men for war so much as that practice in peace. Shooting on the range is excellent in its way; but a hillman is not a white target with a black bull's-eye, nor does he even at 800 yards show even a mark as large as a third class target.

I think the following two quotations should be borne in mind and acted on: —

"There is a general principle which I have laid down for" the regulation of the officers' conduct under my command, "which is, never to break the neutrality of any place, but never" to consider as neutral any place from whence an attack is "made, it is certainly justifiable to attack any vessel in a place from whence she makes an attack."— *Mahan's Life of Nelson.* (For "vessel" read "man" or "tribe".)

"My system is to strike hard and keep on hitting till" resistance is completely over; then at once to form ranks, cease slaughter, and be kind and humane to the "prostrate enemy."—*Skobeleff*.

One important point is to learn the signs which show the presence or absence of an enemy.

For instance, if the women and children are in the villages, the men will not fight. If the villages are empty, then they are ready for war.

A few snipers generally mean only a few enemies about. One of the well known signs of trouble with the Afridis in Kohat is the sudden stoppage of the salt trade between Bahadur Khel and the Kohat Pass.

Marching at night requires very careful training: no officer who has not actually marched on foot with infantry realises the difficulty that the rear of the column has in keeping up, especially over bad ground or in single file. Two and a half miles an hour seems slow when you are marching at the head, but go to the rear of the column, and you will probably find them doubling. The best plan is to make the head of each company go its own pace and halt frequently; the men then come up by companies without unnecessary doubling.

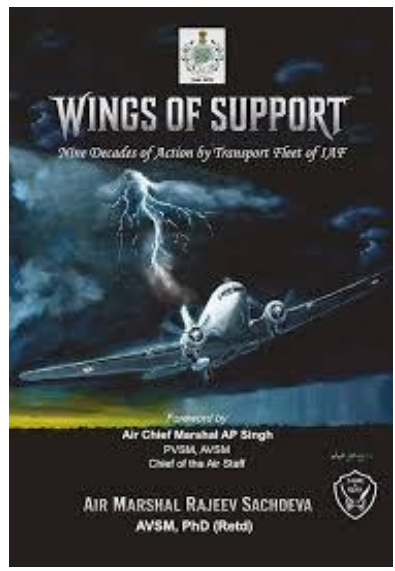
Train your men in peace to the manoeuvres they will have to perform in war. Forms of attack are very good in their way, but they won't do against hill enemies, who are off directly you mean business; and as they are the enemies we usually have to meet, it is worthwhile learning hill tactics beforehand. Don't let a man approach you with his face swathed in his *pagri*. It is frequently a sign that the man means to kill someone.

Review Articles

Review Article 1

Wings of Support: Nine Decades of Action by the Transport Fleet of the IAF

Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd)



Introduction

Histories of military aviation generally focus on fighter aircraft, aerial combat and precision strikes, while transport aviation is treated mainly as a supporting activity. In *Wings of Support*, Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd), addresses this imbalance by documenting the evolution and contribution of the Indian Air Force's transport fleet. The book demonstrates how air mobility has influenced military campaigns, territorial consolidation, humanitarian assistance, strategic outreach and nation-building. Its six chapters combine institutional history, operational narratives, personal

---

Wings of Support by Air Marshal Rajeev Sachdeva, AVSM, PhD (Retd), pages – 450, Price ₹ 2,499, Sabre and Quill, ISBN978-81-690-3858-4

accounts, technological developments and an assessment of India's future air mobility requirements.

Chapter One: Evolution of the Indian Air Force and Maturation of Its Transport Fleet

The first chapter establishes the historical and institutional foundations of Indian military transport aviation. It begins with the development of human flight, examines aviation's transformation during the two world wars, and traces the emergence of military aviation in India. The narrative then moves to the establishment of the Indian Air Force and the raising of No. 12 Squadron in 1946 as its first transport squadron.

A particular strength of the chapter is its explanation of the relationship between geography and air mobility. India's mountainous frontiers, extensive landmass, island territories and inadequate surface communications in remote areas created an enduring requirement for military air transport. The author effectively shows that the transport fleet did not emerge merely as a logistical convenience; it developed in response to fundamental operational and geographical imperatives.

The chapter also outlines the fleet's varied responsibilities, operational risks and progressive capability development. This provides readers with the background required to appreciate the missions discussed later in the book. Its broad historical coverage gives the chapter an encyclopaedic quality. Stronger analytical connections between technological development, organisational change and operational doctrine could further enrich a future edition. Nevertheless, the chapter establishes the transport fleet as an essential component of Indian air power.

Chapter Two: Operations That Changed Indian History

The second chapter serves as the book's operational centrepiece. It examines missions in which transport aircraft directly influenced military and political outcomes. Key examples include the Oct 1947 airlift to Srinagar, the aerial sustenance of Poonch, the pioneering Dakota landing at Leh, Operation Polo, the liberation of Goa,

transport operations during the 1962 and 1965 wars, the Tangail airborne assault in 1971, and Operation Cactus in the Maldives.

The discussion of Srinagar airlift is particularly significant. The rapid movement of Indian troops helped prevent the loss of the Kashmir Valley and demonstrated the strategic value of timely air mobility. Similarly, operations at Poonch and Leh show how transport aircraft enabled India to reinforce and sustain isolated positions despite formidable terrain and inadequate road communications.

The Tangail airborne assault illustrates the transport fleet's contribution to joint planning and operational manoeuvre. The use of multiple aircraft types to deliver paratroopers behind Pakistani positions contributed to the momentum of the Indian campaign in East Pakistan. Operation Cactus presents a different dimension of air mobility: the rapid projection of military power in support of a friendly neighbouring government.

The chapter's principal achievement lies in dispelling the perception of transport aviation as merely a passive supporting capability. It demonstrates that air transport can influence the tempo, reach and outcome of military operations. Greater differentiation among tactical success, operational effect and strategic outcome could strengthen the analysis further, particularly where transport operations formed part of larger joint campaigns. Even so, the range and detail of the operational accounts make this one of the book's most valuable chapters.

Chapter Three: Contributions Towards Nation-Building

The third chapter broadens the discussion from military operations to the transport fleet's contribution to the nation. It covers disaster relief, civilian evacuation, medical assistance, connectivity to remote regions and the movement of essential supplies during emergencies.

The accounts of operations at Daulat Beg Oldie, Leh, Chushul, Thoise, Nyoma and Kargil are among the chapter's highlights. They demonstrate the exceptional demands of operating in the Himalayas, where rarefied air, unpredictable weather, restrictive terrain and limited infrastructure leave little margin for error. The author conveys that these missions depended not only on aircraft performance but

also on professional skill, improvisation, teamwork, and calculated risk-taking.

The chapter also documents relief operations following the Assam and Bhuj earthquakes, the Kerala floods and numerous other natural disasters. Its coverage of evacuations from Kuwait, Libya, Yemen, Afghanistan, Ukraine, Sudan, Israel and other crisis zones highlights the growing international responsibilities of the Indian state. As India's global presence has expanded, the ability to rescue citizens and deliver humanitarian assistance abroad has become an important element of national power.

The chapter stands out for its range and human appeal. It demonstrates that the transport fleet's importance cannot be measured solely through combat missions. Its contribution to national resilience, diplomacy and humanitarian assistance is equally significant. The numerous operational episodes occasionally produce a catalogue-like effect, but collectively they provide an important record of service that might otherwise remain dispersed across institutional archives.

Chapter Four: Sky Sovereigns—The Unsung

The fourth chapter shifts the focus from operations to the people and aircraft that made them possible. Through biographical sketches, the author records the contributions of pioneering aviators and transport personnel whose achievements have not always received adequate public recognition.

Figures such as Group Captain Karori Lal Bhatia and Air Vice Marshal Harjinder Singh give the institutional history a human face. The chapter also pays tribute to aircraft such as the Dakota, Caribou, Avro HS-748, Otter, Devon, C-119G Packet and An-12B. These platforms are presented not merely through their technical specifications but also through their operational employment, reliability and association with historic missions.

The Dakota emerges as a particularly significant aircraft. Its contribution to the defence of Kashmir, airborne operations, humanitarian assistance and territorial integration establishes it as

one of the most consequential aircraft in India's post-independence history.

The chapter makes a valuable archival contribution by bringing together personal accounts, professional achievements and aircraft histories. It also reminds readers that transport operations are collective undertakings involving aircrew, engineers, technicians, loadmasters, ground handlers and numerous support organisations. A more standardised structure for the biographical sketches and aircraft profiles could improve consistency, but the chapter's commemorative purpose is both justified and effectively realised.

Chapter Five: *Atmanirbharta* in Transport Aircraft

The fifth chapter examines India's pursuit of self-reliance in aircraft manufacturing. Beginning with Walchand Hirachand and the establishment of Hindustan Aircraft Limited, it traces the development of India's aerospace industrial capability. The chapter covers the Avro HS-748, Dornier 228, Saras programme, indigenous airborne warning and control initiatives, and the C-295MW manufacturing programme.

One of the chapter's strengths is its treatment of *Atmanirbharta* as a strategic requirement rather than merely an industrial aspiration. Transport aircraft fleets remain in service for several decades and require dependable access to spares, maintenance facilities, upgrades and technical expertise. Excessive dependence on foreign manufacturers can therefore create long-term operational vulnerabilities.

The discussion of the C-295 programme is especially relevant because it represents an important expansion of private-sector participation in military aircraft manufacturing. The programme may help develop domestic supply chains, specialised skills and a broader aerospace ecosystem.

The chapter also recognises that genuine self-reliance requires more than licensed production. Indigenous design, certification, engine development, avionics integration and life-cycle support demand sustained investment and institutional cooperation. A deeper comparative assessment of successful programmes and delayed or incomplete projects could provide additional policy lessons.

Nevertheless, the chapter makes a persuasive case for treating aerospace manufacturing as an important component of national security.

Chapter Six: Envisioning the Transport Fleet of *Viksit Bharat* in 2047

The sixth chapter moves from historical assessment to strategic foresight. It considers the air mobility capability India may require by 2047 in light of its anticipated economic growth, expanding global interests and evolving security environment.

The author examines requirements for strategic and tactical airlift, humanitarian assistance, casualty evacuation, special operations, overseas deployments and joint operations under theatre commands. The chapter appropriately emphasises that future transport aircraft will often operate in contested environments. Their effectiveness will depend on intelligence, electronic warfare, fighter protection, suppression of enemy air defences, secure communications and survivable command-and-control arrangements.

A distinctive feature is the use of a quantitative framework to estimate future fleet requirements. By considering payload, aircraft availability, mission categories and logistics allocation, the author attempts to move beyond general prescriptions. This provides a useful starting point for professional discussion, although the model would benefit from regular updating as operational assumptions, technologies and force structures evolve.

The proposed framework for an IAF Air Mobility Doctrine is another important contribution. It covers force structure, operational concepts, technological integration, infrastructure, training, international cooperation, resources and risk mitigation. The chapter correctly argues that aircraft acquisition alone cannot create an effective air mobility capability; doctrine, infrastructure, personnel, joint planning and industrial support are equally important.

This forward-looking chapter gives the book contemporary policy relevance. It connects the accumulated lessons of nine decades with the future requirements of Indian air power and

presents transport aviation as a cornerstone of India's aspirations for regional and global influence.

Epilogue

The epilogue brings together the book's principal themes. It traces the fleet's progression from approximately 30 tonnes of airlift capacity at independence to more than 3,000 tonnes per mission today. It revisits historic operations in Srinagar, Poonch, Leh, Tangail, and the Maldives while highlighting the increased range, payload, responsiveness, and survivability of modern aircraft.

The epilogue reinforces the author's central argument: the transport fleet has evolved from a small collection of relatively limited aircraft into a strategic capability that supports military operations, humanitarian assistance, regional engagement and global outreach. It also acknowledges emerging threats to large transport aircraft and the need for force protection in contested airspace.

Overall Assessment

Wings of Support is a comprehensive, authoritative and richly documented account of the IAF's transport fleet. Its principal achievement lies in bringing an often-overlooked component of air power to the forefront of India's military history. The book combines operational narratives, personal accounts, aircraft histories, industrial development and strategic foresight in a single volume.

The work stands out for its breadth, professional insight, and archival value. Its extensive collection of mission accounts and individual experiences will be useful to military professionals, scholars, policymakers and aviation enthusiasts. A consolidated bibliography, additional operational maps, comparative fleet tables and further editorial standardisation could enhance a future edition.

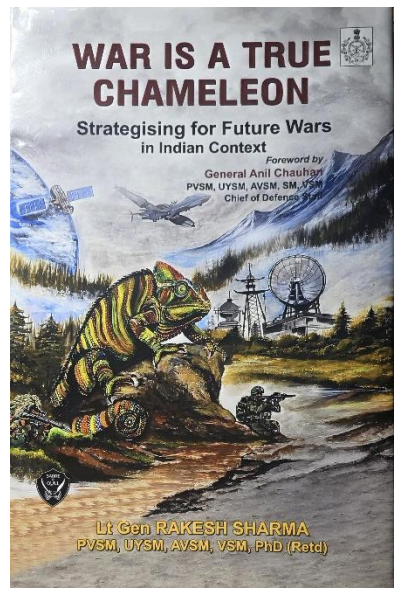
Above all, the book demonstrates that transport aviation is not merely a supporting capability. By enabling the timely movement of forces, sustaining remote positions, assisting citizens during emergencies and extending India's reach abroad, the IAF's transport fleet constitutes a vital instrument of national power.

Major General Sanjeev Chowdhry (Retd)

Review Article 2

War Is a True Chameleon: Strategising for Future Wars in the Indian Context

Lieutenant General Rakesh Sharma,
PVSM, UYSM, AVSM, VSM, PhD (Retd)



A book's cover often provides the first clue to its contents. The striking cover of *WAR IS A TRUE CHAMELEON: Strategising for Future Wars in the Indian Context*, featuring a chameleon against a military backdrop, immediately arouses curiosity. What possible connection could this remarkable reptile have with the future of warfare?

War Is a True Chameleon: Strategising for Future Wars in the Indian Context by Lieutenant General Rakesh Sharma, PVSM, UYSM, AVSM, VSM, PhD (Retd), Pages – 341, Price - ₹ 999/-, ISBN 978-81-690-3827-0

My first thought was the familiar Indian idiom, ‘Changing colours like a chameleon’. The answer, however, lies in one of the most enduring observations in military thought. Nearly two centuries ago, the Prussian strategist Carl von Clausewitz observed in *On War* that "War is more than a true chameleon”. While war remains constant as an instrument of political purpose, its character continually evolves in response to changing political objectives, technological innovation, social conditions, and the strategic environment.

That insight is more relevant than ever. Contemporary conflicts in Eastern Europe and the Middle East show that although war remains shaped by violence, uncertainty, friction, and human will, precision-guided munitions, artificial intelligence, autonomous systems, cyber operations, electronic warfare, satellite intelligence, and information campaigns have transformed how it is conducted. The chameleon on the cover thus becomes a powerful metaphor for the book's central thesis: victory in future wars will belong to those who adapt faster than their adversaries.

The book focuses on India's military strategy and defence preparedness for future warfare. It is divided into three sections:

Section 1: What is War? War is Peace; Peace is War!

Section 2: India Battlefield Singularity: Old Wars, New Wars

Section 3: Strategising for India

Section 1 examines the changing nature of warfare in the twenty-first century, in which conventional and unconventional conflicts increasingly overlap, often without large-scale troop deployments or formal declarations of war. Drawing on recent conflicts, including the US–Israel–Iran confrontation, the author explores whether future wars will increasingly be characterised by limited military action rather than prolonged campaigns. The section also discusses the emerging multipolar world order, the growing influence of the Global South, and the distinction between multipolarity and multilateralism. Institutions such as NATO, the European Union, Quad, BRICS, and the Shanghai Cooperation Organisation are examined as important instruments of multilateral cooperation in addressing global

challenges, including security, climate change, sustainable development, and human rights.

Section 2 shifts the focus to India's strategic geography and evolving security environment. It argues that India's defence planning must be based on an integrated understanding of the battlespace rather than on separate assessments of individual military domains. It pays particular attention to China's military rise, its strategic collusion with Pakistan, the possibility of a two-front conflict, and the implications of Operation Sindoor. As a recognised China watcher, General Sharma provides a detailed and well-informed assessment of these developments.

The author's philosophy is succinctly captured in his own words:

"The future in warfighting belongs to those who can see first, decide first, and strike first.... Understanding and defining future capabilities is absolutely crucial for Strategising, planning, and executing operations efficiently." This statement encapsulates the intellectual foundation upon which the entire work rests.

Gen Rakesh Sharma is uniquely qualified to write this book. A soldier, scholar, and strategic analyst, he has consistently contributed to India's military discourse through his research, lectures, and publications on national security, military transformation, and future warfare. His extensive operational experience, combined with academic rigour, enables him to bridge theory and practice with unusual effectiveness.

Supported by an insightful foreword by former Chief of Defence Staff General Anil Chauhan, himself a distinguished soldier-scholar, the book goes well beyond cataloguing emerging technologies. Instead, it examines how technology interacts with geopolitics, economics, doctrine, and national strategy to reshape the character of conflict. The result is a work that combines intellectual rigour with accessibility, making it valuable to military professionals, policymakers, researchers, and informed readers alike.

Clausewitz Still Matters

The book's intellectual foundation rests firmly on Clausewitz's distinction between the nature and the character of war—a distinction frequently overlooked in contemporary strategic literature. While the nature of war—its violence, uncertainty, political purpose, and human dimension—remains unchanged, its character continues to evolve under the influence of technology, economics, society, and statecraft. Clausewitz defined war as “An act of force to compel our enemy to do our will", while the Merriam-Webster Dictionary describes it as "A state of usually open and declared armed hostile conflict between states or nations".

Gen Sharma demonstrates convincingly that present-day conflicts have become laboratories for observing this evolution. Cheap drones destroy expensive tanks; commercial satellites provide tactical intelligence; cyber-attacks accompany missile strikes; electronic warfare disrupts communications; and information campaigns shape global opinion in real time.

Perhaps the book's most compelling observation is that modern conflict often occurs without a formal declaration of war: “No formal declaration of war is made”. Yet, the world is at war, echoing George Orwell's famous paradox, "War is Peace". This aptly captures the reality of contemporary strategic competition, where coercion increasingly occurs below the threshold of conventional war.

The Battlefield Has Expanded

One of the book's greatest strengths is its lucid explanation of how the battlefield has expanded beyond the traditional domains of land, sea, and air into space, cyberspace, the electromagnetic spectrum, and the cognitive domain.

Space has become indispensable for navigation, intelligence, and precision targeting. Cyberspace enables adversaries to disrupt critical infrastructure without firing a shot. Electronic warfare now contests the electromagnetic spectrum, while information operations seek to manipulate public opinion and political decision-making. Artificial intelligence is accelerating decision-making and enabling increasingly autonomous systems across multiple domains.

The book also provides an insightful discussion of grey-zone warfare, where cyber intrusions, economic coercion, legal warfare, technological denial, and influence operations enable states to achieve strategic objectives while remaining below the threshold of open conflict. The author further examines the full spectrum of contemporary hybrid warfare, including multi-domain operations, multidimensional warfare, network-centric operations, data-centric fusion, cyberspace operations, electromagnetic activities, cyber warfare, and the rapidly evolving role of drone warfare.

Technology Is Not Strategy

One of the book's most refreshing qualities is its rejection of technological determinism. Contemporary military literature often implies that acquiring advanced platforms automatically guarantees battlefield success. Gen Sharma firmly rejects this notion.

Technology, he argues, is an enabler—not a substitute—for sound strategy. Leadership, morale, logistics, doctrine, political clarity, and national resilience continue to determine outcomes because wars ultimately remain contests of human will.

His central argument deserves careful attention: “Superior strategy, combined with the successful integration of technology into an appropriate organisational structure and doctrine, leads to success in warfare.... It is always possible to defeat the best of technologies”. This observation restores strategy—not hardware—to its rightful place at the centre of military thought.

Accordingly, military capability should be developed through a top-down approach, beginning with strategy and doctrine based on future threats, politico-military objectives, and multi-domain operational requirements. Equipment and force structures must emerge from strategy, not the other way around. Within this framework, the author also relates defence preparedness to the broader national vision of Viksit Bharat 2047, emphasising the importance of indigenous defence manufacturing, technological self-reliance, innovation, and integrated national development.

India's Strategic Reality

हिमालय समारभ्य यावत् इन्दु सरोवरम्।

तं देवनिर्मितं देशं हिन्दुस्थानं प्रचक्षते॥

(From the Himalayas to the Indian Ocean stretches the land created by the Divine, known as Hindustan.) — Barhaspatiya Samhita

The author introduces this ancient verse to emphasise India's enduring civilisational identity, while cautioning readers against letting historical sentiment overshadow contemporary strategic realities.

For Indian readers, the book matters because it analyses future warfare through India's own strategic lens rather than merely adapting Western strategic concepts. India confronts one of the world's most complex security environments, characterised by two nuclear-armed adversaries, unsettled borders, persistent cross-border terrorism, maritime competition in the Indian Ocean Region, and an increasingly uncertain global order.

General Sharma argues that preparing for future wars requires far more than military modernisation. Indigenous defence manufacturing, technological self-reliance, research and development, civil-military integration, and strategic decision-making must evolve together within a coherent whole-of-government and whole-of-nation framework.

His analysis of China's military modernisation, its strategic collusion with Pakistan, hybrid warfare, maritime competition, and the prospect of a two-front contingency is particularly valuable. His long experience as a China watcher lends both authority and balance to this assessment.

The author also argues that India's defence preparedness should align with the broader national vision of Viksit Bharat 2047, in which economic growth, technological innovation, and strategic planning reinforce one another to strengthen national security.

Lessons from Contemporary Conflicts

Drawing extensively on the Russia–Ukraine War and recent conflicts in the Middle East, General Sharma demonstrates how drones, loitering munitions, cyber operations, electronic warfare, and commercial satellite intelligence have fundamentally altered military operations.

He rightly cautions against treating 'Drones' as a single capability. The term encompasses everything from inexpensive commercial quadcopters to sophisticated autonomous combat aircraft, each serving a distinct operational purpose and requiring different doctrinal responses.

Equally significant is the growing battle for narratives. Public opinion has become an operational domain in its own right, where information spreads instantaneously across digital platforms, influencing domestic morale, international diplomacy, and political legitimacy.

The book also examines the continuing relevance of mechanised warfare in the Indian context. Rather than accepting simplistic conclusions about the tank's demise, the author evaluates lessons from the Russia–Ukraine War and argues that armour remains relevant when employed within an integrated, multi-domain operational framework.

Jointness and National Preparedness

A recurring theme throughout the book is that future wars cannot be won through isolated military excellence. Success demands seamless integration among the armed forces, government, industry, academia, and society.

The author discusses India's ongoing reforms, including the proposed theatre commands and Integrated Battle Groups, arguing that organisational transformation is indispensable for future operational effectiveness. Jointness among the Army, Navy, and Air Force is no longer merely desirable—it has become an operational necessity.

General Sharma concludes that military capability must be developed through a top-down approach guided by strategy rather than a bottom-up approach driven by equipment upward. He advocates a top-down approach to multi-domain operations in which military capabilities become increasingly integrated and domain-agnostic through the effective fusion of civilian and military resources.

The book also highlights Prime Minister Narendra Modi's strategic mantra for defence preparedness—JAI: Jointness, Atmanirbharta (self-reliance), and Innovation—as a guiding framework for transforming India's defence ecosystem into a cohesive, self-reliant, and future-ready force.

The author further emphasises that a national strategic vision must be future-oriented, inclusive, and sufficiently robust to guide long-term planning, policy formulation, resource allocation, and national action. Such a vision provides coherence across institutions and aligns diverse stakeholders towards common national objectives.

Style and Presentation

Despite addressing highly complex strategic issues, the book remains remarkably accessible. Technical concepts are explained with clarity, the chapters are logically organised, and the arguments are supported by contemporary examples, historical references, and strategic insights.

Rather than prescribing rigid solutions, General Sharma encourages readers to question prevailing assumptions and think critically about India's future security challenges. This approach transforms the book from a descriptive account of modern warfare into an intellectual framework for strategic reflection.

Particularly memorable is his reminder: ‘Armies must not fight tomorrow's wars with yesterday's weapons’.

The message extends beyond military technology; it calls for continuous intellectual adaptation, institutional reform, and strategic foresight during peacetime.

War Is a True Chameleon: Strategising for Future Wars in the Indian Context is far more than a study of emerging military technologies. It is a comprehensive examination of the changing character of warfare and of how India must prepare intellectually, institutionally, and strategically for an era in which conflict increasingly transcends traditional battlefields.

By integrating strategic theory, operational experience, historical perspective, and contemporary examples, Lieutenant General Rakesh Sharma has produced a work that is distinctly Indian in outlook while remaining globally relevant in its analysis. His central message is both timely and enduring: superior preparedness, sound strategy, and institutional adaptability remain the surest guarantees of national security.

Ultimately, the highest form of strategy is not merely winning wars but preventing them through credible preparedness. As the author aptly concludes, the true objective is 'Winning without Fighting'.

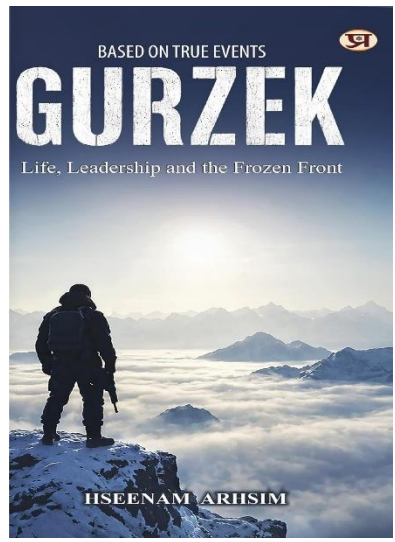
This is a timely, insightful, and significant contribution to India's growing body of strategic literature. It deserves to be read not only by military professionals and defence analysts but also by policymakers, scholars of international relations, students of strategic studies, and informed citizens seeking to understand the rapidly evolving security environment of the twenty-first century.

Colonel RC Patial, SM, FRGS, PhD (Retd)

Review Article 3

Gurzek: Life, Leadership and the Frozen Front

Hseenam Arhsim



Introduction

Writing from within this experience, the author presents military operations without romanticising them, yet with colour derived from the lived knowledge of being closely exposed to the training, leadership and operational dimensions. He focuses on the physical hardship, psychological pressures, uncertainty and stark calculations of survival that typically defines combat in extreme environments. As such, the book is an authentic portrayal of military life and operations in some of the world's most demanding terrain.

About the Book

Hseenam Arhsim brings out certain defining features of command and combat based on true events. In terms of structure, he combines the pace of a military thriller with a deeper exploration of the human

---

Gurzek: Life, Leadership and the Frozen Front by Hseenam Arhsim (pen name), Pages – 208, Price - ₹ 280/-, ISBN 978-93-757-3080-4

and ethical dimensions of leadership, especially under stressful situations in tough terrains. The narrative highlights the pressures of the frozen frontier and focuses on the burdens of command therein, offering readers a deeply moving and nuanced perspective on courage, duty, decision-making, resilience and the human cost of warfare.

This dynamic comes to the forefront especially when the author discusses how a commanding officer has to make life-and-death decisions while simultaneously maintaining the psychological resilience of isolated soldiers in a high-altitude war zone setting. In that regard, this book is not only about combat, but also – and perhaps more importantly – about the isolation of command responsibility in situations that seem almost surreal. It drives home the unyielding truth that every decision demands a cost, often paid ultimately by the men entrusted to lead.

From a reader's perspective, it is safe to say that the author encourages a profound introspection into the different facets of command philosophy, questions of morale maintenance, unit cohesion, decision-making under uncertainty, and highlights the psychological burden of command in the first place. To do so, comprehensively, the book touches upon weather, terrain, intelligence, technology, preparation, movement, risk, execution, tactics and ultimately combat. It then encounters these themes with doubt, responsibility, calculation, moral choices, fear, and uncertainty, operationalizing them to map out the psyche of command under pressure.

The author argues that a commander should not be judged simply by whether an operation succeeded or failed rather by the anatomy of the decision itself: what intelligence was trusted, which risks were absorbed, and which were refused. Crucially, the author forces a deeper reckoning of what price was paid for these decisions and what the commander carries along, long after his command is over.

Conclusion

Gurzek is not a conventional leadership manual; instead it uses military fiction to explore the psychological and ethical dimensions of command, while extending the idea of the 'warrior' beyond the battlefield to the broader question of purpose and responsibility in professional military life. In doing so, the book rises above the conventional military-thriller genre as it touches upon Command, Human Dimension and Leadership dimensions as well. It is not a leadership classic either; however, it combines the elements of a thriller with in-depth lessons in leadership. Most importantly perhaps, the author replaces the conventional imagery of heroism and victory with the more grounded, but no less gloried aspects of responsibility and consequences.

Neelotpal Mishra

USI Latest Publication 2025 to 2026

Pub Code	Type	Title of Publication and Author	Price ₹	Year
Adm/SYB-2025*	Year Book	STRATEGIC YEAR BOOK 2025; Editor-in-Chief: Major General BK Sharma, AVSM, SM** (Retd); edited by Major General Sanjeev Chowdhry (Retd), Komal Chaudhary, Vinayak Sharma, and Richa Sharma **M/s Pentagon Press**	2,950	2025
Adm-1/2025	Book	MODERN CONFLICTS AND CHANGING CHARACTER OF WARFARE: IMPLICATIONS FOR INDIA; edited by Major General Sanjeev Chowdhry (Retd), Colonel Deepak Kumar, Komal Chaudhary, Vinayak Sharma and Richa Sharma **M/s Pentagon Press**	995	2025
CMHCS-14	Book	HONOURS AND AWARDS OF THE INDIAN ARMED FORCES by Dr Amlesh Kumar Mishra **M/s Pentagon Press**	1,995	2025
CMHCS-13	Book	THE SUKRANITI: STATECRAFT AND WARCRAFT by Colonel Pradeep Kumar Gautam (Retd) **M/s Pentagon Press**	995	2025
CMHCS-12	Book	FORGOTTEN: HISTORY OF HONG KONG SINGAPORE ROYAL ARTILLERY by Colonel Mandeep Singh (Retd) **M/s Pentagon Press**	995	2025
CMHCS-11	Book	BECAUSE OF THIS: A HISTORY OF THE INDO-PAK AIR WAR OF DECEMBER-1971 by Air Marshal Vikram Singh (Retd) **M/s Manohar Publishers & Distributors**	7,995	2025
CMHCS-10	Book	PORTRAITS OF VALOUR: TIMELESS MILITARY ART by Lieutenant Colonel Arul Raj (Retd); authored by Major General Ian Cardozo, AVSM, SM (Retd); edited by Squadron Leader Rana Chhina, MBE (Retd) **M/s KW Publishers**	1,280	2025
CMHCS-9	Book	WAR-WOUNDED DISABLED SOLDIERS AND CADETS-A REPORT by Meghna Girish **USI of India**	-	2025
CMHCS	Book	WE TOO WERE THERE: INDIANS AT GALLIPOLI by Colonel Tejinder Hundal, VSM, PhD **M/s Manohar Publishers & Distributors**	3,195	2025
CS3/R-121/2025	Book	CIVIL-MILITARY FUSION AS A METRIC OF NATIONAL POWER AND COMPREHENSIVE SECURITY by Lieutenant General Raj Shukla, PVSM, YSM, SM (Retd) **M/s Pentagon Press**	695	2025
Adm-UNPK/2025	Book	75 YEARS OF INDIA'S CONTRIBUTION TO UN PEACEKEEPING by Major General PK Goswami, VSM (Retd) **M/s Pentagon Press**	895	2025
CS3/R-120/2025	Book	ARTIFICIAL INTELLIGENCE, MILITARY TACTICS, BRIDGES AND ASPIRATIONS: ACTION PLAN INSIDE by Brigadier Pawan Bhardwaj, YSM **M/s Pentagon Press**	1,295	2025
NSP-M-9/2025	Monograph	WHOLE-OF-GOVERNMENT APPROACH TO NATIONAL SECURITY by Lieutenant General AK Singh, PVSM, AVSM, SM, VSM (Retd) and Major General Jagatbir Singh, VSM (Retd) **USI of India**	395	2025
M-8/2025	Monograph	THE EASTERN SECTOR OF INDIA-CHINA BORDER: CHINESE ARGUMENTS, PROBABILITIES AND POSSIBILITIES OF RESOLUTION by Dr Geeta Kochhar and Ritesh Kumar **USI of India**	395	2025
M-7/2025	Monograph	INTERNATIONAL DAY OF UN PEACEKEEPERS 29TH MAY: 75 YEARS OF INDIAN CONTRIBUTION TO UN PEACEKEEPING; compiled by Major General PK Goswami, VSM (Retd) **USI of India**	395	2025
M-6/2025	Monograph	PAKISTAN ARMY'S STRATEGIC CULTURE: IMPLICATIONS AND THREAT ASSESSMENT by Brigadier Sanjay Kannoth, VSM **USI of India**	395	2025
M-5/2025	Monograph	INFORMATION AND CYBER IN NON-KINETIC WARFARE: COUNTER STRATEGIES by Lieutenant General DP Pandey, PVSM, UYSM, AVSM, VSM (Retd) **USI of India**	-	2025
M-4/2025 (UN Forum 2024)	Monograph	USI ANNUAL UN FORUM 2024—CHANGING CHARACTER OF CONFLICTS—CHALLENGES TO PEACE OPERATIONS AND INTERNATIONAL HUMANITARIAN LAW; edited by Major General PK Goswami, VSM (Retd), Major General AK Bardalai, VSM, PhD (Retd) and Colonel KK Sharma (Retd) **M/s Manohar Publishers & Distributors**	350	2025
M-3/2025	Monograph	DRONES AND VIOLENT NON-STATE ACTORS: THE MANKIND'S QUEST FOR VIOLENCE by Major General Anil Kumar Mehra, AVSM, VSM (Retd) **M/s Manohar Publishers & Distributors**	350	2025
M-2/2025	Monograph	CHINA'S STRATEGIC CULTURE AND ITS IMPACT ON THE PEOPLE'S LIBERATION ARMY by Brigadier Sanjay Kannoth, VSM **M/s Manohar Publishers & Distributors**	359	2025
M-1/2025	Monograph	COMPREHENSIVE STRATEGIC DETERRENCE TO MEET INDIA'S FUTURE CHALLENGES by Brigadier Rajeev Bhutani, PhD (Retd) **M/s Manohar Publishers & Distributors**	250	2025
OP-7/2025	Occasional Paper	OPERATION SINDOOR: A BENCHMARK IN INDIA'S MODERN MILITARY DOCTRINE by Brigadier PP Singh, AVSM, VSM (Retd) **USI of India**	250	2025
OP-6/2025	Occasional Paper	BATTLEFIELD SYMPOSIUM HAJIPIR VALOUR BEYOND THE PASS COMMEMORATING DIAMOND JUBILEE OF VICTORY AT HAJI PIR; compiled by Major General PK Goswami, VSM (Retd), Brigadier Rajat Mohan Bhatt, PhD, and Colonel Vikas Kumar, SM **USI of India**	250	2025

USI

(Estd. 1870)

OUR ACTIVITIES

Centre for Strategic Studies and Simulation (CS3)

The erstwhile Centre for Research was re-christened as CS3 on 01 Jan 2005. The Centre focuses on detailed and comprehensive enquiry, research and analyses of national and international security related issues, and undertakes gaming and simulation of strategic scenarios, to evolve options for wider discussion and consideration.

Centre for Military History and Conflict Studies (CMHCS)

The CMHCS was established in Dec 2000 at the behest of the three-service HQs to encourage an objective study of all facets of Indian military history with a special emphasis on the history of the Indian Armed Forces. It focuses on diverse aspects of the history of Indian military evolution, policies, and practices – strategic, tactical, logistical, organisational, socio-economic, as well as the field of contemporary conflict studies in the broader sense.

Centre for Emerging Technology for Atma Nirbhar Bharat (CETANB)

The centre started as the Atmanirbhar Bharat Initiative in 2022 and later rechristened as the CETANB on 01 Jan 2024 and included Cyber Centre of Excellence (CCoE) as part of it, in conjunction with Cyber Peace Foundation. The centre's objective is to forge emerging technologies with geostrategic and geopolitical situations with a view to make the services self-reliant by making possible the indigenous production of defence equipment and spares. The CCoE trains military personnel in artificial intelligence, cyber, and machine learning, in addition to cyber forensic analysis in its well-equipped lab. Furthermore, it helps MSMEs to break into the defence industrial ecosystem.

Centre for United Nations and Humanitarian Studies (CUNHS)

The centre was established under the United Nations Peace Keeping Centre (CUNPK) in 2000. It organises workshops, seminars, and training courses for peacekeepers, observers and staff officers, both Indian and foreign. It also oversees the practical training of the Indian contingents. In Aug 2014, CUNPK moved to Integrated Headquarters (Army) of Ministry of Defence. The USI has now established CUNHS, which is focusing on operational, strategic, and policy issues related to United Nations Peace-keeping. It also organises seminars and conferences on such issues.

Centre for Professional Military Education (CPME)

The Institution conducts regular correspondence – interactive courses and mock test practices and assists and helps officers prepare in online and offline modes to help them prepare for promotion examinations and competitive examinations for entrance to Defence Services Staff College, and the Technical Staff College. Over the years, the activity has been a significant and well-received activity.

Centre for Publications and Library (CP&L)

This section manages the USI's key publications including the Strategic Year Book, USI Journal, books, monographs, occasional papers, and joint publications. These works contribute to an informed discourse on defence, strategy, and national security. The Strategic Year Book offers an annual review of critical developments, while other publications provide deeper analysis and collaborative perspectives. The USI Journal, Asia's oldest defence journal (est 1871), serves as a platform for military and strategic thought, welcoming contributions regardless of rank. The Journal remains a vital space for responsible and quality-driven engagement.

USI Gold Medal Essay Competition

Every year, the institution organises a Gold Medal Essay Competition, open to commissioned officers of the Defence Services and officers of the Territorial Army, Assam Rifles, and the Senior Division of the National Cadet Corps, and Gazetted Officers of the Civil Administration in India, including retired officers. These essays, the first one of which was introduced in 1871, constitutes a barometer of opinion on matters that affect national security, in general, and the defence forces, in particular.

Lt Gen S L Menezes Memorial Essay Competition

This has been instituted from 2015 on a subject related to armed forces historical research. The essay competition is open to everyone across the globe.

USI War Wounded Foundation Joint Essay Competition

This essay competition was instituted in 2021 through a Memorandum of Understanding between the USI and the War Wounded Foundation. The competition is open to all across the globe and must be about issues relating to the experiences and/or rehabilitation of war-wounded and disabled personnel of the Indian Armed Forces.

USI-Lt Gen PS Bhagat Memorial Essay Competition

The USI–Lt Gen PS Bhagat Memorial Essay Competition fosters intellectual inquiry, original research, and professional discourse on military leadership and strategic issues. It honours Lt Gen PS Bhagat's legacy while promoting strategic writing and advancing knowledge in defence and security studies.

MacGregor Medal

This medal is awarded to armed forces personnel for valuable reconnaissance and adventurous activity they may have undertaken.

Lectures, Discussions and Seminars

A series of lectures, discussions, and seminars on service matters, international affairs, and topics of general interest to the services are organised for the benefit of local members in Delhi.

Library and Reading Room

The library includes over 72,000 books, including rare works from the 17th–19th Centuries, with a primary focus on strategy and defence alongside diverse subjects on Indian life. It offers extensive research resources, an air-conditioned reading room with current material, and has been fully automated since 2002.

Printed by Manish Comprint, New Delhi - 110 015 Phone : 011-41037172