ISSN 2319-5177

CLAWS JOURNAL

SUMMER 2025

VOL. 18, NO. 1

CENTRE FOR LAND WARFARE STUDIES

CHANAKYA CONFERENCE HALL: RATE CHART

FULL DAY: INR 25,000/-

HALF DAY: INR 15,000/-

LED Data Wall: INR 10,000/-

CLAWS JOURNAL

ISSN: 2319 – 5177

JOURNAL OF THE
CENTRE FOR LAND WARFARE STUDIES (CLAWS)

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

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

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

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

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

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

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

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

PATRON CLAWS

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

ADVISORY BOARD

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

BOARD OF GOVERNOR(S) {BoG}

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

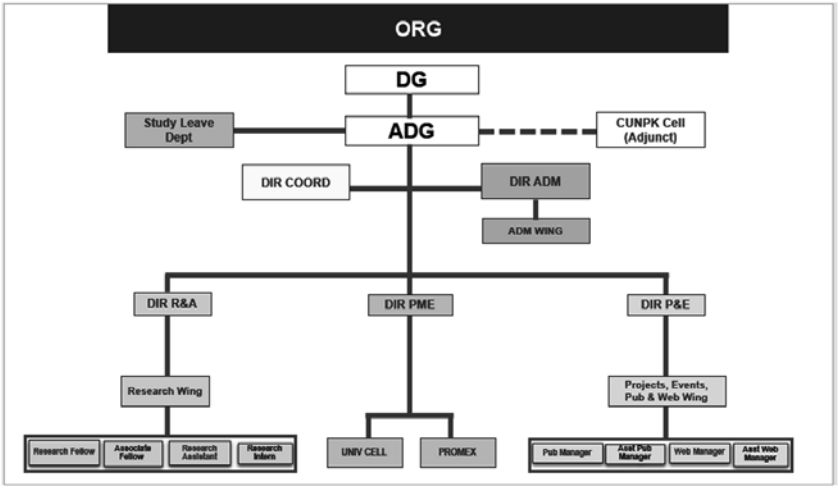
***The Director General, CLAWS will also be a member of the BoG and also act as Member Secretary of the BoG, CLAWS.**

EXECUTIVE COUNCIL (EC)

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

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

ORGANISATION OF CLAWS



CLAWS VERTICALS

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

MEMBERSHIP DETAILS

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

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

Key Benefits of Individual Membership.

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

Eligibility:-

Individual Life Membership

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

Institutional Membership

Corporate / Institutional Membership

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

Associate Membership

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

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

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

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

Passport Size Photograph for Individual Member

APPLICATION FOR INDIVIDUAL LIFE MEMBERSHIP

Please tick any one:-

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

Sir,

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

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

_____
(Counter Signature for Serving Offr only)

Mode of Payment

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

OR

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

Dated …… ……
(Signature of Applicant)

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

FOR OFFICE USE ONLY

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

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

To

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

APPLICATION FOR INSTITUTIONAL MEMBERSHIP

Please tick any one:-

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

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

Sir,

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

Name of Institution _____

Address: _____

_____

_____

Phone/Mobile:_____ Fax: _____

Email:_____

Mode of Payment

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

OR

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

Dated …… ……
(With Institutional Seal) **(Signature of Applicant)**

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

FOR OFFICE USE ONLY

Multi-city Cheque/DD Details: _____

Membership No.:_____Date of Issue of Membership Card:_____

Remarks of Director:_____

Remarks of Director General:_____

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

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

Note(s):-

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

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

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

For Queries Contact
landwarfare@gmail.com

ADVERTISEMENT RATE CARD : CLAWS PUBLICATIONS

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

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

For Queries Contact: landwarfare@gmail.com

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

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

APPLICATION FOR CLAWS STUDY MATERIAL FOR DSSC/ DSTC 2024

Sir,

I would like to apply for DSSC / DSTC 2024 Study Material prepared by CLAWS. I understand that my application is subject to approval and if approved, I will respect and follow the rules and regulations of the Centre.

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

Unit : Address for communication .....

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

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

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

Subscription Rate: Rs 5,000/- for all three subjects, Rs 3,500/- for any two subjects and Rs 2,000/- for any one subject. (Only 50% of the indicated amount needs to be remitted)

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

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

Date: (Signature of Applicant)

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

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

FOR OFFICE USE ONLY

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

INDIAN COUNCIL OF SOCIAL SCIENCE RESEARCH

Social and human sciences research enhances our understanding of the social reality and the issues and problems that need to be solved. The actionable outcomes of research provide policy inputs and frameworks for socio-economic and all-round development and generate ideas, facts, insights and methodologies that can be used in policy framing, teaching and research.

India has had a long, cumulative and rich tradition of thought production in social and human sciences since the *Rigveda* (1500 BCE). The intellectual tradition since Panini has reflected on the social and cultural meaning and evolved epistemologies of enquiry for the attainment knowledge based on observation, logical and rational thinking. Educational and research institutions such as Takshashila, Nalanda, Vikramashila, Vallabhi, Pushpagiri and Somapura flourished as global centres of learning in different parts of India, and produced great knowledge in diverse fields such as Ayurveda, Medicine and Surgery, Jurisprudence, Mathematics, Astronomy, Physics, Metallurgy, Civil Engineering, Architecture, Philosophy, Grammar, Agriculture, Economics, Commerce, Politics, Statecraft, Military Education, Literature, Craft etc. These institutions set very high standards of teaching, learning and research for scholars from across the world. This system of Indian education produced scholars of great stature such as Aryabhatta, Bhaskaracharya, Amarsimha, Chandrabardai, Banbhatta, Dandin, Jivaka Komarabhacca, Mahaviracharya, Charaka, Susruta, Baudhayan, Chanakya, Brahmagupta, Panini, Patanjali, Nagarjuna, Pingala, Gargi, Kanad, Varahamihira, Thiruvalluvar, Tolkappiyar and so on.

After Independence, Bharat sought to regain its indigenous model of social and human sciences research that required decolonization of the education and research. As the country's development process threw up numerous and diverse challenges that required extensive research and analysis, the Government of India established a Committee for Social Science Research under the Chairmanship of Professor V.K.R.V. Rao in 1965 to review the social science research scenario in the country and make recommendations to accelerate its progress. This led to the establishment of the Indian Council of Social Science Research (ICSSR) in 1969 to encourage, promote and fund social science research in the country. Since its inception, ICSSR has played a pivotal roles in building the capacities of early career and senior researchers through grants and projects as well as training in research methodologies with the objective to produce high-quality research usable for policy intervention and policy making. It has also made immense contribution to humanities and cultural research as way to

decolonise the formations of self and society across the length and breadth of the nation.

It has been recognised that the need of the hour is to shift from merely documenting the 'exceptionalism' of India to engaging with the diverse social realities of the country with a philosophical stance of inwardness, so as to be able to develop an original and fresh understanding of a larger variety of issues, generate new theories and perspectives and represent the multiple voices of varied people of India.
In the 21st century, when the nation aims to become a Viksit Bharat by its centenary year of Independence, 2047, ICSSR seeks to establish a symmetry between social research and society. In line with the recommendation of the National Education Policy (2020), we seek make social research equitable, affordable, inclusive, socially sensitive and globally competitive.

We are an autonomous body under the Ministry of Education, Government of India and a premier organisation with 24 **Research Institutes** (grant-in-aid), 17 **Recognised Research Institutes** and Six **Regional Centres** located in different parts of the country.

Mandate

The ICSSR's aims and objectives, as detailed in our **Memorandum of Association (MoA)**, are the following:

- To review and survey the progress of Social Science Research and advise the Government on policy issues;
- To fund and promote Social Science Research in Universities/Colleges/Research Institutes;
- To award Doctoral, Post–Doctoral, Senior and National Fellowships to researchers and faculties;
- To award Minor, Major and Collaborative Research Projects to researchers and faculties;
- To fund National and International Seminars and Conferences to disseminate social science research findings;
- To support Training and Capacity Building Programmes for young researchers and faculties;
- To provide International Travel and Data Collection Grants to scholars and faculties;
- To encourage International Collaboration in social science research with well recognized foreign research funding agencies;

- To fund the publication of journals and books in social science research and also strengthen professional social science associations/organizations;
- To provide library, documentation, data and online services for social science research; and
- To indicate periodic themes in neglected and new critical areas of research.

Organisational Structure

The ICSSR's highest decision-making body, known as the **Council**, has 26 members, which includes the ICSSR **Chairman** and the **Member-Secretary**, 17 Social Scientists (Non-Ex-Officio members), one Co-opted member and six Ex-officio members representing the Government of India.

The Member Secretary is the Chief Executive Officer and heads the ICSSR Secretariat consisting of Directors, Deputy Directors, Assistant Directors and other officials. The ICSSR's officials, apart from their normal official duties, make regular contributions through research papers, articles, articles in edited books, journals etc., and have also delivered lectures during the reporting year.

The Council has three standing committees, namely the **Research Committee (RC)**, **Research Institutes Committee (RIC)** and **Planning and Administration Committee (PAC)**.

Contents

Articles

Threats in Grey Zone Warfare: Securing Systems, Processes and Supply Chain

Partha Pratim Dubey

Introduction

Grey Zone or Hybrid Warfare has evolved over the years—blurring the thin lines between kinetic and non-kinetic means, with revolution in cutting edge communication and information technology being the major enabler. It is now considered as the best available option below the threshold of conventional war or conflict and is being employed rampantly by state as well as non-state actors thereby posing risk of infinite magnitude in the overall paradigm of national security.

India's northern adversary viz. China has been employing Grey Zone Warfare to undermine its adversary as part of its strategy. China's expanding manufacturing base especially in electronics components, assemblies, chips, power packs and batteries together with growing dominance in its supply chain, even outside its frontiers, provides it with an advantage to tweak targeted systems for future exploitation.

The domination of battle space by use of low cost options in the form of Drones and AI enabled technologies has been witnessed in recent times—right from the Armenia-Azerbaijan to Israel-H3I(Hamas, Hezbollah, Houthi & Iran) and in the ongoing Russia-Ukraine Conflict.

Colonel **Partha Pratim Dubey** is Senior Fellow at the Centre for Land Warfare Studies (CLAWS), New Delhi. Views expressed are personal.

As AI technology driven hardware and software captures the battle spaces across the spectrum of conflicts, nations are undergoing transformation in terms of doctrines, war fighting strategies and increasingly focus on acquiring cost effective technology driven solutions for ISR, target acquisition and destruction.

As military hardware reliance shifts more on nanotechnology driven chips, microprocessors, faster communication kits with encryption, power packs/batteries, it poses few challenges from security point of view in terms of embedded technology, deliberate vulnerabilities and tweaking systems within the supply chain. The deliberate exploits within the hardware system and associated software solutions subject the military asset to a high degree of risk, thus jeopardising its mission effectiveness.

Imagine a scenario, wherein an Unmanned Combat Aerial Vehicle (UCAV) with lethal payloads is taken over by an adversary—exploiting the embedded technology or hacking communication. The scenario, highlights the overall security sensitivity while sourcing, adopting and absorbing new fighting technologies and solutions together with a need to create effective safeguards, mitigation measures and secure the diverse supply chain. It is therefore imperative to understand the threats to own critical assets and put in place a robust security framework complimented with adequate policy guidelines, technology innovation, legal support and skilled workforce duly supported with an effective Intelligence network.

Threats

In early 2024, two tactical UAVs of the Indian Army, along the LAC in Eastern Ladakh failed to take off for a mission. In August 2024, a fixed wing UAV of the Indian Army, on a mission in Poonch sector of J&K in vicinity of the line of control, veered off its path and crossed over to Pakistan. The UAV incidents were initially assessed to be technical malfunctions however, detailed investigation revealed the presence of

Chinese components on board the systems which were exploited by means of hacking to take control of the UAVs from the Indian Operators.

India Today in its article titled "Chinese Threat to Indian Drones" dated 31 January 2025, highlighting the two incidents in year 2024, flagged serious concerns with 'Make in India' UAVs for defence sector with existence of Chinese components and related cyber security concerns. It also quoted earlier directives by DGMI barring the use of Chinese origin components in equipment for defence sector and also directions for stringent hardware and software testing to ensure compliance. Overall, the article covered it as a National Security threat and emphasised on the need to create adequate safeguards.

India Today, in its second article on the same subject dated 10 February 2025, covered the MoD and Government of India's decision to cancel three contracts worth 230 crores for procurement of 400 (200 medium-altitude, 100 heavy payload and 100 light payload logistics) 'Make in India' drones for deployment on the Northern Borders.

Israel stunned the world with its operation 'Grim Beeper' to target the Hezbollah leadership in Syria and Lebanon triggering simultaneous explosions involving thousands of handheld Pagers on 17 September 2024 and Walkie-talkies on 18 September 2024. A highly classified operation, exploited the loopholes in the global supply chain, and tweaked the Pagers and Walkie-talkies sourced from specific entities with explosives and malwares. The precision strike operations exploited the vulnerability in existing supply chains to strike a massive blow to Hezbollah terror organisation leading to 42 fatal casualties and injures to over 3500.

Threats related to data leaks culminating into unauthorised access to classified operational issues, back door entries by embedded components passing security architecture though communication module, camera and control systems, results in acquiring of intelligence, disruption of systems and even in taking control of assets while in flight mode. The Chinese

threat is not only limited to defence sector drones but also in civilian domain as the demand for drone based operations has witnessed massive growth in last couple of years.

To broadly illustrate threat to military assets like drones, its sub-assemblies can be broadly be categorised into 'Active' and 'Passive'. Active components primarily include Micro Processors, Communication Interface, Sensors, Flight Control System and Memory storage units. Passive components generally include Printed Circuit Boards (PCBs), Motors and Power generation and control systems. Malicious codes embedded, in the form of firmware or malware, can find its place in each of these components thereby compromising the asset.

China, in the last two decades, has dominated the global electronics manufacturing and supply chain. In view of unprecedented level of control and censorship, China provides its agencies to create substantial amount of grey zone capabilities through means of disruptive approach by injecting malware in electronic components, specifically tweaking critical supply chains with sourcing of electronics components within or outside China. It is therefore important that the threat is not limited to a country, as in case of our fixation with China or a source, but it manifests from across the globe even within our trusted partners and allies.

It is imperative to understand that threat to assets are not completely negated post the induction phase where it undergoes stringent audits, test and certifications. Assets can equally be vulnerable during the period of its unauthorised access—during repairs, overhaul and upgrade. In view of the same, manifestation of threat could be in the form espionage through sharing of sensitive data or sabotage with total destruction of the asset. In cases, remote control of devices can result in both espionage through its use as listening device post its induction and sabotage based on specific missions like targeting key leadership.

The threat is omnipresent with exploitation of wide range of devices or equipment and networks based on criticality of its use in civil/military,

source of origin, supply chain, accessibility and threats in the Grey Zone, within the overall security paradigm, in view of prevailing geo-strategic or geo-political situation.

Case Study

As part of the Case Study, a publication of US Department of Defense titled "Securing Defense Critical Supply Chain" is being reviewed to highlight the manner in which similar threats and vulnerabilities has been studied in detail to forge strategies, mitigation measures, action points and recommendation.

The publication is an Action Plan in response to the former President of the US Joe Biden Executive Order (EO)-14017 with an aim to build a secure, diverse and resilient supply chain. The first part of the action plan identifies four areas of critical vulnerability:

Kinetic Capability	–	All forms of guided missiles and precision weapon systems
Energy Storage and Batteries	–	High capacity types to include Lithium batteries.
Casting and Forging	–	Metals and composites being used for military/strategic assets.
Micro-Electronics	–	To include State of the Practice (SOTP), legacy electronics and State of the Art (SOTA).

Post identification of critical vulnerability, the action plan lists out four strategic enablers to build the overall supply chain resilience.

Work Force	–	trade skills through doctoral-level engineering skills.
Cyber Posture	–	industrial security, counter intelligence, and cyber security.

Manufacturing	–	current manufacturing practices, as well as advanced technology like additive manufacturing.
Small Business	–	the role of key members of DoD supply chains.

The next part of the action plan focus on creating a resilient supply chain structure and providing four actionable grouping to create a framework based on cooperation. The four action grouping built around the Defence Industrial Base (DIB) being named as Supply Chain Resilient Framework are:

Internal	–	All issues within the control of Department of Defense.
Interagency	–	Cooperation and coordination across multiple Government agencies.
International	–	Allies and friendly countries.
Industry Initiatives	–	Industry Partners & Collaborators.

Cross Cutting Recommendations forms next part of the Action Report. Post evaluation of the Focus Areas of Vulnerabilities and Strategic enablers, recommendations are made to address each of the vulnerabilities which needs to be undertaken by the resilient framework working in coordination and cooperation with four identified Strategic Enablers. Broad Cross Cutting Foundational Recommendation for strategic informed acquisition and sustainment decisions are listed as under:

- Build Domestic Production Capacity
- Engage with Partners and Allies
- Mitigate foreign Ownership, Control or Influence and Safeguard Markets
- Conduct Data Analysis
- Aggregate Demand
- Develop Common Standards

- Leverage Commercial Sector Innovations
- Limit Use of Military Unique Requirements
- Update Acquisition Policy

The report has dedicated individual chapters to four identified critical vulnerability (Kinetic Capability, Energy Storage & Battery, Casting & Forging and Microelectronics) to comprehensively address the subject. Each chapter covers the national security significance associated with vulnerability followed up with sector specific challenges with summary and lastly the recommendations to each of the four actionable grouping framework (Internal, Interagency, International and Industry Initiatives) for resilience in supply chain. Issues related to Microelectronics and Status update on 100 days Strategic and Critical Materials Report are briefly covered in subsequent paragraphs.

Microelectronics

National security significance is covered in the initial part of the article highlighting the criticality of Microelectronics in commercial and defence products ranging from smartphones, kitchen appliances, automobiles to precision guided weapon technology, aviation, satellites and critical infrastructure sectors. It highlights the diverse supply of microelectronics as part of the global ecosystem and how securing the supply chain is vital for national security.

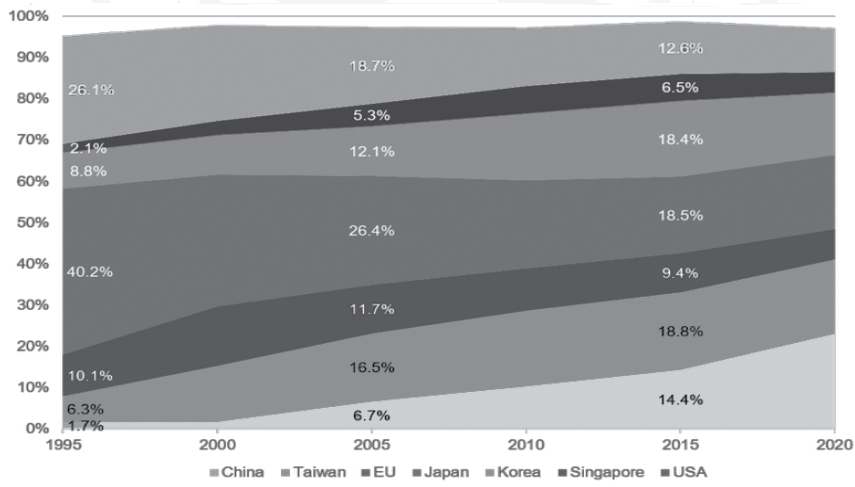
It highlights the broad grouping of microelectronics based on size into State of the Practice (SOTP), Legacy electronics and State of the Art (SOTA) and covers the complex manufacturing process involving 500 steps with a flow as under:

- **Product design**: facilitated by Electronic Design Automation (EDA) tools.
- **Fabrication**: lithographic patterning and manufacturing of silicon die on a common substrate or wafer.

- **Packaging and assembly**: singulation of silicon die and integration of die into package.
- **Final test and quality control**: electrical testing to ensure product functionality and reliability.

The report highlights that manufacturing of microelectronics is centralized in the Asia-Pacific region and the ancillary industries that support manufacturing are globally dispersed. The dimension and intricacies of the global microelectronics supply chain can be understood from data—there are approximately 10,000 large microelectronics manufacturing firms dispersed globally which serves as source for over 500,000 microelectronics components. However, 88 per cent of production and 98 per cent of the assembly, packaging, and testing of microelectronics is undertaken in Taiwan, South Korea, and China. The graph below highlights how the US share the microchip or wafer market has shrunk in contrast to China.

Figure 1: Global Semiconductor Manufacturing by Location (in percent)



Sector challenges in microelectronics covered a wide variety of issues which have been highlighted as under:

- **Supply Chain Visibility**: Limited visibility in sub-tiers of microelectronics supply chain makes it difficult to identify the threats, vulnerabilities and risk.
- **Foreign Dominance in Commercial Production of Semi-conductors**: Impacts next generation capability development that lacks domestic production.
- **Measurably Secure Microelectronics Source**: Counterfeit microelectronics in the supply chain is a major threat leading to premature systems failure, adversely affecting mission reliability.
- **Non-Market Competitive Practices**: Government subsidy for the manufacturers in the Asian markets.
- **Obsolesces**: Due to the faster pace of evolution sustaining production for commercially non-viable microelectronics becomes a challenge.
- **DoD Procurement Practice**: More stringent reliability criteria—testing and operations in harsh environment.

The recommendations to deal with identified sector challenges have been classified based on the vulnerability enablers and action groups to address the issue in cooperation and coordination with all other stake holders. The table below highlights the host of recommendations in the microelectronics sector.

Table 1: Challenges and Recommendations for Microelectronics

		Supply Chain Visibility	Foreign Dominance	Measurably Secure Micro-electronics	Non-market competitive practices	Obsolescence	DoD Procurement Practices	Declining Workforce
Internal	Rec M1.1: Leverage investment authorities			✓	✓	✓		
	Rec M1.2: Develop measurably secure microelectronics	✓		✓				
	Rec M1.3: Use microelectronics digital engineering and prototypes					✓		
	Rec M1.4: Drive domestic microelectronics ecosystem innovation		✓	✓				
	Rec M1.5: Track and prevent counterfeit microelectronics			✓			✓	
Interagency	Rec M2.1: Fund the CHIPS Program		✓	✓	✓			
	Rec M2.2: Support Commerce on EO 14017 100-Day Report Implementation	✓	✓	✓	✓			✓
	Rec M2.3: Continue/expand the advancement of STEM careers and education	✓						✓
International	Rec M3.1: Leverage international interest in microelectronics collaboration	✓		✓	✓			
Industry	Rec M4.1: Align DoD investment authorities to support domestic supplier base	✓		✓	✓		✓	
	Rec M4.2: Collaboratively develop standards			✓		✓		
	Rec M4.3: Expand industry outreach efforts to identify capabilities and opportunities for partnership	✓	✓	✓		✓		
	Rec M4.4: Leverage industry best practices		✓			✓	✓	
	Rec M4.5: Share roadmaps to increase visibility	✓				✓	✓	

Status Update: 100 Day Strategic and Critical Material Report

The action report further shares a status update on the study of US Department of Defense (DoD): 100 days Strategic and Critical Material Report as part of the exercise under Executive Order. The report lists out the Risk to supply chain:

- Concentration of Supplies
- Single Source Suppliers
- Price Shocks
- Human Capital Gaps
- Conflict Minerals and Organised Crimes

The 100 days report further identified four key pillars to enhance resilience in supply chain associated with the sector as part of the Defence Industrial Base, which are listed as under:

- Drive Demand
- Stimulate Supply
- Hedge Risk
- Promote Equity

The two tables below illustrates the clarity with which the study was conducted and also provides a status update of the Strategic and Critical Material Report. The exercise has been a follow up action in response to the Executive Order of the US President, therefore each aspect highlights the objective, status of progress, stakeholder to act, recommendations and overall effectiveness while addressing strategic concerns related to supply chain within the Defence Industrial Base (DIB).

Table 2: U.S. Stockpile Objective

Objective	Status (Action)	Class (Vehicle)
Executive Order delegating National Defense Stockpile release authority	Complete	FY 2021 – Executive
Reinstate the biennial modeling requirement for strategic and critical material supply chains	Complete	FY 2022 – NDAA[52]
Authority to loan material to other Federal agencies to mitigate peacetime disruption risk	Complete	FY 2022 – NDAA
Obtain direct-hire authority for the National Defense Stockpile and mobilization programs	In Progress	FY 2022 – Executive
Obtain new appropriations for the National Defense Stockpile	In Progress	[TBD] FY2022 – Appropriations Law
		[TBD] FY2023 – Budget Request
Grant the National Defense Stockpile the authority to acquire shortfall materials	Rejected	FY 2022 – NDAA
	In Progress	FY 2023 – NDAA
Reform to the Strategic and Critical Materials Stock Piling Act of 1979	In Progress	FY 2023 – NDAA

Table 3: Summary of Implementation for Recommendations in E.O. 14017 Review of Critical Minerals and Materials

Recommendation	Actions To Date	Lead Component
1. Developing and Fostering Sustainability Standards for Strategic and Critical Material-Intensive Industries	EPA is leading interagency comment submissions and development of criteria under the EPEAT eco-label for • Chemicals of Concern • Sustainable Use of Resources • Climate Change Mitigation • Low-embodied Carbon Criteria for Photovoltaic Modules	Environmental Protection Agency (EPA) in partnership with DOE
2. Expanding Sustainable Domestic Production and Processing Capacity, Including Recovery from Secondary and Unconventional Sources and Recycling	Interior is prioritizing the critical minerals list for risk mitigation by the inter-agency Interior is leading work with other federal agencies on developing principles and an engagement strategy for comprehensive mining law reform DOE is using new authority and funding to:[54] • Establish a new Critical Material Consortium to develop substitutes and promote resource efficiency • Support pilot plants to extract rare earths from alternative feedstocks, such as coal or mine waste • Promote battery recycling and value-added processing of battery materials	Department of Interior and DOE
3. Deploy the DPA and Other Programs	DoD is awaiting FY 2022 appropriations to resource industrial base investment projects and initiate new-starts POTUS to release a Determination pursuant to DPA Title III to support battery mineral production	DoD
4. Convene Industry Stakeholders to Expand Production	DoD will develop a pilot program to facilitate B2B risk mitigation	Multiple
5. Promote Interagency Research & Development to Support Sustainable Production and a Technically Skilled Workforce	DOE, in partnership with DoD and other agencies, is leading the development of an R&D roadmap to address critical minerals and materials needs for the Nation	DOD
6. Strengthen U.S. Stockpiles	See Table 6	DOE
7. Work with Allies and Partners and Strengthen Global Supply Chain Transparency	State has led over 5 senior-leader engagements with allies and partners	Department of State

Conclusion

The action report concludes by flagging issues in aftermath of the global COVID-19 pandemic wherein non reliable supply chains can have grave implications on the economic prosperity and national defence of a nation. It is therefore imperative to work closely within and outside and include interagency, international and industry in order to build robust and responsive supply chains.

A total of 64 recommendations has been made as part of the report to increase domestic manufacturing base, electronics capability development, enhance coordinated efforts with partners and allies to further strengthen economic and national security. DoD will use the recommendations to

prioritize policy and investment decisions in coming years to strengthen DIB with improved resilience in its supply chains.

Comments

The comments are specific to the case study highlighting the US DoD Action Plan Report: Securing Defense—Critical Supply Chain. India and many other countries including US continues face similar security challenges in the critical defence sector in view of the growing dominance of China in the global manufacturing with diverse sourcing and supply chain.

The case study has comprehensively covered the subject highlighting all possible aspects in a systematic approach to flag the threats, vulnerability and risk. The identification of strategic enablers holds good for all nations subjected to similar challenges and so is the case for the action group framework for resilience supply chain to spearhead the recommendations across all stakeholders. The action report, with its 64 recommendations, could be used as a reference point for any other studies—to deal with similar challenges related to global supply chain dealing with critical components having strategic or operational ramifications.

The action report however has not highlight any intelligence and security structures to deal with attempted cases of espionage or sabotage attributed to embedded firmware or malware. The report did refer to detected cases of counterfeit microelectronics but did not cover any issues related with procedures to deny, secure or deter, detect such aspects. At the same time, no legal frameworks have been covered to further strengthen investigations of threats, risk, security breaches attributable to components and subsequent prosecution.

Recommendations

In India, MoD is in the process of drafting and implementing stringent policies and framework to ensure adequate procedures to deal with

the threat emanating from embedded systems and threats, risk and vulnerabilities associated with the systems, processes and supply chain of critical components associated within the strategic and sensitive defence sectors.

Having highlighted the threats and the case study related to US DoD on the subject, the article outlines few recommendations in the subsequent paragraphs for the policy makers, researchers and domain experts dealing with the subject.

- **Task Force or Study Group**: As covered in the case study, similar exercise need to be undertaken at the apex level by constituting a Task Force or Study Group. It needs to exhaustively address the issue of threat posed to systems, processes and supply chain in defence and other strategic sectors, to provide a road map comprising of frameworks, structures, standards, action groups and recommendations. The body constituted needs to have representation from Defence Forces, Academia, Industry and Domain experts to include scientist.
- **Action Taken Report**: The report of the Task Force need to be ratified by the Govt and 'Action Taken Report', in the form of status updates, needs to be taken out within a stipulated timeframe.
- **Classification of Components & Projects**: In view of the sensitivity associated with components or projects based on its applications, the same needs to be classified as Very Critical, Critical and Non-Critical. Accordingly, the security safeguards, testing and certification dovetailed during process of induction, upgrades and throughout its service and disposal, needs to be upgraded.
- **Building Domestic Capability**: Efforts on priority to be taken to build domestic manufacturing capability especially in the very critical and critical component segment. In major acquisition, transfer of technology need to be an integral part for expanding the domestic defence manufacturing base.

- **Civil-Military Fusion Approach (Dual use technology solutions)**: Govt, Academia and Industry need to focus on transforming military specific solutions to dual use solutions through ideas and innovations. The initiative enhances the overall scope of development and the scale of demand, which aids in propelling growth with infusion of greater resources for R&D.
- **Dual Level Testing & Certification**: The concept of testing and certification needs to overhaul with Dual level testing and certification for all very critical and critical components and projects. The defence industry ecosystem need to create domestic level testing and certification for firms to test its products to meet the laid down standards. Govt level testing and certification facilities needs to be developed together with Institutions of Excellence like IITs to further boost R&D.
- **Joint Development & Collaboration**: All efforts need to be made to jointly develop niche technology solutions with other nations and foreign institutions. The success of Brahmos is a case in point and there should be more such collaborative projects to further strengthen cooperation in defence manufacturing and technology development.
- **Government Incentives, Concessions and Exemptions**: Govt needs to further provide boost to defence industry ecosystem in the form of incentives, concessions, clearances, attractive policies, tax exemptions. In addition, defence procurement procedures need to be further simplified as part of the 'Make in India' initiative to provide boost to start-ups in the sector.
- **Security Framework**: In view of the sensitivity related to national security associated with defence industry, a comprehensive security framework has to be put in place. It should have adequate safe guards, checks & balances, fix accountability, deter any compromise, high capability of detection to aid further investigation of breaches.

A robust and responsive intelligence network need to compliment the security framework to monitor assets throughout its life cycle and also keep the supply chain under strict scrutiny.

- **Legal Framework**: Cyber security and other associated policies need to be revised to cater for the threats engineered deliberately with defence industry. Stringent laws need to be put in place to aid prosecution and harsh punishments to individuals or organisation involved in any form misadventure and act as a major deterrent.
- **Innovations & IPR**: Government, through its agencies like IDEX, Army Design Bureau (ADB), needs to work in close coordination with Academia and Industry. It also needs to encourage Innovations by providing challenging problem statements for defence technology requirements. Initiatives need to be taken up not only for development but also for stringent testing and certification.
- **Enhanced Funding on R&D**: Government needs to enhance the annual outlay for R&D in the defence and strategic development structures. R&D budget needs to be raised up to 2.5% of the GDP. It is critical from the point of view of self-reliance in defence industries which further provides avenues for exports.
- **Periodic Reassessment**: In view of the dynamic nature of threat, its not a one time exercise, therefore there is a need for periodic reassessment of threats. It is imperative to review the existing procedures and policies to strengthen the people, processes and systems associated with the defence sector.
- **Domestic Capability for Vulnerability Testing**: No system is full proof—building further on the same premise, a third party vulnerability testing is need of the hour. Professionals from diverse fields need to be encouraged to register for projects to test vulnerability of own systems and flag it for further action to plug it.

The recommendations flagged above are only few to provide a general direction to the thoughts of our strategic community while securing our processes, systems and the supply chain. While the organisation undertakes the initiative, one needs to avoid strong biases regarding a particular country or origin of material sourced. The safeguards need to be put in place across the board without any form of discrimination to objectively address the threats, vulnerabilities and mitigate the risk.

Conclusion

India as a nation faces major security challenges from China and Pakistan. In addition, recent political developments in India's immediate neighbourhood viz. Bangladesh, Myanmar, Sri Lanka, Maldives and Nepal further adds to India's security concerns. As India aspires to be Vikhsit Bharat in 2047, as a nation, it needs to focus on four core areas that is Diplomacy, Information & Technology, Military and Economy.

The nature of conflict, over the years, have undergone rapid changes with Grey Zone Warfare evolving as the most preferred low cost option below the threshold of conventional conflict. China, in particular, has been a major proponent in the Grey Zone as the policy of 'Winning War Without Fighting' is in sync with its Three Warfare Strategy of Psychological & Propaganda Warfare, Media Warfare and Legal Warfare.

As India continues to modernize its armed forces with unprecedented level of technology absorption and transformation to take on the future security challenges, it is imperative to secure the processes, systems and the supply chain with robust safeguards. Hence, focus on attaining self-reliance by building a domestic resilient defence industry ecosystem through 'Make in India' is the only way forward in strengthening the overall national security.

Bibliography

https://aft.systems/aerospace-and-defence-testing-and-approval-everything-you-need-to-know/

https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2022/07/defence-standards-and-testing-infrastructure.pdf.coredownload.inline.pdf

https://grcoutlook.com/risk-assessment-for-embedded-systems/

https://usawire.com/top-emerging-threats-in-embedded-systems-security-and-how-to-mitigate-them/

https://www.indiatoday.in/india-today-insight/story/chinese-threat-in-indian-drones-2675751-2025-02-06

https://www.oxan.com/insights/chinas-supply-chain-role-may-pose-cybersecurity-risks/

https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf

https://www.astutegroup.com/news/general/study-finds-that-china-is-still-a-key-dod-supplier/

https://www.orfonline.org/expert-speak/china-s-export-denial-strategy-against-india-a-national-security-challenge

https://economictimes.indiatimes.com/news/economy/foreign-trade/not-just-cctvs-indian-security-checks-may-soon-be-expanded-to-cover-many-other-items-from-china/articleshow/113870657.cms?from=mdr

https://www.ispionline.it/en/publication/indias-latest-move-to-de-risk-its-military-from-china-143085

The Geopolitics of Maps: China's Silent Cartographic Aggression & Battlefield

Jaideep Agarkar

Abstract

This article examines China's strategic use of cartography as a geopolitical tool and instrument of territorial projection— a term well recognized as cartographic warfare. By examining historical precedents, technical advancements, and contemporary geopolitical uses, this research outlines how map production is utilized by China as an instrument to justify territorial claims, construct international opinions, and legitimize internal nationalist narratives. In addition, the article provides a balanced view of the implications of China's cartographic interventions in India, specifically in reference to border skirmishes and regional stability. Based on these findings, it puts forth an integrated policy agenda for India, with preference for development of geospatial intelligence, countering cartographic disinformation, and drawing upon historical cartographic records in strategic diplomatic initiatives. This article offers a critical perspective on the universal ramifications of cartographic aggression in international geopolitics and highlights the imperative of an integrated response towards burgeoning threats in the geospatial space.

Colonel **Jaideep Agarkar** is Senior Fellow at the Centre for Land Warfare Studies (CLAWS), New Delhi. Views expressed are personal.

Introduction

Maps have historically been acknowledged as essential tools for military strategy and statecraft. The development of cartography from ancient maps to contemporary digital overlays, illustrates not only technological advancements but also the shifting dynamics of power, identity and territorial governance (Chapman, 2025). In recent decades, China has increasingly leveraged cartography as a strategic tool for both hard and soft power (Anand, 2023). China has effectively used this approach to assert extensive territorial claims, shape international discourse and strengthen domestic cohesion. Commonly referred to as "cartographic warfare," this practice represents a significant aspect of modern geopolitical competition and China offers the best example of Whole of Nation Approach (WONA) being leveraged towards achieving its desired results. China utilises all available tools at its disposal to wage all forms of warfare (akin to Sam Daam Dand Bhed….) to achieve its national aim.

This article provides an analysis of China's use of weaving a narrative and exploiting cartography. It examines the historical development of Chinese cartographic practices, integration of digital technologies into military doctrine and the role of cartographic propaganda in shaping national/international narratives. How China incorporates its 'Three War Strategy' coupled with its cyber prowess to shape the narrative, both for the Domestic and International audience, under an overarching central guidance. The discussion is framed within a broader strategic context, drawing upon perspectives from international relations and strategic studies. Finally, practical policy implications for India are explored, offering recommendations for enhancing India's geospatial capabilities and addressing external cartographic aggression.

Cartography and War

War is always spatial (Raleigh et al., 2010). Therefore, cartography is one of the most important tools of war (Specht, 2024). For a long

time, armies warred with very few maps, if at all, relying instead upon mental maps or local conductors. The modern cartography-military relationship appeared in its first strong manifestation during the early modern period (Craib, 2000) when war and cartography grew closely interlinked under pressures from protracted wars and novel war techniques (artillery)—not merely supporting but acting as the principal stimulus for cartographic development (Branch, 2014). The development of military strategy, which eventually became the science of warfare itself, further advanced the education of officers in map reading and map-making. A major turning point in this respect was the early 18th century when military academies started putting surveying and map drawing in their curriculum—an extremely important step for military cartography to begin as a subdivision of cartography, concerned solely with the production of maps for military purposes (Chatterjee, 2021). An even tighter mapping-warfare relationship was introduced in the 19th century when dedicated national mapping agencies were set up in front of military forces (Edney, 2020). Further requirements of warfare cartography were felt through military demands in the 20th century (Schneider, 2017). Major developments in mapping for military purposes took place during World Wars I and II not only technically (due to the application of aerial imagery) but also concerning mapping specialization targeting trench warfare, air combat and naval warfare (NYPL Staff, 2015). Although military cartography in World War I consisted largely of national productions with diverse scales, map projections and measurement units, the global character of World War II favourably contributed to a unification of various geodetic and cartographic sign systems into one international standard. Through the application of photogrammetry and satellite imagery during the Cold War, quick mapping was facilitated, thus producing uninterrupted global coverage at medium scale (Cloud, 2002). In the late 20th century, significant transformations in military cartography

and mapping occurred, caused by the digital revolution (Garcia, 2024), the emergence of digital imagery, satellites and GIS technology.

Historical Context and Evolution of Chinese Cartography

Cartography in China has a long history (Yee, 2008). Early Chinese maps, such as those from the Han dynasty, served as navigational aids, administrative tools and resources for military planning (Powell, 2024). Imperial surveys and detailed territorial records supported state governance, allowing rulers to manage extensive and varied territories. The focus on precise measurement and geographic detail in early Chinese cartography facilitated its use in state functions, including defence and strategic planning.

During periods of territorial expansion, Chinese maps were used to delineate borders and plan military campaigns. The detailed nature of these early surveys demonstrated an emphasis on empirical observation and accuracy—qualities that still influence Chinese cartographic practices today. This historical basis is essential for understanding the current development of cartographic strategies in China (Lin, 2022).

In contemporary times, Chinese cartography has experienced substantial transformation due to technological advancements and evolving strategic priorities. The incorporation of Geographic Information Systems (GIS), satellite imagery and digital mapping platforms has drastically improved the methods for collecting, analyzing and distributing spatial data (Niraj, 2016). Modern Chinese mapping capabilities are now integrated into a comprehensive framework that facilitates real-time decision-making, operational planning and long-term strategic forecasting (Zhang et al., 2021).

China's state institutions and military have allocated significant resources to geospatial technologies, thus recognizing their importance in contemporary warfare. This advancement is highlighted by the creation of sophisticated mapping platforms that integrate high-resolution imagery

with real-time data feeds, providing a dynamic, three-dimensional view of the battlefield. These systems play a key role in both tactical operations and strategic communication and diplomatic efforts (Leipnik et al., 2011). With the launch of its International Space Station, hordes of satellites catering to its own homegrown GPS, China has come a long way and it has now started expanding its survey footprint even for oceanic and sub oceanic regions. This is enabling China to map the underwater areas and also find out the minerals/natural resources available in the area so as to enable creation of an historically aligned narrative for laying claims and owning the territories and associated territorial waters.

Strategic Use of Maps in Chinese Policy

Central to China's cartographic strategy is the intentional use of maps to assert territorial claims (Gupta, 2023). Maps produced by the Chinese state often incorporate historical narratives that extend traditional Chinese borders beyond those recognized by international law (Kothari, 2024). This practice is not merely technical but ideologically motivated. By presenting a version of history, in which China's territorial expanse appears both natural and legitimate, these maps function as tools of state policy (Erksine, 2018).

Chinese cartographic practices extend beyond simple territorial claims; they also play a significant role in the country's soft power strategy. Maps are extensively distributed through official publications, educational materials and digital platforms consistently depicting a unified and expansive China. This cartographic narrative is intended to instil national pride and support the government's strategic policies.

By aligning historical memory with modern territorial claims, China employs cartography to project an image of continuity and legitimacy. These representations are essential in garnering domestic support and fostering a sense of unity among the population. Additionally, they serve as a subtle yet effective means of shaping international perceptions,

challenging alternative narratives and asserting China's status as a prominent regional power.

Modern Chinese doctrine incorporates advanced digital mapping technologies as a fundamental component of operational planning (Zhang et al., 2021b). These systems synthesize data from satellites, unmanned aerial vehicles (UAVs) and other sources to generate a real-time, high-resolution battlefield picture (Quamar et al., 2023). This integration extends beyond tactical applications, reinforcing the strategic objectives of maintaining territorial integrity and asserting regional dominance.

China employs various cartographic techniques that result in map distortions, affecting both domestic and international perceptions. These cartographic practices not only affect navigation and geographic understanding within China but also have broader geopolitical implications, as they shape perceptions of territorial extents and sovereignty. Here are some notable examples:

- **GCJ-02 Coordinate System ("Mars Coordinates"):** China mandates the use of the GCJ-02 geodetic datum for all domestic mapping services. This system introduces intentional shifts to latitude and longitude, leading to discrepancies between actual GPS coordinates and their representation on Chinese maps. This practice aims to enhance national security but results in significant misalignments when comparing Chinese maps to global standards. For instance, locations plotted using standard GPS coordinates can appear offset by 100 to 700 meters on Chinese platforms.
- **Misrepresentation of Territorial Boundaries:** Chinese maps often depict disputed regions as unequivocally belonging to China, influencing both domestic and international audiences. For example, the "nine-dash line" in the South China Sea is prominently featured in Chinese maps, asserting claims over vast maritime areas also claimed by other nations. Similarly, regions like Arunachal Pradesh are shown

as part of China, contradicting Indian claims. These cartographic representations serve to reinforce China's territorial assertions.

- **Distortions at the Hong Kong–Mainland China Border:** At the border between Hong Kong and Mainland China, map distortions are quite evident. Satellite imagery may align correctly, but road networks and other features often appear misaligned or disconnected due to the imposed coordinate shifts. This discrepancy can cause confusion, especially in cross-border regions where accurate navigation is crucial.

Case Study: Cartographic Disputes along the Line of Actual Control (LAC)

A key point of contention in current Sino-Indian relations is the disagreement over the Line of Actual Control (LAC) in the Himalayan region (Mehta, 2023). Unlike well-defined international borders, the LAC suffers from ambiguity and absence of mutually agreed-upon markers (Singh, 2020). This lack of clarity has enabled China to promote differing cartographic interpretations that bolster their respective territorial claims.

Cartographic differences along the Line of Actual Control (LAC) highlight the use of maps in territorial disputes. Official maps from India and China show variations in boundary delineations. Indian maps typically emphasize historical survey data and internationally recognized boundaries, whereas Chinese maps often incorporate historical narratives that include disputed areas such as Aksai Chin and Arunachal Pradesh.

These disparate mapping techniques are deliberate instruments meant to affect perceptions rather than only being technical differences. China's narrative of historical entitlement and regional dominance is reinforced by the use of maps that enlarge its territorial claims. On the other hand, addressing these narratives for India calls for the production of authoritative, understandable maps grounded in historical precedent and empirical data.

The cartographic dispute along the LAC has significant strategic implications (Shinde, 2024). Different mapping interpretations not only increase tensions on the ground but also make diplomatic negotiations more complex. Each side uses its cartographic narrative to justify military deployments and mobilize public support.

The LAC's ambiguity permits quick escalation since, even if it has mutually agreed-upon safeguards, varying interpretations frequently result in miscommunications and standoffs. The LAC conflict highlights the importance of precise and open cartography for India. Addressing Chinese claims and reaffirming India's territorial integrity require the development of an authoritative mapping narrative. To support India's viewpoint, this calls for meticulous mapping techniques as well as incorporation of extensive historical and empirical data. The LAC case also emphasizes the importance of multilateral participation, where issues can be resolved with aid of international boundary consensus and independent verification.

Comparative Analysis: Cartographic Warfare in the Contemporary Geopolitical Landscape

China's use of cartography can be viewed within the context of modern strategic competition. In an era marked by hybrid warfare—where information operations, cyber capabilities and conventional military forces intersect—maps have become important tools for power projection and strategic influence.

China's use of cartographic techniques is indicative of a larger movement among superpowers to strategically employ digital mapping and geospatial intelligence. China is not the only country that uses maps as a strategic tool. Mapping systems are also used strategically by other nations. To enhance operational coordination and real-time situational awareness, for example, the United States and its allies invest heavily on digital mapping systems such as Ukraine's Delta system

(Bondar, 2025) and the Android Team Awareness Kit (ATAK) (Usbeck et al., 2015). In China's situation, however, use of maps to support historical assertions and shape national narratives is more obvious. Western mapping traditions, which represent a rules-based approach to cartography, emphasize technically precise boundaries and worldwide recognition. Particularly in disputed areas like the South China Sea, this divergence in cartographic ideology may have an effect on diplomatic discussions and regional security.

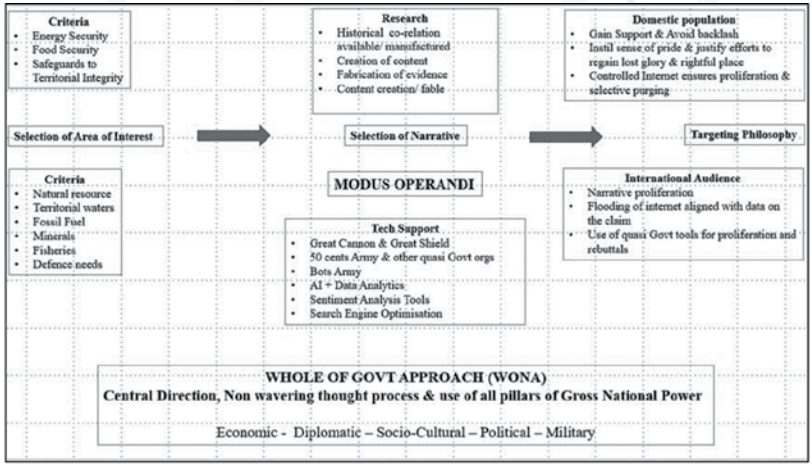
Modus Operandi of China: WONA at its best

An educated guess at deciphering the modus operandi for China and its use of Whole of Nation Approach can be described as below:

- **Selection of Area**. The area of interest is selected keeping in mind the need to fulfil Energy Security, Food Security and safeguard Territorial Integrity, hence areas that are rich in natural resources (fossil fuels, minerals etc.), increase claims on territorial waters (fishing and off shore drilling opportunities), offer good locations to place security outposts/ astride SLOCs for monitoring move of adversary/ provides adequate buffer to the mainland.
- **Selection of Narrative**. Once an area is selected, there is adequate research in the narrative building and creation of historical evidence/ co-relation (even though perceptional) leading to creation of content to match the claims.
- **Targeting Philosophy**. The target for China/CPC is clearly two folds—Domestic and International. First, the Domestic population is indoctrinated innocuously with narrative with an aim to get population support for the cause so as to ensure no backlashes. Moreover, closely controlled internet ensures that the population is only shown what it needs to see and contrarian views are blanked out/removed/purged. Near simultaneously, the international audience too gets targeted through a slow build up of narrative

and thereafter flooding the internet with data that is aligned to the claims. Here quasi Govt tools, such as 50 Cent Army, is used to ensure proliferation and rebuttal.

- **Technology to the fore**. Tech tools such as Satellites, UAVs, Ships, GIS tools etc., are used to qualify the claim; Bots to spread and block the claim and rebuttals respectively; AI tools to carry out analysis of proliferation of claim; Great Cannon and Great Shield used to block and disrupt contrarian views thus allowing only the supporting ones to proliferate. Use of sophisticated tools such as Search Engine Optimisation to augment the efforts to proliferate false narratives.
- **WONA**. All forms of warfare and tactics are employed—from pleasing to coercion, using the economic, political, cultural, social and diplomatic tools, are unleashed to gain traction on the claims with increased military presence in the area to legalise the claim. Military means generally start at transgressions to patrolling (with increased frequency making it new normal) to intimidation and finally resulting in annexation through use of force. Chinese Govt generally shows scant regards to international arbitration (as in case with Philippines) and uses its Gross National Power to avert any fallouts—a near perfect case of using WONA.



Modus Operandi: WONA at its Best

Policy Implications for India

Considering the importance of cartographic practices and use of mapping to assert territorial claims, there are several challenges and opportunities for India. The following policy recommendations aim to improve India's geospatial capabilities and address external cartographic narratives.

India can establish a national policy that outlines principles and practices related to cartography especially concerning maps with territorial claims. This policy should set standards for producing official maps and offer strategies to address misleading or inaccurate cartographic representations. It should also include procedures for monitoring global map circulation and taking appropriate diplomatic and legal actions when necessary.

A comprehensive public diplomacy campaign is crucial to inform both domestic and international audiences about India's legitimate territorial claims. This campaign could encompass strategic communication efforts that emphasize India's historical and legal perspectives on boundary issues and contradict unfounded claims with thoroughly documented evidence. Leveraging international seminars, publications and collaborations with global think tanks will serve to present and reinforce India's position convincingly. It is also time to leverage the Indian diaspora and certainly the power of internet proliferation in the most populous nation of the world.

India can utilise multilateral organisations and regional alliances to address cartographic discrepancies. India must work in collaboration with nations that have similar concerns regarding China's assertive strategies, thereby forming a coalition capable of presenting a unified stance in tackling these issues.

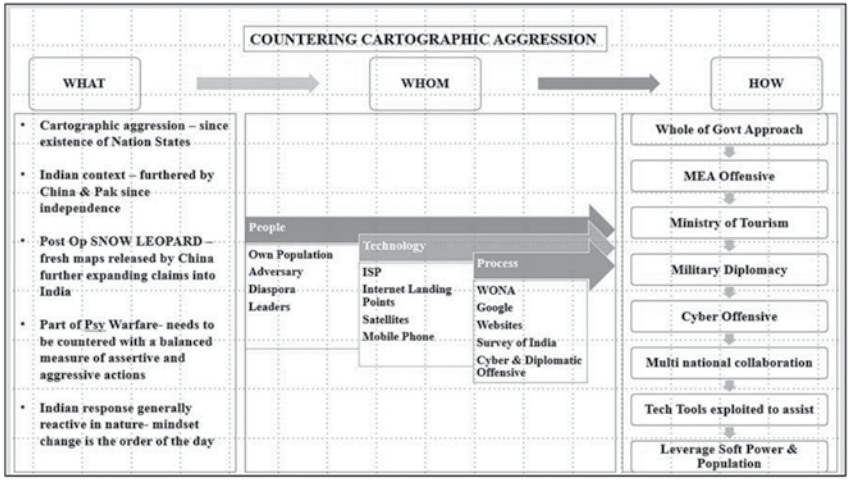
India could consider enhancing investment in geospatial research and data verification technologies to identify and contest any inaccurate cartographic claims promptly. This strategy includes leveraging artificial intelligence (AI) and machine learning (ML) capabilities to monitor and scrutinize cartographic content disseminated by various platforms. Furthermore, advanced satellite and drone technologies can play a crucial role in providing precise mapping and evidence to counter false representations.

One of the most important means is documentation and it is an imperative to document transgressions/violations/patrolling activity etc. of PLA in any and all areas along the LAC. It is necessary to geotag and timestamp the activity. It would serve two purposes, one, as a repository and second, lend itself to data analytics to bring out trends and future predictions.

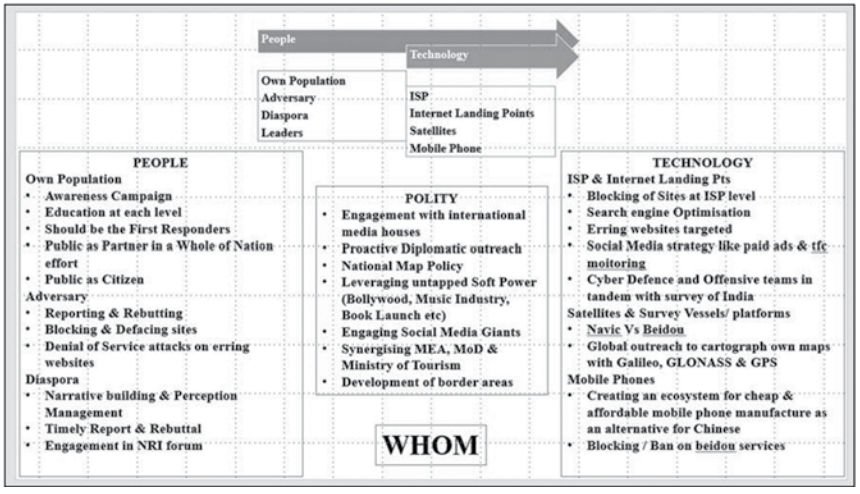
The use of cartographic tactics can influence military strategy, making it important for India to work with strategic partners who experience similar pressures. Joint exercises and intelligence-sharing agreements can enhance India's capacity to address information warfare and cartographic inaccuracies.

Forming specialized digital task forces dedicated to addressing misinformation and advocating for India's legitimate territorial maps is crucial. These teams should focus on identifying and correcting inaccurate maps distributed online, conducting thorough fact-checking and issuing counter-statements in both English and regional languages. Additionally, developing mobile applications and web platforms that provide users with accurate maps, information on India's official positions and mechanisms for reporting discrepancies, will enhance the country's efforts to counteract false narratives effectively.

Strategy of What – Whom – How to counter Chinese Cartographic Aggression



Action on People & Technology



Actionable Points for WONA from Indian perspective

- All ministries and Govt apparatus to be involved in countering.
- Cutting across political party lines, aligning of views in support of national cause.
- Proactive diplomatic outreach.
- Engagement with international media.
- Timely detection and reportage of misrepresented/distorted maps.
- Exploiting cartographic discourse on social media.
- Dedicated cyber team for proactive response be made available to Survey of India.
- Populate/Flood correct version of the maps on internet.
- Target the cartographic dispute of adversarial countries with other nation states.
- Leveraging adversaries' disputes with other countries and forming an e-association to counter cartographic aggression.
- The Ministry of Tourism to flood the internet with advertisements having correct cartographic data and promote tourism of such areas to ensure presence and legitimise claims.
- All Indian visas to have watermarked maps.
- All delegations/international guests be presented with Map based souvenirs.
- Military Diplomacy to be leveraged for propagating cartographic correctness.
- Strong Military presence at the Areas of Interest/Disputed sites to counter/deter any adventurism—Strength respects Strength.
- Create and publish an accurate database of any and all transgressions in the areas claimed by us. These events to be properly geo-tagged, geo-referenced and time stamped to be utilised as a data set for analytics and future course predictions.
- Leverage the vast diaspora and embassy offices to give out the correct perception.

- Leverage the status of being the second largest internet facing population.
- Leverage good relations with tech giants and tech superpower countries.
- Soft Power : Music, Videos, Movies, Books, Art & Concerts to be leveraged.
- Learn best practices from China to counter its narrative.
- Setting up of Cyber Task Force at the national level to ensure proper and commensurate response utilising tools such as Search Engine Optimisation, Artificial Intelligence, Data Analytics etc.

Conclusion

The progression of cartography from ancient hand-drawn maps to advanced digital overlays highlights the lasting significance of maps as tools for warfare and statecraft. In the contemporary strategic landscape, digital mapping systems such as Ukraine's Delta and the US military's ATAK exemplify the essential role that real-time geospatial intelligence plays in operational planning and decision-making. Concurrently, China's use of cartographic tactics—illustrated by its extensive territorial claims and the symbolic application of the nine-dash line—demonstrates that maps are powerful instruments of geopolitical influence and propaganda which becomes a potent tool when supplemented by the WONA.

These developments pose both challenges and opportunities for India. By improving its geospatial capabilities, addressing external cartographic influences and utilizing its historical background in mapping, India can enhance border security, operational coordination and strategic interests at regional and global levels. Investments in advanced mapping technologies, cybersecurity and educational programs are necessary for developing a strong geospatial infrastructure to meet the needs of modern warfare.

Additionally, through multilateral diplomatic initiatives and the promotion of precise, evidence-based cartographic narratives, India can counter any alternative territorial boundary representations and strengthen its claims over disputed regions. By incorporating emerging technologies such as AI, machine learning and augmented reality into mapping systems, India can further enhance its strategic capabilities, thus ensuring its position at the forefront of contemporary military innovation.

As the global strategic landscape evolves, the importance of maps in warfare and diplomacy continues to grow. China's practice of cartographic warfare demonstrates the power of maps as tools for navigation, operational planning, national identity and geopolitical influence. For India, it is essential to harness modern geospatial intelligence and counter external cartographic narratives to secure its strategic interests and position itself as a leader in the field of cartographic and digital warfare given the fact that India, being a peace loving nation, is non-hegemonistic in its dealings with its neighbouring nations.

References

Bondar, K. (2025). *Does Ukraine already have functional CJADC2 technology?* CSIS. Accessed from: https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology. Accessed on February 10, 2025.

Branch, Jordan. (2014). The Cartographic State. *Cambridge.*

Chapman, K. (2025, January 9). *The history of cartography: From ancient maps to Google Earth.* Earth Site Education. Accessed from: https://www.earth-site.co.uk/Education/the-history-of-cartography-from-ancient-maps-to-google-earth/. Accessed on February 08, 2025.

Chatterjee, B. (2021). Founding Empire: James Rennell and the Eighteenth-Century Survey of British Bengal. *XVII-XVIII*, *78.* Accessed from: https://doi.org/10.4000/1718.8375. Accessed on February 08, 2025.

Cloud, J. (2002). American Cartographic Transformations during the Cold War. *Cartography and Geographic Information Science*, 29(3), 261–282. Accessed from: https://doi.org/10.1559/152304002782008422. Accessed on February 08, 2025.

Craib, R. B. (2000). Cartography and Power in the Conquest and Creation of New Spain. *Latin American Research Review*, 35(1), 7–36. Accessed from: http://www.jstor.org/stable/2692056. Accessed on February 09, 2025.

Edney, M. (2020, November 6). *The growth of map history in the nineteenth century*. Mapping as Process. Accessed from: https://www.mappingasprocess.net/blog/2020/11/6/the-growth-of-map-history-in-the-nineteenth-century. Accessed on February 08, 2025.

Erskine, John. (2018, July 11). *Politics and Cartography: The Power of Deception through Distortion*. Carnegie Council. Accessed from: https://www.carnegiecouncil.org/media/series/ethics-online/politics-and-cartography-the-power-of-deception-through-distortion. Accessed on February 09, 2025.

Garcia, L. (2024, September 26). Cartography in the Digital Age: Evolution and applications of modern mapping techniques. *Geoinformatics & Geostatistics: An Overview*. Accessed from: https://www.scitechnol.com/peer-review/cartography-in-the-digital-age-evolution-and-applications-of-modern-mapping-techniques-OwmH.php?article_id=26529. Accessed on February 08, 2025.

Gupta, S. (2023, September 2). View: New China map signals Xi's assertion over Asia. *Hindustan Times*. Accessed from: https://www.hindustantimes.com/analysis/new-china-map-signals-xi-s-assertion-over-asia-101693625253928.html. Accessed on February 09, 2025.

Kothari, N. (2024, March 30). Maps as Weapons: Legal implications of territorial claims. *Oxford Political Review*. Accessed from: https://oxfordpoliticalreview.com/2024/03/30/maps-as-weapons-legal-implications-of-territorial-claims/. Accessed on February 09, 2025.

Leipnik, M. R., Ye, X., & Gong, G. (2011). Geo-spatial technologies and policy issues in China: status and prospects. *Regional Science Policy & Practice*, 3(4), 339–356. Accessed from: https://doi.org/10.1111/j.1757-7802.2011.01047.x.

Lin, G. (2022). Using ancient maps to examine historical changes in China's territory and concept of territory. *Journal of Chinese Humanities*, 8(3), 322–338. Accessed from: https://doi.org/10.1163/23521341-12340139.

Niraj. (2016, May 13). China geospatial industry – The flight of the dragon. *Geospatial World*. Accessed from: https://geospatialworld.net/article/china-geospatial-industry-the-flight-of-the-dragon/. Accessed on February 08, 2025.

NYPL Staff. (2015). The Great War and Modern Mapping: WWI in the Map Division. *New York Public Library*. Accessed from: https://www.nypl.org/blog/2015/05/15/wwi-map-division. Accessed on February 08, 2025.

Powell, Eric. (2024, November 20). Mapping the Past - Han Dynasty Map. *Archaeology Magazine*. Accessed from: https://archaeology.org/issues/may-june-2019/collection/maps-china-han-dynasty-topographic-map/mapping-the-past/. Accessed on February 08, 2025.

Quamar, M. M., Al-Ramadan, B., Khan, K., Shafiullah, M., & Ferik, S. E. (2023). Advancements and Applications of Drone-Integrated Geographic Information System Technology—A Review. *Remote Sensing*, 15(20), 5039. Accessed from: https://doi.org/10.3390/rs15205039. Accessed on February 09, 2025.

Raleigh, C., Witmer, F. D. W., & O'Loughlin, J. (2010). The Spatial Analysis of War. *Oxford Research Encyclopedia of International Studies*. Accessed from: https://doi.org/10.1093/acrefore/9780190846626.013.485. Accessed on February 08, 2025.

Schneider, Ute. (2017). Maps, Geography and the Representation of Space. *International Encyclopaedia of the First World War*. Accessed from: encyclopedia.1914-1918-online.net/article/maps-geography-and-the-representation-of-space/?format=pdf. Accessed on February 08, 2025.

Shibani, Mehta. (2023). *Impasse at the LAC: An examination of the 2013, 2014 and 2015 standoffs*. Carnegie Endowment for International Peace. Accessed from: https://carnegieendowment.org/research/2023/08/impasse-at-the-lac-an-examination-of-the-2013-2014-and-2015-standoffs?lang=en. Accessed on February 09, 2025.

Shinde, Ved. (2024). *Cartographic aggression: Playing it the China way*. Lowy Institute. Accessed from: https://www.lowyinstitute.org/the-interpreter/cartographic-aggression-playing-it-china-way. Accessed on February 09, 2025.

Singh, S. (2020, July 10). Galwan incident leads to more calls for early delineation of LAC. *The Indian Express*. Accessed from: https://indianexpress.com/article/india/galwan-incident-leads-to-more-calls-for-early-delineation-of-lac-6498605/. Accessed on February 09, 2025.

Specht, Doug. (2024, 10 April). *Mapping the Unmappable: Cartography at War*. Living Maps Network. Accessed from: https://www.livingmaps.org/mapping-the-unmappable. Accessed on February 08, 2025.

Usbeck, K., Gillen, M., Loyall, J., Gronosky, A., Sterling, J., Kohler, R., Hanlon, K., Scally, A., Newkirk, R., & Canestrare, D. (2015). Improving situation awareness with the Android Team Awareness Kit (ATAK). *Proceedings of SPIE, the International Society for Optical Engineering/Proceedings of SPIE*. Accessed from: https://doi.org/10.1117/12.2180014. Accessed on February 10, 2025.

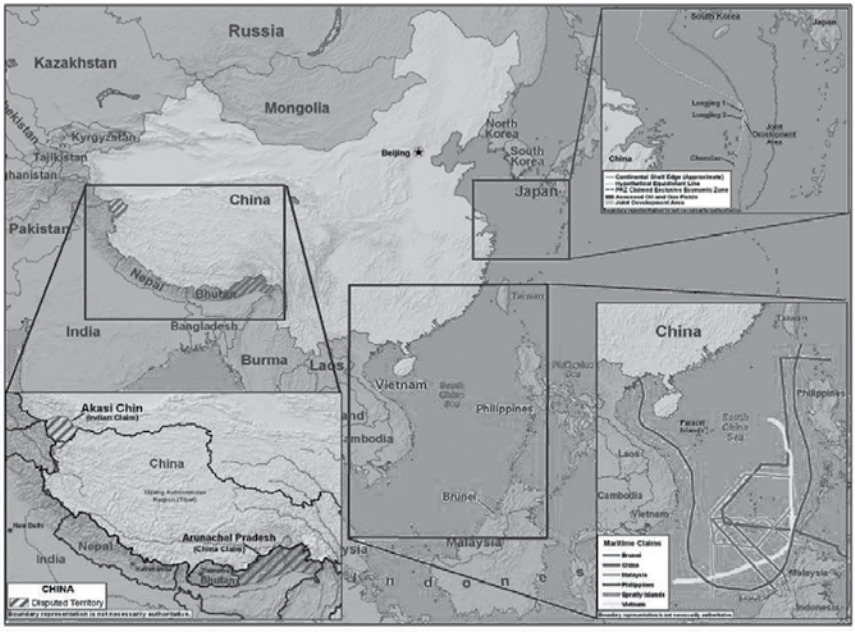
V. Anand. (2023, September 28). *A map to expansion: Understanding China's 'cartographic aggression.'* Frontline. Accessed from: https://frontline.thehindu.com/world-affairs/china-cartographic-aggression-back-to-playing-mind-games-with-maps-claiming-foreign-territories-as-its-own/article67298568.ece. Accessed on February 08, 20255.

Yee, C.D.K. (2008). Maps and Mapmaking in China. In: Selin, H. (eds) Encyclopaedia of the History of Science, Technology and Medicine in Non-Western Cultures. *Springer*. Accessed from: https://doi.org/10.1007/978-1-4020-4425-0_8721.

Zhang, J., Gu, H., Hou, W., & Cheng, C. (2021). Technical progress of China's national remote sensing mapping: from mapping western China to national dynamic mapping. *Geo-spatial Information Science*, 24(1), 121–133. Accessed from: https://doi.org/10.1080/10095020.2021.1887713.

Zhang, J., Gu, H., Hou, W., & Cheng, C. (2021b). Technical progress of China's national remote sensing mapping: from mapping western China to national dynamic mapping. *Geo-spatial Information Science*, 24(1), 121–133. Accessed from: https://doi.org/10.1080/10095020.2021.1887713. Accessed on February 09, 2025.


CHINESE TERRITORIAL DISPUTES
CURRENT DISPUTES
RESOLVED DISPUTES


Russia
Kazakhstan
Mongolia
Kyrgyzstan
Tajikistan
Beijing
North Korea
South Korea
Japan
China
Pakistan
Nepal
Bhutan
India
Bangladesh
Burma
Laos
Vietnam
Philippines
Brunei
Malaysia
Taiwan
Akasi Chin
(Indian Claim)
Arunachal Pradesh
(China Claim)
CHINA
Disputed Territory

China's territorial claims serve multiple purposes: strategic military positioning, control over natural resources, expanding influence over trade routes, and reinforcing historical narratives to strengthen national identity.

Name of the Country	Details of Territorial Dispute (Incl. Areas)	Benefits and Reasons for the Dispute
India	- **Aksai Chin** (occupied by China, claimed by India) - **Arunachal Pradesh** (claimed by China as "South Tibet") - **Doklam Plateau** (trilateral dispute with Bhutan, strategic for India)	- **Aksai Chin**: Strategic control for linking Xinjiang and Tibet. - **Arunachal Pradesh**: Water resources, buffer zone, and strengthening Tibet claims. - **Doklam**: Control over Siliguri Corridor (India's "Chicken's Neck").
Taiwan	- Claims Taiwan as a province under its "One-China Policy."	- Political control over a high-tech economy (TSMC & semiconductor industry). - Strategic dominance in the South China Sea.
Japan	- **Senkaku/Diaoyu Islands** in the East China Sea.	- Access to rich fishing grounds and potential undersea oil and gas reserves. - Strategic naval positioning against US-Japan alliances.
Philippines	- **Scarborough Shoal**, part of the South China Sea dispute.	- Dominance over South China Sea trade routes. - Military expansion and control over rich marine resources.
Vietnam	- **Paracel Islands** (controlled by China, claimed by Vietnam). - **Spratly Islands** (disputed).	- Control over rich fishing zones. - Oil and gas exploration rights.

Malaysia	- **Spratly Islands**, including features like Fiery Cross Reef and Mischief Reef.	- Extension of China's Exclusive Economic Zone (EEZ). - Strengthening the "Nine-Dash Line" claim over the South China Sea.
Brunei	- Overlapping **Exclusive Economic Zone (EEZ)** claims in the South China Sea.	- Energy resources and economic dominance over the region.
Indonesia	- **Natuna Islands EEZ dispute**, as part of the "Nine-Dash Line" claim.	- Access to oil and gas reserves. - Strengthening China's position in Southeast Asia.
Bhutan	- **Doklam Plateau** (also affects India). - Several other smaller border areas in western and central Bhutan.	- Strategic pressure on India. - Potential buffer zone expansion for Tibet.
Nepal	- Disputed border areas, including in Humla district.	- Gradual encroachment to expand influence. - Strategic presence along Nepal's borders.
Mongolia	- Implicit claim over "Inner Mongolia" as part of a greater "historical China."	- Soft power pressure over Mongolian politics and economy.
Kazakhstan, Kyrgyzstan, Tajikistan	- Historical claims to border regions based on old Qing Dynasty maps.	- Expanding influence in Central Asia for Belt and Road Initiative (BRI).
Russia	- Historic claims over Vladivostok and parts of Siberia (though settled, some Chinese maps still depict these regions as "lost territories").	- Long-term demographic and economic influence through migration and trade.

Global Operations of China's State Intelligence Ecosystem to Include MSS, Cyber Hubs, FWO, UFWD, Confucius Institutes and Implications for India

Nayyer Siddiqi

Abstract

China's Communist Party (CCP)-controlled intelligence network operates to maintain domestic control while simultaneously increasing its international reach. This complex system of government agencies, military departments and covert operations enables China to conduct extensive espionage operations, cyber attacks and strategic influence campaigns. The Ministry of State Security (MSS), Intelligence Bureau of the People's Liberation Army (PLA) and the United Front Work Department (UFWD) stand out as most vital organisations. The organisations have distinct responsibilities which work together to support the overall mission. China's influence extends beyond the realm

Colonel **Nayyer Siddiqi** served as a platoon commander in the Indian Military Academy and Instructor in Gunnery in School of Artillery, Devlali and is Former Military Observer & a Staff Officer in Military Observer's Regional Headquarters in United Nations Mission in the Democratic Republic of Congo (MONUSCO). Views expressed are personal.

of traditional intelligence operations. China is responsible for cyber attacks against countries of Southeast Asia, while Confucius Institutes are working to propagate Chinese culture in other parts of the world. International operations of these organisations focus on shaping the elites and institutions of the world. China's activities pose significant threats to India's national security together with its economic resilience and diplomatic power because of their shared border disputes and competing regional interests. This paper examines China's intelligence structure, worldwide operations and their effects on India together with possible Indian strategic responses. The article aims to deliver a comprehensive evaluation of Chinese intelligence structures and their effects on Indian national interests.

Ministry of State Security

The Ministry of State Security of China was founded in 1983 as the main civilian intelligence agency of the nation. The organisation's main duties include protecting the political security of the Chinese Communist Party (CCP), foreign intelligence collection and domestic espionage defence. The MSS operates from its main headquarters in Beijing with an estimated 100,000-strong workforce and extensive regional office network.[1] Since Xi Jinping became President in 2012 the MSS has functioned with greater independence while following his government centralisation policies. The MSS functions as a key force in cyber operations and overseas opposition suppression by monitoring foreign entities which pose risks to national stability for the broader goals of the CCP.

Operational capabilities and historical activities of espionage executed by the primary functional divisions of the MSS

Human Intelligence (HUMINT) Operations Abroad: MSS operatives disguise themselves as diplomatic personnel, journalists and corporate officials to obtain foreign intelligence through State Owned Enterprise

covers.[2] The 2023 Australian inquiry revealed MSS efforts to influence local politicians which constituted direct foreign intelligence gathering.[3] MSS linked operations targeted the acquisition of foreign technology and intellectual property. Germany removed suspected MSS agents from its territory in 2022 as they were suspected of conducting illegal technology acquisition activities.

Counter Espionage

MSS executes counter espionage duties while monitoring CCP threats and takes steps to neutralise them. MSS implemented a national reporting system which included both a hotline and website for citizens to identify possible foreign spies and collaborators. The MSS expanded its surveillance capabilities through an innovative crowd sourced program that relied on state support for counter espionage operations beyond conventional institutions.

Cyber Espionage

Moderna COVID-19 Data Theft (2020): The MSS faced accusations for stealing vital COVID-19 vaccine research information during the worldwide health crisis.

US Sanctions Case (2024): The MSS operated front company received US sanctions because it implanted malware in essential national infrastructure.[4]

Advanced Persistent Threat (APT), APT10 and APT41[5]: MSS supports these groups which perform complex cyber attacks including supply chain attacks and zero-day exploits against industries throughout North America, Europe and Asia.

Political Espionage

Australia faced MSS attempts to influence local politicians who would adopt China-friendly positions through influence operations. The MSS

demonstrated its efforts to disrupt democratic institutions through foreign policy manipulation. In Europe, MSS operatives have been linked to espionage cases involving technology transfers, with Germany expelling suspected agents in 2022.[6]

Transnational Espionage

Surveillance of Overseas Chinese Communities: The MSS uses threats and coercion to monitor discussions about sensitive political matters including Tibet, Xinjiang and Hong Kong across all territories including China.

Global Propaganda and Recruitment Campaigns: The MSS uses international propaganda activities to promote CCP ideological loyalty while shaping both domestic and foreign Chinese public perception.

People's Liberation Army Intelligence Bureau

The People's Liberation Army (PLA) Intelligence Bureau was previously known as the Second Department (2PLA) of the PLA General Staff Department (GSD). It is currently located within the Joint Staff Department of the Central Military Commission—the highest military body in China and is responsible for the military intelligence of China's armed forces. It was reorganised in 2016 to include the Information Support Force and the Cyberspace Force. It specialises in signals intelligence (SIGINT), cyber operations and human intelligence (HUMINT) to improve military modernisation and regional dominance.[7] The bureau, with an annual budget of $15 billion, focuses on defence technologies, personnel deployments, and geopolitical policies in the Asia-Pacific and South Asian regions.[8]

PLA cyber teams performed advanced attacks through the 2021 Microsoft Exchange Server breach wherein APT31 was linked to while affecting thousands of organisations worldwide.[9] Underwater gliders operated by the PLA were detected in Indonesian waters during 2020 while

conducting maritime intelligence collection for South China Sea conflict purposes.[10] Hence, the Chinese government shows its commitment to dominate regional security through strategic use of cyber and physical assets.

The agency shows ability to attract foreign assets—the case of a Singaporean engineer who transmitted naval intelligence to PLA operatives during 2019, is an apt example.[11] PLA recruiters operating in the United States have targeted defence firms through their attempts to steal aeronautical technology which became apparent in 2020.[12] The PLA Intelligence Bureau operates differently from the MSS because it prioritises military objectives while expanding its dual-purpose technology like AI and Quantum Computing interests by working with universities and tech companies through civilian fronting organisations.[13]

This military-civil fusion approach enhances the PLA's global influence facilitating access to advanced research through academic collaborations. The PLA's emphasis on border surveillance, missile systems and regional alliances presents direct threats to us especially along the Line of Actual Control (LAC), where information collection entails strategic planning.

United Front Work Department

The United Front Work Department (UFWD) operates under the Central Committee of the Chinese Communist Party and performs influence operations to make Non-Party entities, such as expatriate communities religious organisations and global elites, to support Beijing's goals. The UFWD controls operations from a $2.6 billion budget while managing a vast network of front organisations including cultural associations, media outlets and business councils, to shape narratives and acquire intelligence.[14] The organisation conducts international operations to advance CCP priorities through the Belt and Road Initiative while suppressing opposition regarding Taiwan, Hong Kong and Human Rights concerns.

The UFWD funded organisations in Canada ran political campaigns during 2022 to advance China-friendly policies which resulted in

government investigations about foreign interference.The UFWD has successfully infiltrated Australian community organisations through its agents who used diaspora networks to monitor dissidents and shape local political developments. The UFWD also supports academic research programs in order to shape global perceptions about China's worldwide standing.

The UFWD agents disguise themselves as diplomats or cultural representatives to control governments of countries which heavily rely on Chinese investment in South Asia. They also operate programs in Nepal and Sri Lanka and combines infrastructure development with intelligence gathering from local elite groups. Through its secret integration into open societies, the UFWD leverages democratic liberties to become a hidden yet all-pervasive intelligence tool.

The organisation uses its Confucius Institutes arm to expand its reach by combining cultural outreach programs with intelligence gathering activities. The UFWD's surveillance of diaspora populations and Northeast Indian ethnic groups creates political fragmentation that requires immediate countermeasures.

Comparison of China's MSS, PLA Intelligence Bureau, and UFWD

Aspect	**Ministry of State Security (MSS)**	**PLA Intelligence Bureau (Joint Staff Department)**	**United Front Work Department (UFWD)**
Organisational Structure	Civilian intelligence & security ministry under the State Council. Reports to top CCP organs and operates across the country through local bureaus.	Military intelligence arm of the PLA, under the Joint Staff Department of the Central Military Commission. Formerly known as the Second Department (2PLA).	Department under the CCP Central Committee dedicated to united front political work. Coordinates influence and outreach, including diaspora affairs.

Main Functions	Conducts foreign espionage, counter-intelligence, and regime protection. Monitors dissidents and internal threats. Engages in covert global operations.	Collects and analyzes foreign military information. Manages spy networks and supports defence strategy and early warning.	Implements political influence operations. Gathers intelligence on elites and co-opts influential groups domestically and abroad.
Primary Targets	Targets both domestic dissidents and foreign governments, intelligence services, and tech sectors.	Targets foreign military and defence institutions. Limited domestic role except within military security.	Targets individuals and groups outside the Party, including overseas Chinese, minorities, and foreign influencers.
Operational Methods	Employs spy networks, informants, cyber operations, and secret police powers including detention and interrogation.	Uses military attachés, covert operatives, and coordinates with technical intelligence units for analysis.	Operates through front organisations and alliances. Uses persuasion, co-optation, and narrative influence.

Source: Author's Conceptualisation.

Cyber Hub Activities in Southeast Asia

MSS and PLA units of China executes cyber operations in Southeast Asia through the region's economic links and weak cyber security to support Beijing's political goals. State-sponsored groups including Mustang Panda, RedDelta & APT31 conduct cyber attacks against government networks and vital infrastructure and private enterprises across ASEAN to gather political, military and economic intelligence.[15]

The Indonesian government, revealed in 2021, that 11 government institutions including the State Intelligence Agency suffered cyber attacks from Chinese hackers who sought marine policy information.[16] The Philippines faced continuous defence system attacks because of South China Sea territorial disputes which exposed naval communication weaknesses in 2023.[17] RedDelta launched attacks on Vietnamese state-

owned companies in 2020 to steal information about Belt and Road projects which demonstrated China's interest in economic espionage.[18]

The energy and telecommunications sectors of Malaysia and Thailand have experienced incursions from Chinese hackers who targeted both economic assets and dissident surveillance.[19] A 2022 Malaysian investigation confirmed that Chinese-affiliated entities stole 5G technological data which demonstrated China's expansionist goals in digital infrastructure.[20] The cyber hubs utilise advanced tactics including supply-chain attacks, zero-day vulnerabilities and AI-enhanced phishing because ASEAN member states maintain insufficient cyber security systems.[21]

Physical intelligence supports these initiatives as Chinese surveillance drones were detected in Malaysian waters in 2023 and underwater sensors were found in Philippine territory in 2024.[22] China's control over Southeast Asian cyber and maritime domains weakens ASEAN solidarity while pushing against Indian influence in the Indo-Pacific region.

Intelligence Activities of Confucius Institutes around the World

Since their founding in 2004, Confucius Institutes (CIs) have operated as institutions of the Ministry of Education's Hanban (now Chinese International Education Foundation) which promotes Chinese language and culture through more than 550, across 180 countries and are located within universities.[23] The UFWD monitors CIs to assess their intelligence collection and propaganda activities while using academic access to advance CCP goals. The Confucius Institutes function as CCP propaganda outlets which prevent discussions about Taiwan, Tibet and human rights as shown in the 2019 US Senate investigation. Senate investigation that revealed their threat to academic freedom.[24] The Australian disclosure of CI contracts revealed Beijing's authority to review both curriculum content and academic staff selection, thus compromising university

autonomy.[25] The Canadian intelligence agency viz. CSIS has identified CI personnel who possess MSS connections while monitoring Chinese students and obtaining information about host university operations.[26]

The Swedish government ended all Confucius Institutes in 2020 because of espionage concerns about technological development, and Germany followed suit in 2023.[27] Thailand operates 16 CIs throughout Southeast Asia which promote CCP narratives while monitoring local elites and expatriate populations.[28] The governments of Malaysia and Indonesia have strengthened their oversight because they recognize the risks of propaganda activities.[29]

India restricted Confucius Institutes in 2020 after the Ministry of External Affairs recognised their role in spreading propaganda.[30] The Western world has shut down more than 100 Confucius Institutes, however, these institutions continue their role as international intelligence assets while maintaining cultural programs.[31] Their dual purpose makes them an efficient tool for China to spread soft power and conduct intelligence operations.

Foreign Work Operations

China implements its overseas operations through MSS, PLA and UFWD and targets global elites, institutions and industries for CCP strategic objectives. The operations include economic espionage, political manipulation and technological theft which are carried out through front organisations, academic partnerships and diaspora networks.

The FBI documented more than 1,000 Chinese operations targeting US intellectual property since 2018 before a 2023 indictment showed MSS agents stealing semiconductor blueprints.[32] The Dutch conducted a 2022 investigation which discovered Chinese intelligence agents entering European IT companies by posing as academic researchers.[33] The Australian intelligence agency stopped a 2024 Chinese espionage operation that used consultant disguises to get defence contracts.[34]

Chinese companies linked to espionage activities have secured infrastructure contracts in Africa and Latin America as these regions emerge as strategic points. A Kenyan investigation from 2023 discovered that Chinese telecom infrastructure included monitoring systems which caused espionage concerns.[35] Brazil's space program suffered cyber attacks in 2024, which was later found to be linked to PLA-affiliated individuals who sought satellite technology acquisition.[36]

These operations take advantage of economic weaknesses by making investments to establish control. Chinese companies in South Asia have acquired port and railway contracts through which they inserted intelligence capabilities by presenting themselves as developers. The UFWD plays a vital role in establishing diplomatic ties with foreign elite groups to influence political decisions as shown by New Zealand's 2022 probe into Chinese political donations to politicians.[37]

Chinese investments in Indian technology and infrastructure create economic vulnerabilities which put the country at risk of espionage threats. The solution requires strict oversight together with international cooperation to dismantle China's global espionage networks.

Implications for India

The complex nature of the intelligence threat, China presents to India stems from territorial disputes, regional competition and economic vulnerabilities. The MSS, PLA, UFWD, and their cyber, cultural, and foreign operations endanger India's security, infrastructure, and social unity. India, therefore, must develop a complete response to defend national interests.

Political and Military Espionage

The MSS and PLA focus on understanding India's defence capabilities together with its missile systems and border policies. Indian intelligence discovered MSS operations, to infiltrate Tibetan exile organisations in

Dharamshala in 2018, wherein they targeted the Dalai Lama's activities.[38] PLA cyber teams conducted a 2022 cyber attack on India's defence ministry to steal LAC military placement information.[39] PLA surveillance capabilities, which included drones and SIGINT monitoring of Indian positions, became apparent during the 2020 Galwan confrontation as China demonstrated its goal to control border dynamics.

A 2023 report reveals how China has intruded into ISRO facilities which makes India's space and nuclear programs more vulnerable to risk.[40] The MSS has built its resources across Northeast India through ethnic conflicts to gather intelligence while destabilizing the region. These actions endanger both Indian territorial sovereignty and military readiness, hence, improved counterintelligence methods are essential.

Cyber Threats

The digital infrastructure of India faces threats from Chinese cyber operations. The power grid of India became vulnerable to sabotage through Chinese hacker malware in 2021 which increased fears about potential attacks during critical situations.[41] The unconfirmed 2020 Mumbai blackout sparked suspicions about Chinese involvement which revealed weaknesses in fundamental infrastructure systems. The Indian 5G expansion and fintech industry face espionage threats because Chinese companies including Huawei are suspected of installing backdoors.

A Chinese-affiliated group attacked India's banking system in 2024 to steal transaction data which demonstrated the risks of economic espionage.[42] The expected growth of India's digital economy to $1 trillion by 2030 makes the country more prone to cyber attacks, hence a robust cyber security regulation is required.

Influence Operations

Through its diaspora and Northeast community outreach, the UFWD exploits cultural and linguistic ties to acquire intelligence while spreading

CCP propaganda. The UFWD associated non-governmental organisations face investigations for financing activities against India including spreading false information about Kashmir. Chinese business entities, with a $100 billion trade value, control Indian elites through their relationships with corporate leaders who manipulate policy decisions.[43]

The restrictions on Confucius Institutes have driven UFWD agents to direct their efforts toward Indian academic institutions through funding research to shape perceptions about China's Asian position. The activities create national divisions among Indian citizens and destroy unity which requires public education campaigns to address this situation.

Regional Dynamics

The espionage activities of China throughout Southeast Asia and South Asia create additional problems for India to handle. Cyber attacks launched against ASEAN member states weaken India's Act East Policy by disrupting regional solidarity. The 2023 research evidence shows how China provides training to rebels in Kashmir and Northeast India through its intelligence-sharing partnership with Pakistan.[44]

The United Front Work Department's expansion to Nepal, Sri Lanka and the Maldives creates political separation from India while incorporating intelligence systems into vital ports through Chinese investments. The 2024 Hambantota Port agreement with Sri Lanka with Chinese surveillance features demonstrates these security risks.[45] The region needs India to take measures against such strategic actions.

Economic and Technological Espionage

International labour operations by Chinese companies target India's technology sector through data-stealing incidents in startup companies and IT facilities. The 2023 discovery revealed how Chinese spies, disguised as investors, tried to penetrate AI research operations in Bengaluru thus threatening India's technological leadership.[46] Surveillance device

integration alongside espionage concerns arises from Chinese investments in essential infrastructure that include ports and railways.

Indian dependence on Chinese supply chains, for electronics and medicines, makes India an easy target, as was made evident by the 2024 medical equipment supply chain attack.[47] The solution to these risks depends on establishing domestic manufacturing capabilities which will reduce external dependency.

Suggestions for Improving Security

To offset China's intelligence threats, India has to follow a thorough, multi-layered approach:

Improve counterintelligence: Use artificial intelligence-powered analytics to help the Research and Analysis Wing (RAW) and Intelligence Bureau (IB) track MSS, PLA, and UFWD agents. Regular audits of foreign-funded NGOs, academic programs, and enterprises can help to reduce covert influence.

Build homegrown 5G infrastructure: Apply cyber security criteria for vital industries including power, finance, and defence. Using real-time data analytics, public-private cyber defence hubs, similar to Israel's CyberSpark, can speed attack detection and response.[48] Though it requires quicker execution, India's 2023 cyber security strategy requiring zero-trust architectures is a step forward.[49]

Limit Cultural and Academic Activities: All Confucius Institutes must be shut down while Chinese academic partnerships need thorough examination to reveal institutional relationships. The government should support Indian cultural institutions like ICCR centres to develop competing regional perspectives against CCP propaganda.

Counter Foreign Employment Activities: A dedicated task force should monitor Chinese investments and corporate operations that focus on technology and infrastructure. The Indian government should adopt foreign direct investment restrictions similar to its 2020 amendment,

which requires Chinese investments to obtain official approval to reduce espionage threats. The exchange of intelligence about Chinese front firms should be conducted with international partners.

Regional alliances need strengthening: The Quad nations should increase their intelligence information exchange to monitor Chinese cyber and marine activities throughout the Indo-Pacific region. The 2024 India-Vietnam cyber accord should be expanded into bilateral agreements with ASEAN nations to check Chinese control in the region.[50]

Public awareness campaigns combined with resilience initiatives, should focus on both diaspora communities and Northeast regions while running national programs to educate people about cyber threats, UFWD strategies and false information. The society will gain strength through media and social channel revelations about Chinese influence operations.

Modernisation of Borders and Defence: The LAC should receive modern surveillance systems which combines AI-driven drones with satellites and sensor networks to counter PLA intelligence-gathering. The military should accelerate its modernisation process by developing cyber warfare capabilities and electronic countermeasures to fight hybrid threats. The $75 billion increase in India's 2024 defence budget enables the management of procurement delays while supporting this initiative.[51]

Economic Decoupling: The encouragement of home-based manufacturing of electronics, pharmaceuticals and vital technology should be done to offset Chinese supply chains. The 2024 Production-Linked Incentive program has a target of $100 billion in IT exports but needs faster implementation. The supply networks should be diversified through alliances with Japan and South Korea.

The implementation of these policies will assist us to counter Chinese intelligence risks and thus guarantee its sovereignty, economic independence and regional leadership. A proactive, coordinated strategy combining intelligence, technology, diplomacy, and public involvement is vital to offset China's several problems.

Notes

1. Mattis, P. (2019, January 17). *China's intelligence agencies: Reform and reorganisation*. Jamestown Foundation. https://jamestown.org/program/chinas-intelligence-agencies-reform-and-reorganisation/ Accessed on February 8, 2025.
2. Joske, A. (2022). *Spies and lies: How China's greatest covert operations fooled the world*. Hardie Grant.
3. Australian Broadcasting Corporation. (2023, June 12). "China's Influence Operations in Australia Uncovered." https://www.abc.net.au/news/2023-06-12/china-influence-operations-australia/102345678. Accessed on April 13, 2025.
4. U.S. Department of Justice. (2020, July 21)."Chinese Hackers Indicted for Targeting U.S. Vaccine Research." https://www.justice.gov/opa/pr/chinese-hackers-indicted-targeting-us-vaccine-research. Accessed on February 8, 2025.
5. Mandiant. (2023). "Advanced Persistent Threat Groups." https://www.mandiant.com/resources/apt-groups. Accessed on February 8, 2025.
6. Deutsche Welle. (2022, August 15). "Germany Expels Chinese Agents Over Espionage Concerns." https://www.dw.com/en/germany-expels-chinese-agents-over-espionage-concerns/a-62812345. Accessed on February 8, 2025.
7. Kania, Elsa B. (2023, March 15). "China's Military Intelligence in the Age of AI." Brookings Institution. https://www.brookings.edu/research/chinas-military-intelligence-in-the-age-of-ai/. Accessed on February 9, 2025.
8. Gertz, Bill. (2019). "Deceiving the Sky: Inside Communist China's Drive for Global Supremacy." New York: Encounter Books.
9. Microsoft Threat Intelligence Center. (2021, March 2). "Hafnium Targeting Exchange Servers." https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/. Accessed on February 10, 2025.
10. Reuters. (2020, December 31). "Indonesia Finds Suspected Chinese Surveillance Device in Waters." https://www.reuters.com/article/indonesia-china-surveillance/indonesia-finds-suspected-chinese-surveillance-device-in-waters-idUSKBN2950K8. Accessed on February 10, 2025.
11. The Straits Times. "Singaporean Jailed for Spying for China." (2019, August 10). https://www.straitstimes.com/singapore/courts-crime/singaporean-jailed-for-spying-for-china. Accessed on February 13, 2025.
12. U.S. Department of Justice. (2020, September 25). "Chinese Operatives Target U.S. Defence Contractors." https://www.justice.gov/opa/pr/chinese-operatives-target-us-defence-contractors. Accessed on February 14, 2025.
13. Fedasiuk, Ryan. (2021, June). "China's Military-Civil Fusion Strategy." Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/chinas-military-civil-fusion-strategy/. Accessed on February 15, 2025.
14. Brady, Anne-Marie. (2017). "Magic Weapons: China's Political Influence Activities Under Xi Jinping." Washington, DC: Wilson Center.

15. Insikt Group. (2021, August 12) "Chinese Cyber Espionage in Southeast Asia." Recorded Future. https://www.recordedfuture.com/chinese-cyber-espionage-southeast-asia/. Accessed on February 24, 2025.
16. Reuters. (2021, September 14). "Indonesia Says Government Networks Breached by Chinese Hackers." https://www.reuters.com/technology/indonesia-says-government-networks-breached-by-chinese-hackers-2021-09-14/. Accessed on February 26, 2025.
17. Center for Strategic and International Studies. (2023, April 20). "China's Cyber Operations in the Philippines." https://www.csis.org/analysis/chinas-cyber-operations-philippines. Accessed on February 13, 2025.
18. Mandiant. (2020, July 28) "RedDelta Targets Vietnam's Government." https://www.mandiant.com/resources/reddelta-targets-vietnam-government. Accessed on February 28, 2025.
19. Nikkei Asia. (2023, October 5). "Malaysia, Thailand Face Rising Chinese Cyber Threats." https://asia.nikkei.com/Politics/International-relations/Malaysia-Thailand-face-rising-Chinese-cyber-threats. Accessed on February 28, 2025.
20. The Star. (2022, December 10). "Malaysia Flags Chinese Cyber Espionage in 5G Sector." https://www.thestar.com.my/news/nation/2022/12/10/malaysia-flags-chinese-cyber-espionage-in-5g-sector. Accessed on February 19, 2025.
21. Insikt Group. (2021, August 12). "Chinese Cyber Espionage in Southeast Asia." Recorded Future.https://www.recordedfuture.com/chinese-cyber-espionage-southeast-asia/. Accessed on February 20, 2025.
22. The Star. (2023, March 15)."Malaysia Detects Chinese Surveillance Drone." https://www.thestar.com.my/news/nation/2023/03/15/malaysia-detects-chinese-surveillance-drone. Accessed on February 22, 2025.
23. Chinese International Education Foundation. (2023). "About Confucius Institutes." http://www.cief.org.cn/confuciusinstitutes/. Accessed on February 20, 2025.
24. U.S. Senate Permanent Subcommittee on Investigations. (2019, February 27). "China's Impact on the U.S. Education System." https://www.hsgac.senate.gov/subcommittees/investigations/hearings/chinas-impact-on-the-us-education-system. Accessed on February 24, 2025.
25. The Australian. (2019, August 14). "Confucius Institutes Under Scrutiny for Censorship." https://www.theaustralian.com.au/higher-education/confucius-institutes-under-scrutiny-for-censorship/news-story/1234567890. Accessed on February 26, 2025.
26. National Post. (2021, March 5). "CSIS Warns of Confucius Institute Espionage." https://nationalpost.com/news/csis-warns-of-confucius-institute-espionage. Accessed on March 1, 2025.
27. Reuters. (2020, April 21). "Sweden Closes All Confucius Institutes." https://www.reuters.com/article/sweden-china-confucius/sweden-closes-all-confucius-institutes-idUSKCN2231V8. Accessed on March 2, 2025.
28. Shullman, David, ed. (2021). "China's Influence in South Asia". Washington, DC: National Bureau of Asian Research.

29. Nikkei Asia. (2023, June 15). "Indonesia Tightens Oversight of Confucius Institutes." https://asia.nikkei.com/Politics/International-relations/Indonesia-tightens-oversight-of-confucius-institutes. Accessed on March 4, 2025.
30. The Hindu. (2020, July 30). "India Rejects Confucius Institutes in Schools." https://www.thehindu.com/news/national/india-rejects-confucius-institutes-in-schools/article32234567.ece. Accessed on March 6, 2025.
31. U.S. Senate Permanent Subcommittee on Investigations. (2019, February 27)."China's Impact on the U.S. Education System." https://www.hsgac.senate.gov/subcommittees/investigations/hearings/chinas-impact-on-the-us-education-system. Accessed on March 10, 2025.
32. Federal Bureau of Investigation. (2023, March 15). "Chinese Operatives Target U.S. Semiconductors." https://www.fbi.gov/news/stories/chinese-operatives-target-us-semiconductors. Accessed on March 6, 2025.
33. Reuters. (2022, October 20). "Netherlands Uncovers Chinese Espionage in Tech Sector." https://www.reuters.com/technology/netherlands-uncovers-chinese-espionage-in-tech-sector-2022-10-20/. Accessed on March 8, 2025.
34. Australian Broadcasting Corporation. (2024, February 10). "China's Espionage in Defense Contracts Disrupted." https://www.abc.net.au/news/2024-02-10/chinas-espionage-in-defense-contracts-disrupted/103456789. Accessed on March 2, 2025.
35. Business Daily Africa. (2023, July 12). "Kenya Flags Chinese Surveillance in Telecom Projects." https://www.businessdailyafrica.com/bd/data-hub/kenya-flags-chinese-surveillance-in-telecom-projects-4301234. Accessed on March 11, 2025.
36. Reuters. (2024, April 5). "Brazil's Space Program Hit by Chinese Cyberattacks." https://www.reuters.com/technology/brazils-space-program-hit-by-chinese-cyberattacks-2024-04-05/. Accessed on March 3, 2025.
37. New Zealand Herald. (2022, June 15). "Chinese Donations to Politicians Probed." https://www.nzherald.co.nz/nz/chinese-donations-to-politicians-probed/ABC123456789/. Accessed on March 5, 2025.
38. The Times of India. (2018, December 10). "Chinese Spies Target Tibetan Exiles in India." https://timesofindia.indiatimes.com/india/chinese-spies-target-tibetan-exiles-in-india/articleshow/67023456.cms. Accessed on March 18, 2025.
39. Hindustan Times. (2022, April 7). "China's Cyberattacks on India's Defense Systems." https://www.hindustantimes.com/india-news/chinas-cyberattacks-on-indias-defense-systems-101649123456789.html. Accessed on March 28, 2025.
40. The Indian Express. (2023, October 10)."Chinese Cyberattacks Target ISRO Facilities." https://indianexpress.com/article/india/chinese-cyberattacks-target-isro-facilities-8971234/. Accessed on March 23, 2025.
41. The Indian Express. (2021, March 1). "Chinese Hackers Target India's Power Grid." https://indianexpress.com/article/india/chinese-hackers-target-indias-power-grid-7203456/. Accessed on March 25, 2025.

42. Business Standard. (2024, January 15). "Chinese Hackers Target India's Banking Sector." https://www.business-standard.com/india-news/chinese-hackers-target-indias-banking-sector-124011500123_1.html. Accessed on March 16, 2025.
43. Ministry of Commerce and Industry, Government of India. (2024). "India-China Trade Statistics 2023." https://commerce.gov.in/trade-statistics/. Accessed on March 31, 2025.
44. The Print. (2023, January 20). "China-Pakistan Intelligence Nexus." https://theprint.in/defence/china-pakistan-intelligence-nexus/1324567/. Accessed on March 29, 2025.
45. Reuters. (2024, March 10). "Sri Lanka's Hambantota Port Deal Raises Espionage Concerns." https://www.reuters.com/world/asia-pacific/sri-lankas-hambantota-port-deal-raises-espionage-concerns-2024-03-10/. Accessed on March 14, 2025.
46. The Indian Express. (2023, December 5). "Chinese Operatives Target Bengaluru AI Research." https://indianexpress.com/article/india/chinese-operatives-target-bengaluru-ai-research-9056789/. Accessed on March 13, 2025.
47. Business Standard. (2024, April 1). "Chinese Supply-Chain Attack on Indian Medical Equipment." https://www.business-standard.com/india-news/chinese-supply-chain-attack-on-indian-medical-equipment-124040100123_1.html. Accessed on April 08, 2025.
48. Cybersecurity Ventures. (2023, October 10). "Israel's Cyber Defense Model." https://cybersecurityventures.com/israels-cyber-defense-model/. Accessed on April 4, 2025.
49. The Hindu. (2023, December 20). "India's Cybersecurity Policy 2023." https://www.thehindu.com/news/national/indias-cybersecurity-policy-2023/article67678901.ece. Accessed on April 10, 2025.
50. The Hindu. (2024, February 15). "India-Vietnam Cyber Pact Signed." https://www.thehindu.com/news/international/india-vietnam-cyber-pact-signed/article67845678.ece. Accessed on April 4, 2025.
51. The Economic Times. (2024, January 25). "India's Defense Budget 2024." https://economictimes.indiatimes.com/news/defence/indias-defense-budget-2024/articleshow/107123456.cms. Accessed on April 10, 2025.

Lawfare and Narrative Warfare: Countering China's Expansionist Claims Over Arunachal Pradesh

Vikas Raj Gupta

Abstract

China's territorial claims over Arunachal Pradesh form a key component of its broader expansionist agenda—merging legal revisionism with disinformation and narrative control. Despite clear historical treaties, consistent governance, and international recognition affirming Arunachal Pradesh as Indian territory, Beijing continues to assert its claim by referring to the region as "South Tibet." This article argues that India must adopt an integrated approach combining legal warfare and information warfare, to effectively counter China's assertions. By invoking the McMahon Line, international legal precedents, and the principle of effective control, the article establishes India's sovereignty under international law. Simultaneously, it examines how China leverages cartographic manipulation, diplomatic coercion, and cultural appropriation to construct alternative narratives. The article advocates for a robust Indian strategy that includes legal

Brigadier **Vikas Raj Gupta** is an Army Air Defence officer with Master's degree in Strategic Studies from the University of Madras and International Relations from Deakin University, Melbourne. He has operational experience along the Line of Control and currently commands an Infantry Brigade along the Line of Actual Control. Views expressed are personal.

documentation, diplomatic engagement, public diplomacy, and strategic communication. Ultimately, it posits that narrative and legal assertion are critical to safeguarding territorial integrity and countering China's hybrid warfare in the Indo-Pacific.

The border dispute between India and China, over Arunachal Pradesh, remains one of the most complex and enduring geopolitical challenges in South Asia. China claims approximately 90,000 square kilometres of Arunachal Pradesh, referring to it as "South Tibet," despite the region's unequivocal status as an integral and fully governed state of India. This territorial contention extends beyond cartographic assertions; it is a crucial component of China's 'broader expansionist strategy', which combines diplomatic coercion, military posturing, and information warfare to challenge India's sovereignty. While military preparedness and diplomatic negotiations are indispensable, India must also adopt a proactive and multi-pronged strategy that integrates legal and information warfare to effectively counter China's claims.

A robust legal warfare strategy necessitates the systematic compilation and presentation of historical treaties, official maps, administrative records, census data, and other documentary evidence that substantiate India's longstanding control over Arunachal Pradesh. This evidentiary foundation is critical in reinforcing India's claim under international law and countering China's revisionist narratives. However, in an era where geopolitical disputes are increasingly shaped by public perception and global discourse, legal arguments alone are insufficient. Therefore, complementing legal warfare is the strategic deployment of information warfare, which involves shaping narratives, influencing public opinion, and countering disinformation campaigns.

While China has often demonstrated selective adherence to international rulings and norms, India cannot afford to remain passive. To effectively safeguard its territorial integrity, India must strategically

employ legal and information warfare—not with the naive expectation of immediate Chinese compliance, but as long-term strategies to build international pressure, shape global opinion, and reinforce its domestic position.

This essay critically examines China's expansionist tactics, the legal foundations of India's claim over Arunachal Pradesh, and the imperative for India to leverage legal and information warfare to safeguard its territorial integrity and assert its rightful sovereignty over the region.

HISTORICAL AND LEGAL FOUNDATIONS OF INDIA'S SOVEREIGNTY OVER ARUNACHAL PRADESH

The territorial dispute between India and China over Arunachal Pradesh is deeply rooted in history, international treaties, and principles of international law. While China asserts its claims over the region based on historical and cultural linkages with Tibet, India's sovereignty over Arunachal Pradesh is firmly established through legal agreements, consistent governance, and the principle of effective control and administration. This section examines the legal and historical foundations of India's sovereignty over the region, drawing on international legal precedents and the principle of self-determination.

The McMahon Line and the Simla Accord (1914)

The McMahon Line, delineated under the Simla Accord of 1914, forms the primary legal basis for India's sovereignty over Arunachal Pradesh. The accord was negotiated between Sir Henry McMahon, the plenipotentiary representing British India, Ivan Chen, representing China's Qing government, and Lonchen Shatra, the envoy of the autonomous Tibetan government. The Agreement clearly demarcated the boundary between British India and Tibet, placing Arunachal Pradesh within British Indian territory.

Although the Chinese representative initially participated in the negotiations and initialled the agreement, China subsequently refused to ratify the same, later claiming that Tibet did not have the independent authority to enter into such agreements. However, at the time, Tibet functioned as an autonomous political entity with the capacity to conduct foreign affairs. Therefore, the Simla Accord remains a valid legal instrument supporting India's territorial claims. Upon independence in 1947, India inherited these boundaries, in line with the principle of *Uti Possidetis Juris*—a recognized doctrine in international law, that affirms that newly independent states should retain pre-existing colonial boundaries.

Further illustrating the inconsistency in China's stance, it is notable that China settled its border with Myanmar in the 1960s based on the McMahon Line. However, when it comes to India, the same McMahon Line is deemed illegal by China. This exemplifies the selective and contradictory nature of China's territorial claims.

Furthermore, historical records demonstrate that China has never exercised actual sovereignty over Arunachal Pradesh at any point in its history. The Qing Dynasty's influence over Tibet was nominal and did not extend to governance or administration over what is now Arunachal Pradesh. This absence of effective control severely undermines China's territorial claims, especially in the context of established international legal principles.

International Legal Precedents Supporting India's Sovereignty

The legal principle that, effective control and administration take precedence over historical claims, is well established in international jurisprudence. Several landmark cases support India's sovereignty over Arunachal Pradesh:

- **Island of Palmas Case (1928, Netherlands vs. US)**: This ruling by the Permanent Court of Arbitration held that continuous and

effective sovereignty outweighs historical assertions. In this case, the Netherlands' long-term governance of the Island of Palmas was deemed superior to Spain's historical claim. Similarly, India's uninterrupted administration of Arunachal Pradesh overrides China's historical arguments.

- **Burkina Faso vs. Mali (1986, International Court of Justice - ICJ)**: The ruling reaffirmed the principle that post-colonial states must uphold their inherited boundaries, even if contested by historical claims. This supports India's stance, as Arunachal Pradesh was legally incorporated into India's administrative framework upon independence.
- **Pedra Branca Case (2008, Singapore vs. Malaysia)**: The ICJ ruled in favour of Singapore based on its long-term administration of Pedra Branca, emphasizing the importance of effective governance as a determinant of sovereignty. India's long and democratic governance of Arunachal Pradesh similarly establishes its legal sovereignty over the region.

These cases reinforce a crucial point—historical claims alone do not establish sovereignty; rather, it is the demonstration of effective control, governance, and international recognition that determines legitimacy. Applying these principles, India's uninterrupted governance over Arunachal Pradesh since independence, along with the presence of an elected government and administrative institutions, further solidifies its legal standing.

The Principle of Effective Control and Self-Determination

Under the international law, effective control and administration serves as a primary determinant of sovereignty. This principle requires consistent governance and administrative control, a permanent and settled population and long-term political integration.

India fulfils all these criteria in relation to Arunachal Pradesh. The state is fully integrated into India's political and administrative framework, with elected representatives, local governance structures, and participation in national policymaking. Since its inclusion as the North-East Frontier Agency (NEFA) and later as a full-fledged state in 1987, Arunachal Pradesh has since functioned as an inseparable part of India.

Additionally, the will of the people is a critical factor in determining territorial legitimacy. The people of Arunachal Pradesh overwhelmingly identify as Indian, participate in India's electoral processes, and have never expressed allegiance to China. UN Resolution 1514 (Declaration on the Granting of Independence to Colonial Countries and Peoples) underscores the right of people to self-determination, further invalidating China's claim that the region should be considered "South Tibet."

China's position that Arunachal Pradesh is historically linked to Tibet, fails to account for the rights and agency of the region's inhabitants, who have consistently rejected any association with China. By prioritizing the self-determination of Arunachal Pradesh's people, international legal norms favour India's sovereignty over historical revisionist claims.

Global Recognition of Arunachal Pradesh as Indian Territory

A significant indicator of territorial legitimacy is international recognition, which overwhelmingly supports India's sovereignty over Arunachal Pradesh. The United Nations and major global powers, including the United States, Russia, France, Japan, Australia, and the European Union, recognize Arunachal Pradesh as an integral part of India.

- The **United States** has explicitly acknowledged Arunachal Pradesh as Indian Territory in multiple statements. For instance, in March 2023, the U.S. State Department reaffirmed that Arunachal Pradesh is part of India, rejecting China's claims and condemning its renaming of places in the region as part of disinformation tactics.

- **Russia**, despite its close strategic ties with China, has never officially endorsed Beijing's claim over Arunachal Pradesh.

This widespread recognition significantly weakens China's ability to advance its claims through diplomatic channels. The absence of global support for China's position reinforces the legitimacy of India's territorial control under international law.

The Pakistan Occupied Kashmir (PoK) Comparison: Legal and Strategic Consistency

Critics may contend that reliance on international treaties—such as the 1914 Simla Agreement and the McMahon Line—to assert India's sovereignty over Arunachal Pradesh appears inconsistent with its rejection of Pakistan's demand for a UN-mandated plebiscite in Jammu and Kashmir. However, this comparison oversimplifies the distinct legal, historical, and political dimensions of both disputes.

The fundamental difference lies in the nature of territorial control and historical legitimacy. Arunachal Pradesh has always been under India's undisputed administration, with its status reaffirmed through international treaties and customary law. In contrast, PoK is the result of an external military invasion, violating the principle of territorial integrity—a cornerstone of international law. India's legal position on Arunachal Pradesh aligns with recognized sovereign rights, while its stance on Kashmir is grounded in the 1972 Simla Agreement, which established that all disputes between India and Pakistan must be resolved bilaterally, effectively superseding earlier UN resolutions. Crucially, the plebiscite proposed under UN Security Council Resolution 47 was contingent on Pakistan's withdrawal from the region—a condition it has never fulfilled, rendering the resolution inoperative in practice.

Moreover, China's claims over Arunachal Pradesh lack any active international legal dispute and are instead based on retroactive historical

narratives rather than binding agreements or customary international law. Conversely, India's position on PoK is supported by well-established legal principles, particularly the prohibition on territorial acquisition by force. Unlike China's expansionist claims, which hinge on selective historical interpretations, India's position on Kashmir does not seek to "reopen" the issue but rather underscores Pakistan's violation of international norms through continued occupation.

Thus, far from being contradictory, India's approach reflects a clear legal and strategic distinction—defending territories that are historically, legally, and administratively part of India (Arunachal Pradesh) while challenging the illegal occupation of its sovereign land (PoK). This nuanced legal position reinforces India's broader strategic objectives—countering both territorial revisionism and unlawful occupations, while maintaining its commitment to international law and established diplomatic frameworks.

CHINA'S EXPANSIONIST TACTICS AND INFORMATION WARFARE STRATEGIES

China employs a combination of information warfare, diplomatic coercion, military intimidation, and cultural influence strategies to challenge India's sovereignty over Arunachal Pradesh. These tactics are designed to create an alternative historical narrative, manipulate global perception, and incrementally assert territorial claims. The primary objective of these efforts is to weaken India's position and shift the geopolitical balance in Beijing's favour. This section explores the various methods China uses to pursue its expansionist agenda.

Historical Revisionism and Cartographic Manipulation

A key pillar of China's information warfare strategy is historical revisionism, whereby it selectively interprets historical events to justify territorial claims. Beijing asserts that during the Qing Dynasty

(1644–1912), Tibet was under Chinese suzerainty, and since Arunachal Pradesh was culturally linked to Tibet, it should also fall under Chinese jurisdiction. This "South Tibet" narrative forms the foundation of China's claims over the region. China actively promotes this assertion by:

- **Publishing official maps** that depict Arunachal Pradesh as part of "South Tibet."
- **Renaming towns and villages** in Arunachal Pradesh to fabricate historical links with Tibet. In 2023 and 2024, China issued multiple lists renaming locations in Arunachal Pradesh—an act India strongly condemned as an attempt at "territorial aggrandizement through disinformation."
- **Using state-controlled media and diplomatic channels** to reinforce its narrative internationally. Chinese news outlets, academic research papers, and official statements continuously push the claim that Arunachal Pradesh historically belonged to Tibet and, therefore, to China.
- **Pressuring foreign nations** to avoid recognizing Arunachal Pradesh as part of India. For instance, in March 2024, after the United States explicitly reaffirmed Arunachal Pradesh as Indian territory, China strongly opposed the statement, claiming that the border dispute was a bilateral issue in which no third country should intervene.

However, China's historical arguments are weak and inconsistent when evaluated against facts and international legal principles. The Qing emperors exercised only nominal suzerainty over Tibet, lacking direct administrative control. Tibet, for much of its history, conducted independent foreign relations, managed its own governance, and functioned as an autonomous entity. Even when the Qing exercised influence, their authority never extended to Arunachal Pradesh.

The fall of the Qing Dynasty in 1912 left Tibet effectively independent until China forcefully occupied it in 1951. Arunachal Pradesh, in

contrast, was never governed by China or Tibet. The region's indigenous communities maintained distinct governance systems, and British India established administrative control over the area in the early 20th century. Given these facts, China's historical revisionism is an artificial construct designed to support an expansionist agenda rather than being rooted in legitimate claims.

Diplomatic and Political Coercion

China also employs diplomatic and political pressure tactics to challenge India's sovereignty over Arunachal Pradesh and shape international opinion.

- **Raising the Arunachal Pradesh issue in diplomatic engagements and global forums**: China persistently brings up the territorial status of Arunachal Pradesh in international settings to legitimize its claims and keep the dispute alive. After Prime Minister Narendra Modi's visit to Arunachal Pradesh in March 2024, China's Defence Ministry reiterated its opposition, claiming that "the southern part of Xizang (Tibet) is an inherent part of China's territory" and that Beijing "never acknowledges and firmly opposes the so-called Arunachal Pradesh illegally established by India."
- **Obstructing India's diplomatic ambitions**: China has consistently used its permanent membership in the United Nations Security Council (UNSC) to block India's bid for permanent UNSC membership. This is part of a broader strategy to limit India's global influence and ensure that India does not gain a more powerful voice in international diplomacy.
- **Pressuring other countries to reject India's sovereignty over Arunachal Pradesh**: When the United States reaffirmed Arunachal Pradesh as part of India in 2024, China responded with diplomatic protests. Chinese Foreign Ministry spokesperson Lin Jian stated that China "strongly deplores and firmly opposes" such statements,

insisting that the territorial issue is a bilateral matter and should not involve third parties. This reaction underscores Beijing's persistent attempts to isolate India diplomatically.

Through such diplomatic strategies, China seeks to erode India's territorial legitimacy and create international ambiguity regarding Arunachal Pradesh's status.

Military Coercion and "Salami Slicing" Tactics

China's military coercion strategy involves incremental territorial encroachments, known as "salami slicing" tactics, where it makes small, gradual moves to alter the status quo without triggering a full-scale conflict. These tactics involve:

- **Infrastructure development in disputed areas**: China has aggressively built roads, bridges, military outposts, and civilian settlements along disputed regions, including areas near Arunachal Pradesh. A major example is China's plan to build a hydroelectric dam on the Yarlung-Tsangpo River near Arunachal Pradesh, raising concerns about water security in northeast India. Such projects enhance China's ability to exert hydrological and geopolitical pressure on India.
- **Direct military confrontations**: China has engaged in multiple border conflicts to assert control over disputed areas.
  - In **2017**, Chinese forces attempted to construct a road into the **Doklam plateau**, leading to a 73-day military standoff with India.
  - In **June 2020, the Galwan Valley clash** between Indian and Chinese troops led to 20 Indian casualties and an undisclosed number of Chinese casualties. This marked the most serious border confrontation in decades.

- **The Tawang Region** in Arunachal Pradesh has witnessed **repeated clashes**, indicating China's intent to escalate military pressure on the region.

China's military activities seek to challenge India's border defences while avoiding large-scale conflict that could invite international intervention.

Cultural and Religious Influence Campaigns

China also leverages cultural and religious influence to justify its territorial claims over Arunachal Pradesh, particularly in Tawang—a region with strong Tibetan Buddhist heritage.

- **Manipulating Tibetan Buddhist heritage for territorial claims**: Tawang Monastery, one of the most important centres for Tibetan Buddhism, is central to China's expansionist narrative. Beijing claims that because Tawang has deep ties to Tibetan Buddhism, hence should be part of China. However, local Buddhist leaders firmly reject this claim. Gyangbung Rinpoche, the abbot of Tawang Monastery, has stated that China lacks any spiritual or religious authority over Tibetan Buddhism.
- **Interfering in the Dalai Lama's succession**: China insists on its right to appoint the next Dalai Lama, viewing control over Tibetan religious leadership as a means to legitimize its governance over Tibet and Arunachal Pradesh. However, the current Dalai Lama has proposed alternative succession plans to counteract Beijing's influence.
- **Soft power economic strategies**: China uses economic incentives, infrastructure development, and trade to sway local populations in disputed areas. Through targeted investments, Beijing seeks to create economic dependencies that could later serve as a basis for territorial integration.

INDIA'S STRATEGIC RESPONSE: LEGAL AND INFORMATION WARFARE APPROACHES

Reinforcing Legal and Historical Sovereignty

China's territorial claims over Arunachal Pradesh are rooted in 'historical revisionism' and 'cultural assertions' linking the region to Tibet. To counter these claims, India must implement a proactive legal and historical strategy to reinforce its sovereignty over Arunachal Pradesh. This approach should encompass publicizing historical treaties and legal precedents, engaging international legal experts, strengthening diplomatic outreach, and amplifying the region's democratic governance, economic development, and cultural identity as an integral part of the Indian nation-state.

Publicizing Historical Treaties and Legal Precedents

India must actively promote historical agreements that substantiates its territorial claims. A key focus should be the McMahon Line, established during the 1914 Simla Accord between British India and Tibet, which serves as the internationally recognized boundary between India and Tibet. India should highlight this agreement in global forums and diplomatic engagements to reinforce its claim over Arunachal Pradesh. The government should also publish archival documents and legal references to counter China's historical revisionism.

Engaging International Legal Experts

To strengthen its position in global legal forums, India should collaborate with international legal scholars and historians and challenge China's revisionist claims. A legal advisory body should be established to counter China's interpretation of international treaties and historical sovereignty. Think tanks, research institutions, and universities should be encouraged to produce scholarly work validating India's claims and disseminating these findings through international platforms.

Strengthening Diplomatic Outreach

India must intensify diplomatic engagements with the international community to promote a fact-based narrative, thus emphasizing its adherence to international law and peaceful dispute resolution. Strategic partnerships with nations such as the United States, the European Union, ASEAN countries, and Japan should be strengthened to build a strong international stance against China's territorial claims. India should work with friendly nations to pass resolutions recognizing Arunachal Pradesh as an integral part of India, similar to the 2023 US Senate resolution reaffirming the McMahon Line as the international boundary. The Ministry of External Affairs should also ensure that international organizations and map publishers accurately depict Arunachal Pradesh as part of India in all official documents.

Amplifying Democratic Governance and Local Identity

India must emphasize that Arunachal Pradesh is a full-fledged state within the Indian Union, with democratically elected representatives in the Lok Sabha and Rajya Sabha. Unlike Tibet, which is under authoritarian Chinese control, Arunachal Pradesh enjoys full political participation and autonomy within India's democratic framework.

India should showcase its significant infrastructure and economic development initiatives in Arunachal Pradesh, including:

- **The Trans-Arunachal Highway**, connecting remote districts and enhancing regional connectivity.
- **Hydropower projects**, improving energy access and economic growth.
- **Educational institutions and universities**, supporting local aspirations.
- **Healthcare advancements**, ensuring better living standards for local populations.
- **Digital and physical connectivity initiatives**, such as Digital India and the Act East Policy.

- **The Vibrant Villages Programme**, aimed at integrating border communities into national development efforts.

Unlike China, which focuses on militarizing Tibet, India prioritizes development and economic prosperity in Arunachal Pradesh, thus countering Beijing's claims of neglect.

Highlighting Arunachal Pradesh's Deep-Rooted Cultural Ties with India

China has consistently employed cultural and religious narratives to justify its territorial claims over Arunachal Pradesh by labelling the region as "South Tibet." India must counter these claims by emphasizing Arunachal Pradesh's historical ties to Hindu, Vedic, Puranic traditions, and Buddhism. Key points include:

- **Hindu Epics and Scriptures:** The Mahabharata and Ramayana mention Arunachal Pradesh in connection with the Pandavas and Sage Parashurama.
- **Sacred Texts:** The Kalika Purana, Skanda Purana, and Brahma Purana refer to Arunachal Pradesh as a sacred land associated with Lord Shiva and Goddess Parvati.
- **Kamakhya Tradition:** Linked to Assam and Arunachal Pradesh, reinforcing its deep spiritual connection to India.
- **Parashuram Kund:** A revered Hindu pilgrimage site that attracts thousands of devotees annually.
- **Indigenous Traditions:** Local tribes such as the Monpa, Adi, Nyishi, and Apatani maintain traditions distinct from Tibet, with the Donyi Polo faith sharing similarities with Hindu rituals.
- **Buddhism's Indian Roots:** While China emphasizes religious ties between Arunachal Pradesh and Tibet, India must assert that Buddhism originated in India, with Rinpoche Padmasambhava introducing Buddhism to Tibet.

- **Tawang Monastery and the 6th Dalai Lama:** The Tawang Monastery, historically linked to Indian Buddhist traditions, and the birthplace of the 6th Dalai Lama in Tawang, reinforces the region's Indian identity.

China's interference in Tibetan Buddhism, including its attempts to control the Dalai Lama's succession, highlights the stark contrast between religious freedom in Arunachal Pradesh and repression in Tibet. India must collaborate with the Tibetan government-in-exile, Buddhist scholars, and monks to counter China's narrative and assert India's role as the true custodian of Buddhist heritage.

Strategic Communication Approach

To effectively challenge China's claims and amplify Arunachal Pradesh's democratic governance and cultural identity, India should leverage international media and strategic communications:

- **Showcase Arunachal Pradesh's growth** in global media outlets.
- **Strengthen cultural exchanges** with Southeast Asian nations, emphasizing shared Buddhist heritage.
- **Empower local leaders and scholars** to engage in international forums and academic discussions.
- **Launch social media campaigns** highlighting Arunachal Pradesh's democracy and economic progress.

Countering Chinese Disinformation

China frequently uses misinformation, altered maps, and propaganda to claim Arunachal Pradesh as "South Tibet." To counter these tactics, India must implement a comprehensive information warfare strategy:

- **Establish a government-backed fact-checking portal** to debunk Chinese disinformation with legal documents and historical treaties.

- **Collaborate with independent fact-checkers** and international legal experts to dismantle China's revisionist claims.
- **Create rapid response teams** within the Ministry of External Affairs (MEA), Indian Army, and think tanks to counter misinformation.
- **Monitor and counter Chinese disinformation** on platforms like Weibo, X (formerly Twitter), and YouTube through fact-based counter-narratives.
- **Engage prominent Indian diplomats, journalists, and academics** to challenge China's narratives in mainstream and social media.
- **Produce short documentaries, infographics, and podcasts** to highlight Arunachal Pradesh's historical, legal, and cultural ties to India.
- **Expose Chinese territorial encroachments** through satellite imagery, open-source intelligence (OSINT), and global media partnerships.
- **Collaborate with global media organizations** such as BBC, Reuters, and The New York Times to ensure accurate coverage of the Arunachal Pradesh dispute.
- **Raise Chinese border violations at international forums** including the United Nations, G7, QUAD, and ASEAN.
- **Work with think tanks** such as ORF, Carnegie India, and Brookings Institution to publish research countering China's expansionist claims.

By systematically countering Chinese disinformation, India can reinforce global awareness of its legitimate sovereignty over Arunachal Pradesh and expose China's revisionist tactics as part of a broader expansionist strategy.

Risk of Escalating Tensions

Some may argue that adopting an assertive narrative warfare strategy could provoke China into more aggressive military or diplomatic actions, exacerbating regional instability. However, India can mitigate this risk

through a measured and fact-based narrative that avoids inflammatory rhetoric. By consistently promoting its legal claims and emphasizing its commitment to peaceful dispute resolution, India can present itself as a responsible actor. Furthermore, engaging with regional organizations like ASEAN and QUAD would foster collective deterrence against any coercive Chinese responses.

China's Narrative Dominance

Given China's extensive control over state media and its influence in the Global South, some critics may argue that India's narrative efforts could be overshadowed. However, India's advantage lies in the credibility of its democratic institutions and free press. By collaborating with independent international media, think tanks, and historians, India can amplify its narrative. Additionally, aligning with other nations that share concerns over Chinese expansionism, can create a stronger collective voice for countering China's disinformation campaigns.

Domestic and International Disinterest

Sceptics may contend that the Arunachal Pradesh issue lacks sufficient global resonance, thus limiting international support for India's stance. Nonetheless, India should reframe the dispute as part of a broader challenge to the rules-based international order. Emphasizing China's pattern of territorial assertiveness in the South China Sea, the Himalayas, and other regions would resonate with countries that value territorial integrity and sovereignty. Furthermore, highlighting the implications for regional security in the Indo-Pacific will ensure greater global engagement on the issue.

Conclusion

To reinforce its sovereign claims over Arunachal Pradesh, while maintaining its commitment to bilateral dialogue, India can adopt a comprehensive

strategy that integrates legal principles, narrative management, and diplomatic engagement. Legal instruments such as the Simla Accord and established principles of international law provide a solid foundation for India's position. Although the enforcement of international rulings may be limited, the symbolic and diplomatic weight of legal affirmation can strengthen India's global standing. Presenting consistent, evidence-based claims in international forums will further reinforce India's legitimacy.

In parallel, India must proactively engage in narrative warfare to counter China's disinformation campaigns. By leveraging independent media, collaborating with think tanks, and using diplomatic channels, India can ensure that its factual narrative gains global traction. Partnerships with democratic allies can amplify these efforts, particularly through coordinated messaging and joint public statements. Additionally, India's commitment to transparency and adherence to international norms will enhance its credibility in contrast to China's assertive manoeuvres.

Domestically, a unified and informed public is essential for sustaining long-term resilience against external narratives. Promoting accurate historical accounts through educational initiatives, public diplomacy campaigns, and scholarly research will counter China's revisionist claims. Furthermore, celebrating Arunachal Pradesh's cultural diversity, economic development, and democratic participation will reinforce its integral status within India.

While immediate Chinese compliance with legal or diplomatic outcomes may remain unlikely, the broader objective is to shape the global public opinion and garner sustained international support. A well-executed legal and narrative strategy will deter further territorial assertiveness from China, strengthen India's diplomatic standing, and maintain Arunachal Pradesh's rightful place within the Indian Union. By upholding its principled approach and aligning with like-minded nations, India will not only protect its territorial integrity but also contribute to the preservation of a rules-based international order.

Bibliography

Books

Ajay Mitra Shastri, *The Ramayana Tradition in Historical Perspective* (Delhi: Motilal Banarsidass, 1991).

Alastair Lamb, *The McMahon Line: A Study in the Relations Between India, China, and Tibet, 1904–1914* (London: Routledge, 1966).

Ashley J. Tellis, *India's Emerging Strategic Partnership with the United States* (Washington, DC: Carnegie Endowment for International Peace, 2000).

C. Raja Mohan, *Modi's World: Expanding India's Sphere of Influence* (New Delhi: HarperCollins, 2015).

D. C. Sircar, *Studies in the Religious and Cultural History of India* (Delhi: Motilal Banarsidass, 1971).

Dalai Lama XIV, *Freedom in Exile: The Autobiography of the Dalai Lama* (New York: HarperOne, 1991).

Dibyesh Anand, *Tibet: A Victim of Geopolitics* (London: Routledge, 2007).

Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007).

Harish Kapur, *China's Policy in the Himalayas* (London: Routledge, 1987).

Ian Brownlie, *Principles of Public International Law*, 8th ed. (Oxford: Oxford University Press, 2008).

Jasjit Singh, *China's Strategic Encirclement of India* (New Delhi: Knowledge World, 2001).

John W. Garver, *Protracted Contest: Sino-Indian Rivalry in the Twentieth Century* (Seattle: University of Washington Press, 2001).

Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004).

Malcolm N. Shaw, *International Law*, 6th ed. (Cambridge: Cambridge University Press, 2008).

Margaret W. Fisher, *Himalayan Battleground: Sino-Indian Rivalry in Ladakh* (New York: Praeger, 1963).

Melvyn C. Goldstein, *A History of Modern Tibet*, Vol. 1 & 2 (Berkeley: University of California Press, 2007).

Monika Chansoria, *China's War on Law: The Strategic Use of Legal Warfare by Beijing* (New Delhi: KW Publishers, 2020).

Neville Maxwell, *India's China War* (London: Jonathan Cape, 1970).

P. Stobdan, *The Great Game in the Buddhist Himalayas: India and China's Quest for Strategic Dominance* (New Delhi: Penguin, 2019).

R. Jennings and A. Watts, *Oppenheim's International Law: Disputes and Legal Precedents* (Oxford: Oxford University Press, 2008).

Subhash Shukla, *Border Security and India-China Relations* (New Delhi: Pentagon Press, 2018).

Vijay Gokhale, *Tiananmen Square: The Making of Modern China and Its Relations with India* (New Delhi: HarperCollins India, 2021).

Articles in Newsmagazines / Newspapers

"Arunachal Pradesh: US Senate committee passes resolution recognising Arunachal Pradesh as Indian territory," *The Times of India*, July 14, 2023. https://timesofindia.indiatimes.com/india/us-senate-committee-passes-resolution-recognising-arunachal-pradesh-as-integral-part-of-india/articleshow/101741339.cms

"China's Increasingly Aggressive Tactics for Foreign Disinformation Campaigns," *The Diplomat*, September 18, 2023. https://thediplomat.com/2023/09/chinas-increasingly-aggressive-tactics-for-foreign-disinformation-campaigns/

"China's Disinformation Campaign in the Philippines," *The Diplomat*, October 2020. https://thediplomat.com/2020/10/chinas-disinformation-campaign-in-the-philippines/

"China Is Waging a 'Gray Zone' Campaign to Cement Power. Here's How It Looks.," *The Wall Street Journal*, March 15, 2025. https://www.wsj.com/world/china/china-expansion-taiwan-himalayas-146aff72

"How China could try to strangle Taiwan without firing a shot," *Vox*, December 16, 2024. https://www.vox.com/world-politics/390895/china-taiwan-conflict

"India protests over China's new map; 'complicates resolution of boundary issue'," *The Hindu*, August 29, 2023. https://epaper.thehindu.com/ccidist-ws/th/th_erode/issues/49748/OPS/GUVBMB7JH.1%2BG3ABMBRJ8.1.html

Tobias Burgers and Scott N. Romaniuk, "China's Real Takeaway From the War in Ukraine: Grey Zone Conflict Is Best," *The Diplomat*, October 6, 2022. https://thediplomat.com/2022/10/chinas-real-takeaway-from-the-war-in-ukraine-grey-zone-conflict-is-best/

"What is behind China's renaming spree?," *The Hindu*, April 4, 2023. https://epaper.thehindu.com/ccidist-ws/th/th_tiruchirapalli/issues/31761/OPS/GT9B3BQNE.1%2BGQ7B3CSDO.1.html

Reports / Government Documents

Carnegie India, *Arunachal Pradesh: India's Northeast Frontier and China's Claims* (New Delhi: Carnegie Endowment for International Peace, 2022).

Indian Chamber of Commerce, *Trade and Border Development in Arunachal Pradesh* (New Delhi: Government of India, 2019).

Ministry of External Affairs, Government of India, *Annual Report on India-China Relations* (New Delhi: MEA Publications, 2023).

Indian External Affairs Ministry, *Reports on Chinese Disinformation Campaigns* (New Delhi: Government of India, various years).

Indian Ministry of Culture, *Arunachal Pradesh: A Land of Ancient Traditions* (New Delhi: Government of India, 2022).

Indian Ministry of Defence, *Annual Report on Border Management & Strategic Threats* (New Delhi: Government of India, 2021).

Indian Ministry of External Affairs, *White Paper on Sino-Indian Relations* (New Delhi: Government of India, 1959–1965).

Observer Research Foundation (ORF), *China's Expansionism and India's Response: A Strategic Overview*, ORF Issue Brief (New Delhi: ORF, 2023).

Reports on India's Act East Policy and QUAD's Strategic Initiatives (New Delhi: ORF, Carnegie India, and Ministry of External Affairs).

United Nations, *Charter of the United Nations* (New York: United Nations, 1945).

United Nations, *United Nations Convention on the Law of the Sea (UNCLOS)* (Geneva: United Nations, 1982).

U.S. Congressional Research Service, *China's Territorial Disputes: Implications for U.S. Interests*, Report R47219 (Washington, DC: CRS, 2023).

Reports and Papers by Think Tanks / Institutions

Abhay Kumar Singh, *China's Information Warfare Strategy: Implications for India*, IDSA Occasional Papers (New Delhi: IDSA, 2018).

RAND Corporation, *Chinese Disinformation Campaigns and Influence Operations in Asia* (Santa Monica, CA: RAND Corporation, 2021).

Legal Cases and Judgments

Burkina Faso v. Mali, 1986, *International Court of Justice Reports*, p. 554.

Island of Palmas Case (Netherlands v. United States), 1928, *Reports of International Arbitral Awards*, Vol. 2, p. 829.

Pedra Branca Case (Malaysia v. Singapore), 2008, *International Court of Justice Reports*, p. 12.

Historical Agreements / Archival Sources

Agreement on the Political Parameters and Guiding Principles for the Settlement of the India-China Boundary Question, 2005 (New Delhi: Government of India).

Convention Between Great Britain, China, and Tibet (Simla Accord, 1914) (London: British Government, 1914).

India-China Simla Agreement (1914), British Archives and Government of India Documents.

Religious / Cultural Sources

Central Tibetan Administration (CTA), *Cultural Significance and Historical Claims in Arunachal Pradesh* (Dharamshala: CTA, 2020).

Kalika Purana and *Skanda Purana*, trans. and ed. Banaras Hindu University Archives (Varanasi: BHU, n.d.).

Tawang Monastery Archives, *Records on Historical and Religious Significance*, compiled in 2018 (Tawang: Monastic Office, 2018).

China's Territorial Ambitions

Narendran Gurumurthy and Rajan Bakshi

Abstract

General Secretaries of the Communist Party of China have described "national rejuvenation" as the central mission of their Party since the Thirteenth Party Congress in 1987. Their wording intentionally echoes the language used by Sun Yat-sen and the nationalist revolutionaries who overthrew the Qing Dynasty at the cusp of the modern era. Those revolutionaries dreamed of restoring a broken nation to its traditional station at the centre of human civilisation. Xi Jinping similarly describes national rejuvenation as a "strategic plan" for "achieving lasting greatness for the Chinese nation" (Xi, 2022). *The formal term for this plan is the "National Rejuvenation of the Chinese Nation," a term that could be alternatively translated as the "National Rejuvenation of the Chinese Race." In the modern era, national rejuvenation has been formally identified as the overarching goal of all activities of both Party and State.*[1]

Captain (*IN*) **Narendran Gurumurthy** is an alumnus of the 56th Naval Academy Course and is a Navigation and Direction Specialist. The Officer has extensive Staff tenures including at Directorate of Foreign Cooperation and Directorate of Naval Operations at Naval Headquarters, as well as Fleet Headquarters. He has commanded ships and has also been a Directing Staff at Defence Services Staff College. Views expressed are personal.

Colonel (Dr) **Rajan Bakshi** (Retd) is a veteran of the Indian Army and is presently an Associate Professor at the Amity Institute of Defence and Strategic Studies. Views expressed are personal.

In addition to this term, there has been another phrase which has been coined by Xi Jinping in 2011 viz., "Advance Towards the Centre of the World Stage", which was elevated to a slogan of national importance in the 19th Party Congress. During this Party Congress, the term was explained as follows:[2]

> *"China has stood up, grown rich and become strong. It will advance toward center stage and make greater contributions for mankind. By 2050, two centuries after the Opium Wars, which plunged the "Middle Kingdom" into a period of hurt and shame, China is set to regain its might and re-ascend to the top of the world.*
>
> *…China's success proves that socialism can prevail and be a path for other developing countries to emulate and achieve modernization. China is now strong enough, willing, and able to contribute more for mankind. The new world order cannot be just dominated by capitalism and the West, and the time will come for a change (Xinhua, 2017)."*

This quest for assuming centre stage along with its economic ascendancy and military might includes restoration of its borders to its perceived former glory. In this regard, the 'Map of National Shame' which China published in 1938 is of note. With the publication of this map China has claimed that during the century of national humiliation between 1839 (First Opium War) to 1937 (Japanese invasion of Nanjing), China lost territories owing to western imperialism and subsequent Japanese expansion. The Map is an interesting study, and covers Mangolia, Southeast part of Siberia, Ryukyu Islands, the First Island Chain including territory covered in the Nine-Dash Line, Vietnam, Combodia, Thailand, the Malaysian Peninsula, Myanmar, the Northeast states of India, Nepal, Tibet, going further west into Pakistan as well as most of Central Asian countries.[3]

The article discusses the territorial ambitions of China in its quest to achieve centrality on the world stage. China has undertaken a steady expansion in its territorial claims, both maritime and on land, the nine dash line, the maritime boundary conflicts with its maritime neighbours in South China Sea, creation of artificial islands to base its military, its maritime forays to the 'far seas' including its recent transit through the Tasmanian Sea. Further, the concept of neo-colonialism, using its economic clout to create a debt trap through the benign sounding, yet insidious 'Belt and Road Initiative' as well as leveraging its vast supplies of rare earth metal to get ahead in technological sector to further its territorial interests has also been discussed.[4]

Introduction

General Secretaries of the Communist Party of China have described "national rejuvenation" as the central mission of their Party since the Thirteenth Party Congress in 1987. Xi Jinping similarly describes national rejuvenation as a "strategic plan" for "achieving lasting greatness for the Chinese nation" (Xi, 2022). The formal term for this plan is the "National Rejuvenation of the Chinese Nation," a term that could be translated as the "National Rejuvenation of the Chinese Race."[5]

In addition to this term, there has been another phrase which has been coined by Xi Jinping in 2011 viz., "Advance Towards the Centre of the World Stage", which was elevated to a slogan of national importance in the 19th Party Congress. During this Party Congress, the term was explained as follows:[6]

> *"China has stood up, grown rich and become strong. It will advance toward centre stage and make greater contributions for mankind. By*

2050, two centuries after the Opium Wars, which plunged the "Middle Kingdom" into a period of hurt and shame, China is set to regain its might and re-ascend to the top of the world.

… The new world order cannot be just dominated by capitalism and the West, and the time will come for a change (Xinhua, 2017)."

This quest for assuming centre stage along with its economic ascendancy and military might include restoration of its borders to its perceived former glory. In this regard, the '*Map of National Shame'* (國恥地圖 *"Guo chi ditu"*)[7] (Figure 1), which China published in 1938, is of note. With the publication of this map, China claimed that during the 'century of national humiliation,'[8, 9] between 1842 (end of first Opium War) to 1949 (end of Chinese civil war), China lost territories owing to western imperialism and subsequent Japanese expansion. The Map is an interesting study, and covers Mongolia, Southern parts of Siberia, Outer Manchuria including Vladivostok, Ryukyu Islands, the First Island Chain including territory covered in the Nine Dash Line, Vietnam, Cambodia, Thailand, the Malaysian Peninsula, Myanmar, the Northeast states of India specifically Arunachal Pradesh, Nepal, Tibet, going further west into Pakistan as well as some parts of Central Asian countries.[10] This map was based on the analogy of a 'Mulberry leaf' enunciated in the geography textbooks published during the latter half of *Qing Dynasty* and thereafter reproduced in textbooks in the 1930s.[11] Hence, the nationalist claim that territorial losses during the century of humiliation led to the Chinese Map to look like a 'shrivelled Mulberry Leaf' eaten away by Silkworms (Figure 2).[12]

Figure 1:[13] Map of National Shame [Hong Maoxi ,eds. The New Chinese Map. Authorised by Ministry of Interior for Elementary School, Chongqing, Dongfang Yudi Xueshe,1938]

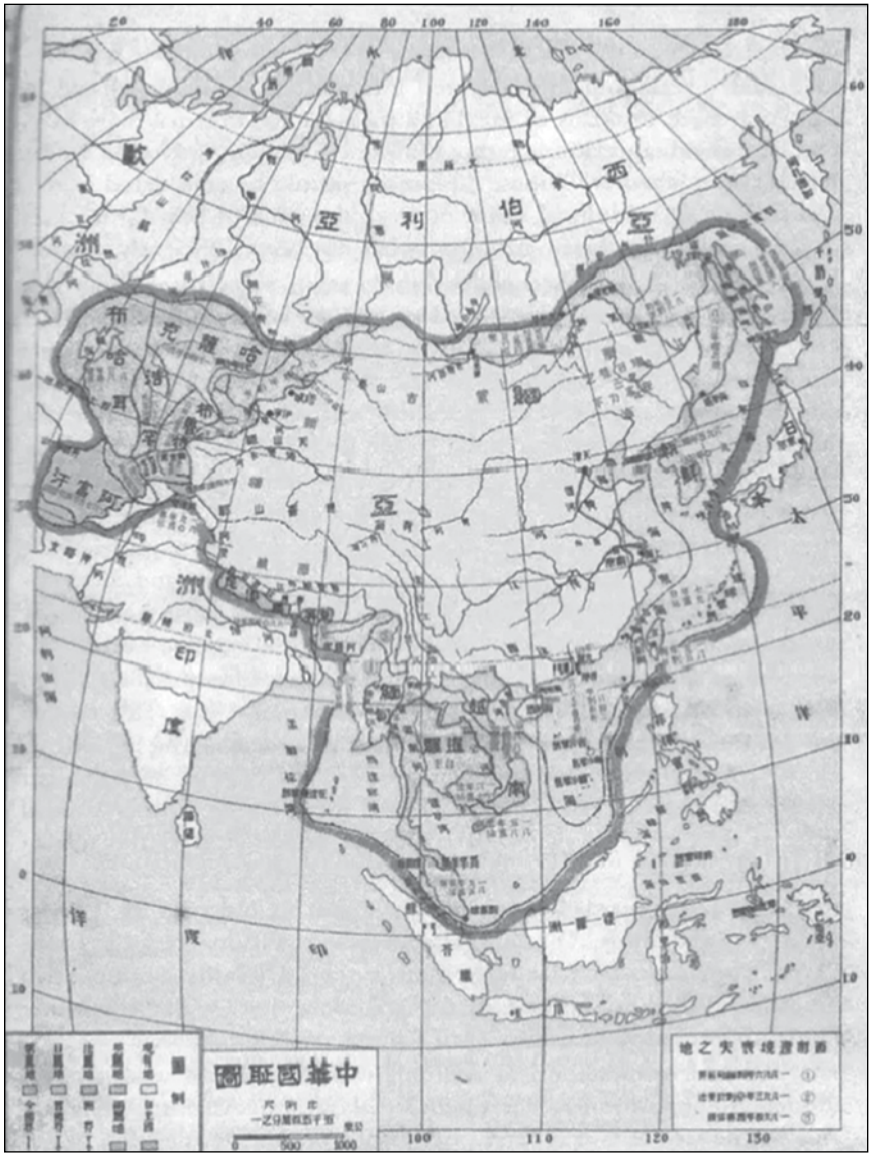
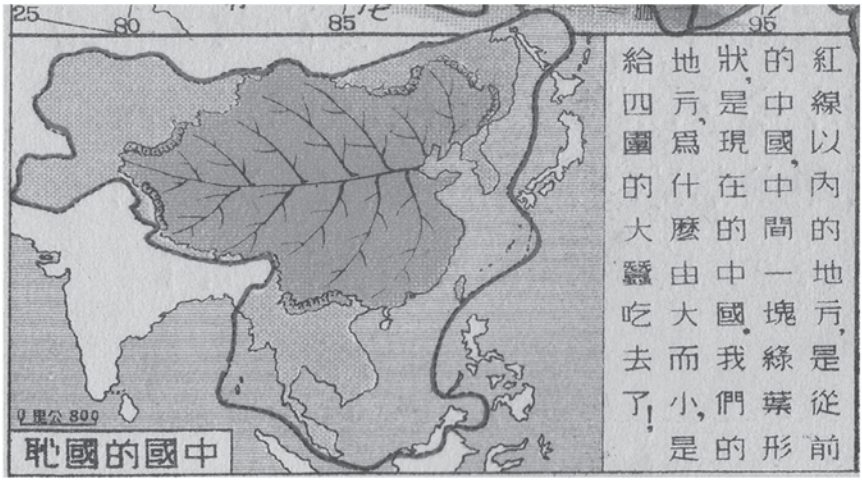


Figure 2: An illustration titled "China's National Humiliation" depicts six silkworms nibbling at a green leaf



Source: Chen Duo, ed., Zhongguo xingxiang ditu [Pictographic maps of China] (Shang hai: Zhonghua shuju, 1939), 2.[14]

In 1949, in his inaugural speech Mao Zedong described the 'century of national humiliation'[15] to justify the need for a strong China, so as to obviate any further incursions by any external power on China's sovereignty and interests and prevent the loss of territories which occurred during weak Qing empire and weak KMT government. CCP has thus used this highly nationalistic narrative to justify its domestic and foreign policies.[16] *Mao* famously declared "*China can never win genuine independence and equality by following the present policy of the Kuomintang government.*"[17] However, prior proceeding ahead, it is imperative to understand the reasons behind Chinese perception that they lost territory due to imperial expansion and Japanese invasions.

Territories Lost Prior 1949

Qing Dynasty (1644-1911) and the Unequal Treaties. In 1661, Manchus established the Qing Dynasty subjugating the Korean peninsula,

Mongolia, Taiwan, southern Russia, area corresponding to current Nepal, Myanmar, Laos and Vietnam.[18] After a prolonged battle with Russia, the Qing Dynasty officially acquired a large area of Siberia, outer Manchuria including the area fronting the Sea of Japan with Vladivostok as the major port and the adjacent Kurile islands with the signing of the 'Treaty of Nerchinsk' in 1689.[19] These territories included Inner Mongolia and Outer Mongolia.[20] After the culmination of the second Opium War, China was forced into a series of unequal treaties which led to providing unequal concessions in trade, extra-territoriality viz., inability to punish foreign offenders, right of establishing garrison in treaty and non-treaty ports, setting up foreign enclaves with administrative rights over these enclaves and cede/lease territories.[21] The territories ceded or leased due to these unequal treaties, as perceived in 1949, are as enunciated below:

- **With Russia**.[22] China believes that the Czarist regime in Russia imposed unequal treaties on a much weakened China, thereby forcing her to cede a staggering 5.5 million sq km of area (Depicted in Figure 3 and 4) and leading to the loss of Outer Manchuria (Vladivostok is a key port of this region), which cut it off from the Sea of Japan, southern Siberia, the Northwest territory including parts of Tajikistan, Kazakhstan and Kyrgyzstan as well as the Ili basin of North Xinjiang province.[23]
- **With Britain**. After the culmination of the First World War, Britain forced China with the unequal treaty of Nanking in 1842 to cede the economically vital Hong Kong to Britain (Macau was already under Portuguese control since the 16th century). The treaty was subsequently re-negotiated in 1898 for Hong Kong to be leased to Britain for a period of 99 years.[24] [25]
- **With Japan**. The loss in the first Sino-Japanese war of 1894-95 resulted in the 'Treaty of Shimonoseki' whose terms included reparations of 365 million Yen to be paid by China to Japan[26], recognize Korea as an independent state, cede Liaodong (or *Liaotung)* Peninsula, Penghu Islands and Taiwan to Japan.[27] Japan, after the Russo-Japanese war

of 1905, gained control over Manchuria, the Kurile Islands as well as the Shandong peninsula and the garrisons of Germany during the initial years of World War I.[28]

- **With France**. Annam, a state comprising large parts of modern-day Vietnam, Laos and Cambodia was a part of China during the Tang dynasty and gained independence in 938 CE. However, she remained a vassal state of China throughout. Annam was militarily forced to sign the 'Treaty of Tonkin' allowing France the entire Annam state south of the Red River, corresponding to large parts of modern day Indo-China (Vietnam, Laos and Cambodia).[29]

Consequently, over the period of next 50-60 years, China lost territories. Figure 3 and 4 depicts the overall territorial losses that China perceives occurred as a result of Western and Japanese imperialism during the weak Qing dynasty.

Figure 3[30]

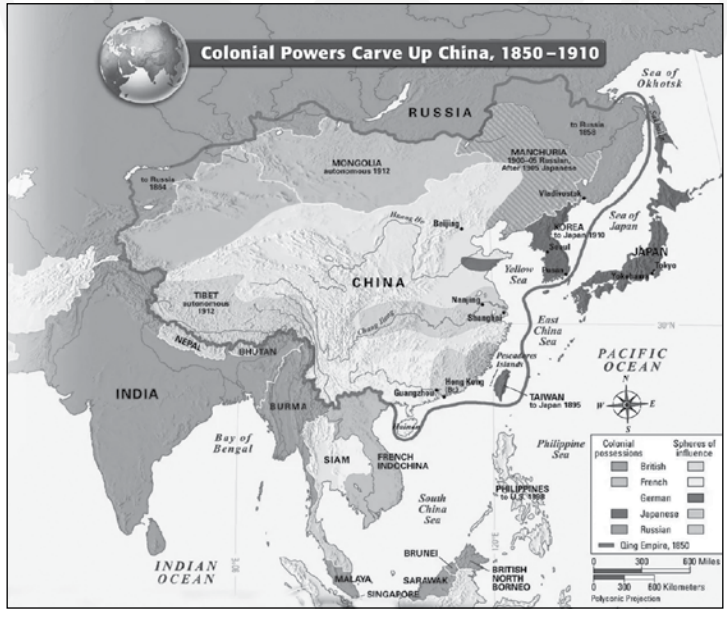


Figure 4[31]

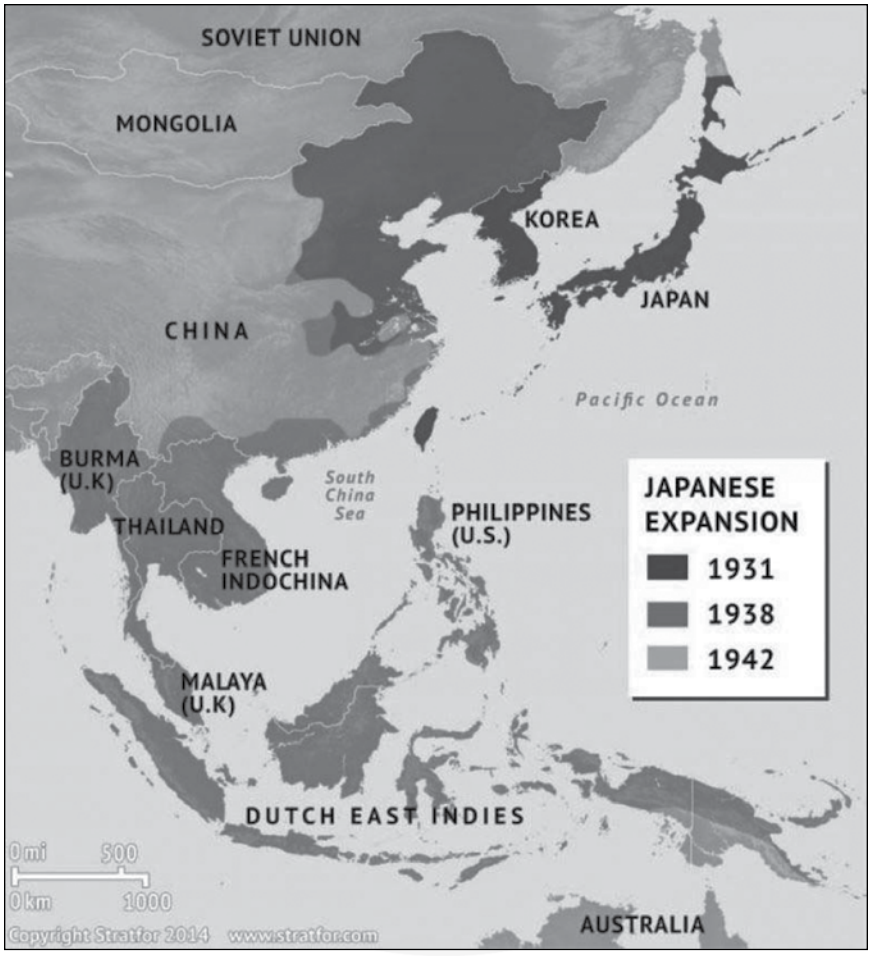
(This map is originally from the 1941 edition of *Xie Bin's A History of China's Territorial Losses*. It was published for school children just months before the Japanese occupation of Shanghai's foreign concessions. It became a standard image for displaying China's territorial losses since the Opium Wars).
Source: (Xie Bin, 1941).[32]

Territories Lost Between 1912-1939. On 1 January 1912, after the Xinhai Revolution of 1911 led by Sun Yat-sen which overthrew the Qing Dynasty, China was rechristened as the Republic of China. Sun Yat-Sen, who took over as the President, handed over the presidency to Yuan Shikai who was the leader of the Beiyang Army. However, Yuan tried to establish an empire, which led to large scale rebellion and the society being fragmented into territories controlled by warlords.[33] It was in these tumultuous times, when an inward-looking China could not adequately defend itself, that World War I happened.

Meanwhile, in 1913, the 13th Dalai Lama proclaimed the independence of Tibet as a theocratic state with rich traditions of art and culture.[34] China considers Tibet as part of China since the Yuan dynasty in 13th century when the Mongols integrated both China and Tibet in their empire.[35] However, a weakened China, at that time, could not prevent Tibet from declaring its independence, adding one more 'cartographic bead' on the map of national humiliation.

Between 1915 to 1937, the rebellion and subsequently the civil war between the Nationalist Party under Chiang Kai-Shek and the Communist Party under the leadership of Mao Zedong continued, further exacerbating the inward outlook of China. Meanwhile, with the installation of Emperor Hirohito in 1926, came the ascendancy of military in Japan. In 1931, Japan's Kwantung Army (Japanese Nationalistic Army) marched into Manchuria after the Manchurian Railway Line incident. Over a period of next seven years till 1938, Japan continued to expand its presence in China, indicated in Figure 5. In 1940, Japan occupied Indo-China, further adding to the humiliation of China.[36]

Figure 5[37]



In 1938, as can be seen, China was a much weakened and highly invaded country. This resulted in the Nationalists publishing the 'map of national shame' in 1938.[38, 39, 40] There has thus been a clear perception in China that it lost territory to the western imperialism and Japanese invasions justifying their historic legitimacy and right to regain these territories.

China's Strategy to Regain Territories

In October 1951, smarting under the century of national humiliation, the Chinese Army marched into Tibet and forced the 14th Dalai Lama to sign the 'Seventeen Point Agreement' on 24 October 1951. The agreement essentially rendered Tibet under the control of PRC and in turn the CCP. Whilst a military operation, CCP claims that this was the 'peaceful liberation of Tibet'.[41]

Russia which had gained control of Dalian and Lushun in the Liaoning province especially Port Arthur through the 'Sino-Russian Luda Land Lease Treaty' in 1898[42] returned the same to China in 1955, following the signing of 'Sino-Russian Land border Treaty'.[43]

During the 1962 India-China War, several strategic and tactical mistakes made by India allowed China a virtual walkover and gain the area of Aksai Chin.[44]

Ito Hirobumi, the first Prime Minister of Meiji Japan who had led the delegation to Shimonoseki in 1895 for determining the terms of surrender after the first Sino-Japanese war famously believed that "victor is of course entitled to claim any place he likes"[45]. CCP firmly embraced this policy during the Mao era and thereafter the Deng Xiaoping era to develop economically and militarily. China during the initial years sent numerous expeditions to Japan to learn the developmental model followed by Meiji Japan.[46] Learning their lessons from their past victories as well as failures, Deng Xiaoping famously articulated his '24-Character Strategy' which is roughly translated as "Observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership".[47, 48]

Thus, China first tried to integrate those territories, which were typically the 'low hanging fruits' and could be achieved through minimum military action or through peaceful negotiations. In this regard, the first victory was its recognition as a Permanent Member of the UN Security Council in 1971 in lieu of Republic of China (Taiwan), giving the CCP

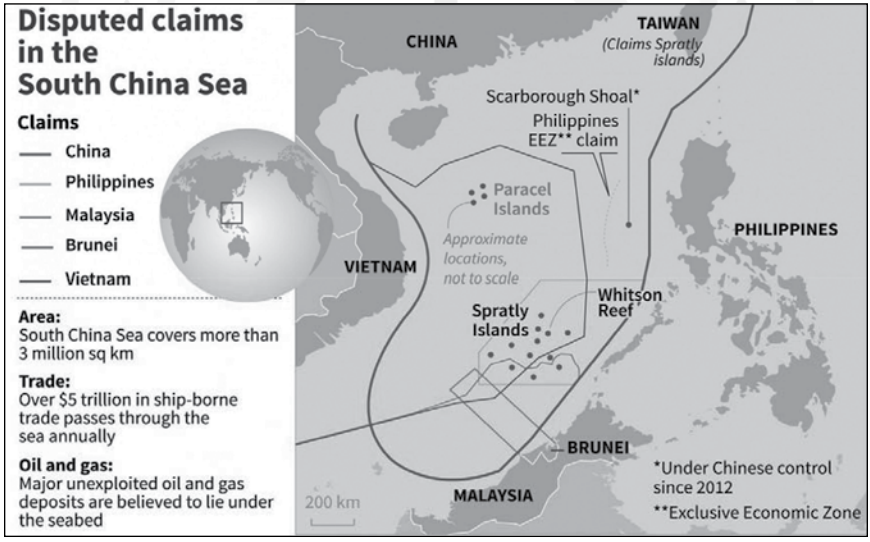
a definitive say in various world matters. Hong Kong in 1997 after the completion of the 99-year lease to Britain[49] and the peaceful handing over of Macau in 1999 from Portugal after 442 years,[50] were symbolic of China's peaceful re-integration policy.

In the maritime domain, especially in the South China Sea, China pursued this policy of forcibly occupying unmanned islands and creating its defensive line along the 'First Island Chain'. In 1947, the Kuomintang Party staked the claim in the South China Sea by promulgating a '11 dash line'. This was subsequently amended by the CCP under the chairmanship of Mao Zedong to a 'Nine-Dash Line' in 1953, excluding the Gulf of Tonkin from their original claim. This claim is invoked till this day by China. The key gains during the period prior the coronation of Xi Jinping are enumerated below:[51, 52]

- **Paracel Islands and Woody Island**. Between 1974-75, after the Vietnam War, a much-disillusioned US and a weakened Vietnam enabled China to quietly occupy the western portion of Paracel Islands including the garrison held by South Vietnamese troops. The South Vietnamese troops fled to Spratly Islands, which China claims to this date and is a matter of contention between Vietnam and China. In addition, China developed a military installation, artificial harbour and airstrip on Woody Island, which is one of the largest islands of Paracel Island group. China maintains at least 1000 troops in Paracel Islands with large scale reclamation of nearly 3000 acres to build artificial islands with military infrastructure.
- **Fiery Cross Reef**. Philippines discovered oil off Palawan basin, triggering the prospect of large hydrocarbon reserves in the South China Sea. After a decade long period of relative calm, China in March 1988, sank three Vietnamese ships killing 74 sailors near Johnson Reef in one of the most serious military confrontations in the South China Sea. China occupied the Fiery Cross Reef and Subi Reef in the Spratly's after this skirmish.

- **Legalising their Claim in the South China Sea**. In February of 1992, China passed a law which laid claim to the entire South China Sea based on their perception that China exerted control over the South China Sea since the Western Han dynasty. The inability of ASEAN and US from dislodging China from these islands or dissuade any further incursions on the island has further strengthened the Chinese beliefs.
- **Mischief Reef**. In Jan 1996, Chinese naval ships engaged in a 90 min battle with a Philippines Gun boat near Capone Island of Mischief Reef, which is a part of the Spratly Island Chains. China after winning this short skirmish landed its forces on Mischief Reef.

Figure 6[53]



Grand Strategy of China

China's Grand Strategy revolves around its vision of restoring its position as the pre-eminent power in the world, around which the global geopolitics revolves reflective of its historical status as the

leading civilization.[54] The key competitor that China perceives in these endeavours is the United States of America. China's endeavours thus have focused on reducing the dependency of other countries on the United States by presenting a viable and more acceptable alternative.[55]

China's expansionism has been based on four major imperatives viz. (a) Regain lost territories through diplomatic and peaceful negotiations, which China has achieved through treaties. (b) Re-integrate key territories viz. Taiwan, Hong Kong, Outer Manchuria, Outer Mongolia etc. to consolidate its perceived sovereign regions and border definition. (c) Gain overseas bases in Pacific, Indian Ocean and the Atlantic, especially in countries inimical or on poorer terms with the United States of America to facilitate global deployment of their forces. (d) Replace the United States as the pre-eminent power in Asia and the Pacific.[56]

In this regard, China's worldview is of four concentric rings with Beijing at the centre of world stage. The first ring covers China itself, and this is the most important and sensitive area. The second concentric ring is China's periphery. The next ring outwards comprises the larger Asia-Pacific region, which China believes is its rightful sphere of influence. The final ring stretches the rest of the way around the globe, encompassing increasingly important areas such as the Middle East and Africa.[57]

It is thus evident that China has territorial ambitions beyond consolidating its borders and aims to regain territories lost during the century of national shame, as well as have access/gain control over real estate/bases overseas, even beyond the Asia-Pacific. The former would need military action and will be discussed subsequently. However, the latter pertaining to the third and the fourth ring is being achieved through the Flagship program of 'Belt and Road Initiative'.

Belt and Road Initiative. In an effort to provide a viable alternative to the United States of America as well as to assure the world that China's rise is concomitant with global development, Xi Jinping launched his flagship program of Belt and Road Initiative in 2013. On the surface, China provides loans and other assistance for a multi-continent infrastructure project that includes an overland Silk Road Economic Belt, a Maritime Silk Road, and a Digital Silk Road. It has expanded to include Asia, Europe, Africa, Latin and South America and Oceania. In this regard, the overtures made by China with various nations in the pacific has been critical. In addition, morally questionable flexible terms with the dispensation of the day have made BRI a popular choice amongst the poorer African and Pacific Island nations. But the often discussed debt trap and thereafter leveraging this debt to gain access to real estate and strategic control in these recipient countries has become a reality. Chinese military bases in Djibouti, Hambantota in Sri Lanka, Feydhoo Finolhu Island in Maldives, The Ream Naval base in Cambodia etc. are classic examples of these.[58, 59]

Neo-Colonialism. A natural extension of the BRI has been Neo-Colonialism that China has followed to gain significant leverage in the poorer country. "Kwame Nkrumah (1965- 'Neo-Colonialism—The Last Stage of Imperialism') developed the term neo-colonialism to describe a country in theory independent yet has its economic and political policies largely controlled by external powers."[60] AA Fatouros in his 1965 work 'Sartre on Colonialism' also posited that "Neo-colonialism arises as the successor of colonialism, by which developed nations can no longer use military force to exert control and rather mask their exploitation through economic means."[61] The Belt and Road Initiative has all the characteristics listed above resulting in many countries, especially the island nations in the Pacific and IOR as well as the African countries, deeply indebted and under the influence of China.[62]

Territorial Expansion through Military Means—The First and the Second Ring

On 08 July 2013, *Wen Wei Po*, a Hong Kong daily having close links with CCP published an article titled "The Six Wars to be Fought by China in Next 50 Years".[63] According to this article, China will wage six wars to regain territories lost during the 'century of national shame'. These wars include the following:[64] [65] [66]

(a) The war to unify Taiwan (2020–2025).
(b) The war to recover the various islands of the South China Sea (2025–2030) specifically the Spratly's, Paracel and the Scarborough Shoals.
(c) The war to recover southern Tibet (2035–2040).
(d) The war to recover Diaoyutai and the Ryukyus (2040–2045).
(e) The war to unify Outer Mongolia (2045–2050).
(f) The war to recover the territory seized by Russia (2055–2060).

The article, that was removed within a short time, was purportedly printed with the tacit approval of CCP and PLA.[67] The article gives a keen insight into the possible territorial sovereignty that CCP has been declaring since 1949. Are these wars inevitable? Whilst the dynamic geo-political situation makes crystal gazing difficult, the possibilities of the above are being discussed in the subsequent paragraphs.

Taiwan. Of all the purported wars that have been enunciated, the most critical and in that regard the first amongst equals is the re-unification of Taiwan with China's mainland. In this regard, there is a core belief that Taiwan's integration with mainland China is part of their founding principles of maintaining territorial sovereignty (One China Policy), and any action, peaceful or military, would be akin to a civil war to suppress the separatist regime in Taiwan. Economically, Taiwan's Semiconductor industry is being keenly eyed upon by China and the

re-unification would enable China to become the leader in this field. Most importantly, Taiwan is the central cog in the First Island Chain allowing China the much-needed defence in depth as well as a strategic oversight location vis-à-vis the maritime trade in the region. Annexation of Taiwan would also undermine US interests in the region, which is one of the unstated goals of China, including challenging the Freedom of Navigation Operations. Last but not the least, it is imperative for China to unify Taiwan since, Taiwan's democratic system directly undermines the much-professed successful Chinese Communist ideology of CCP.[68] Diplomatically, China has undermined Taiwan's position as an independent and separate nation by using its Veto powers to block its participation in international organisations.[69] In addition, at least three quarters of the member states of the United Nations support China's claims over Taiwan. Of the 19 major island nations in the Pacific Ocean, only three nations diplomatically support and recognise Taiwan, whilst 11 support and recognise China's legitimacy over the island of Taiwan.[70] With the installation of Trump 2.0 government, and his realist outlook, there is confusion within the strategic community as to whether the USA would honour the 'Taiwan Relations Act' of 1979 and come to Taiwan's aid or if they come, then to what extent. However, recently concluded 'Exercise Strait Thunder 2025A'[71] undertaken by China indicates that it is highly possible that whilst the world is reeling under the 'Tariff Wars', China may make a blitzkrieg attack on Taiwan, the possibility of which cannot be ruled out. USA's and NATOs pre-occupation with the Israel-Hamas war as well as the Russian-Ukraine war may just be the moment which China capitalises upon. The timeline certainly fits with that of the article of 2013.

Territories in South China Sea. China has been, since 1975, making military and coercive overtures in the South China Sea. Their military presence in the Paracel and Spratly's is well documented.

Concomitant with the fact that the South China Sea is likely to contain 11 billion barrels of oil reserves[72] and are also a busy transit lane for merchant marine, China is likely to continue asserting its claims within the 'Nine-Dash Line'. However, a firm military action to gain control of these islands would be subject to its success in annexation of Taiwan as only then will they get the launch pad from which to exert control over these islands and be able to counter any NATO action in the region.

Arunachal Pradesh. Arunachal Pradesh is an integral part of India and is well defended by the Indian Security Forces. China considers Arunachal Pradesh as an integral part of Tibet¸ which China already controls and hence claims sovereignty over Arunachal Pradesh based on historicity and calls it Zangnan.[73] China's claims are based on the historical ties between the Tawang Monastery and Tibet's Lhasa Monastery, as well as the diaspora drawing similarity and association with Tibet. China further refutes the MacMahon Line drawn during the KMT Nationalist Government as CCP, which took power in October 1949, does not consider any border agreements prior 1949 as legitimate.[74] In August 2023, China promulgated a new 'Standard Map' (Figure 7)[75] which included Arunachal Pradesh and Aksai chin as part of their territories, indicating them to be contested by India. Overt military efforts till date have not been successful. It is thus highly possible that China would use water diplomacy being the upper riparian state with respect to the Brahmaputra River as strong-arm tactics to put pressure on India. In any case, it is evident, that China is likely to bide its time, make efforts at weakening India, try and gain a foothold at Doklam to gain control over the Chicken's Neck at the western border of North East states as well as encircle the region through its BRI project in Nepal, Bangladesh and Myanmar prior making any overt military efforts to gain control over Arunachal Pradesh.

Figure 7:[76] **China Standard Map Edition 2023**

Diaoyutai and the Ryukyus including Okinawa. The 'Standard Map' published in 2023 by China included a '10 Dash Line', essentially adding an additional line to encompass Taiwan and the Ryukyus. The claims are based on their historical control during the Ming dynasty. The *Diaoyu* and the *Ryukyus* were used as navigational checkpoints by Admiral

Zeng He and other mariners at that time and accepted the suzerainty of the Emperor at that time.[77, 78] Whilst the article talks of this war between 2040-2045, it is to be considered that if and when China gains control of Taiwan any operation in the South China Sea or towards Ryukyus would conflagrate into a major war between China and the NATO. Hence, whether this operation would happen, is best left to be pondered. Again, Taiwan annexation is the first and the key check post for China prior any operation in this region.

The balance two territorial 'conquests' have been proposed by the Chinese author based on the 1941 Map (Figure 4) wherein China claims sovereignty over Mongolia, Outer Manchuria, parts of Central Asia and Southern Siberia. The timing proposed is between 2045-2055 when as Xi Jinping declared that, China would be the pre-eminent power at that time. Considering the realist aspirations of various countries, the failure of the United Nations to prevent any war as has been evident in the recent decades as well as the possibility that the world powers may not have adequate wherewithal to counter China's 'might is right' approach, these military re-integrations may occur and cannot be ruled out. However, what is evident is China's vociferous claims for Vladivostok to be returned to China, which China eyes as its own.[79] In addition, considering the access that it provides to the Sea of Japan and gets it closer to the highly contested and lucrative Arctic, it is highly possible that China would inevitably pressurise Russia to make good these claims at some point. In the interim, China has strengthened its BRI investments and is slowly gaining footholds into Mongolia and Southern Russia through its BRI projects connecting Eastern China and Russia to Central Asia.

Conclusion

'National Rejuvenation' and 'Advancing towards the Centre of the World Stage' are the two key tenets that has been driving CCP and in effect

China during the past seven and a half decades. Any and every strategy that has been formulated has been towards meeting these two goals. For achieving this, China has bided its time, developed its military and economy, slowly gained diplomatic clout and shaped the environment. 'Territorial Sovereignty' being a central theme has been driven by the 'Century of National Humiliation' and the scar that the territorial losses left on the psyche of the CCP leaders. China has maintained a national as well as international narrative that China aims for a peaceful rise to its rightful place on the global stage, commiserate with its civilizational greatness and ancient roots.

Chinese leaders have been driven by Mao Zedong's credo that China should not be beholden to any nation for its independence and administration. In addition, a critical factor has been the security of CCPs rule and its primacy within China as well as its influence upon various nations. Accordingly, China's understanding of its territories has been commiserate with its original expanse during the early period of Qing dynasty, which provided it the reach that it desired to resources to sustain its population as well as access to trade routes and strategic territories. In this regard, the 'Map of National Shame' published in 1938 defines China's claims which it argues as its sovereign right. CCP has refuted every border agreement prior to 1949 scoffing at their legitimacy and its perception of their unequal nature. Hence, China in its immediate neighbourhood claims rights over parts of central Asia, Southern Siberia, Outer Manchuria (which has the port of Vladivostok) lost to Russia; Mongolia, which it considers as Outer Mongolia; Taiwan which it argues was occupied by the Nationalist rebels and hence is an inalienable part of mainland China, the Ryukyus lost to Japan; Arunachal Pradesh or Zangnan which it purportedly lost to the partial delineation which occurred during the independence of India; the 'Nine-Dash Line' which it now has amended to the '10 Dash Line' in the South and the East China Sea. In addition, China through its BRI has claimed inroads into

Cambodia, and Laos, part of the Annam State and corresponding to modern day Indo-China region.

The 'Four Ring' worldview of Chinese leaders further proves CCPs territorial ambitions, wherein every aspect of their Comprehensive National Power viz. DIME has been utilised to gain territories/bases/influence in Asia, Pacific, Africas as well as in South Americas. The Belt and Road Initiative has been the vehicle used by Xi Jinping to attain overseas bases, economic leverage and political influence in these regions.

The July 2013 article in *Wen Wei Po*,[80] also gave an insight into the possible efforts that China may undertake in the near and subsequent future to regain its territories. Whilst Taiwan annexation as well as gaining control over the Paracel, Spratlys and the Scarborough Shoals seem realistic in their likelihood, the balance territorial reintegration may not be an immediate priority for China. However, Taiwan operation itself may trigger the 'Thucydides Trap' with the United States likely to get involved to counter China's hegemony in the region. In addition, any other re-integration efforts which would lead to direct confrontation with Russia or India or Japan as the case maybe would be at a time of China's choosing, when it is assured of its victory in accordance with Sun Tzu's teachings.

China has always been the inscrutable dragon, whose intentions can only be discerned from the occasional signalling that it does. In this regard, a clear signal transmitted has been its quest to achieve centrality in global affairs and gain back the territories that it lost (as it perceives) due to maleficent imperialists. India and the world thus need to be on notice and lookout for triggers which may lead to China gaining the access to these territories.

Notes

1. Fùxīng, Zhōnghuámínzú Wěidà. n.d. "Great Rejuvenation of the Chinese Nation." *The Centre for Strategic Translation*, https://www.strategictranslation.org/glossary/great-rejuvenation-of-the-chinese-nation. Accessed on February 23, 2025.

2. Zhōngyāng, Zǒu Jìn Shìjiè Wǔtái. n.d. "Advancing Towards the Centre of World Stage." *The Centre for Strategic Translation,* https://www.strategictranslation.org/glossary/advancing-towards-the-center-of-the-world-stage. Accessed on February 23, 2025.
3. Wade, George. 2013. "China's Six Wars in Next 50 Years." *The Strategist,* November 26, https://www.aspistrategist.org.au/chinas-six-wars-in-the-next-50-years/. Accessed on February 21, 2025.
4 Rishi, Ajay Mishra and Shraddha. 2024. "China's Imperial Design; The Drive from Trade and debt Diplomacy." *Organisation for research on China and Asia,* August 29, https://orcasia.org/article/853/chinas-imperial-design. Accessed on February 21, 2025.
5. Ibid., n. 1.
6. Ibid., n. 2.
7 Chang, Yu-Chi. 2024. "Leaves, Silkworms, Yue Fei: ways of Imagining the Territory in 1930s China." *Twentieth Century China* (John Hopkins University Press) 49 (2): 89-110, https://doi.org/10.1353/tcc.2024.a925422.p96. Accessed on March 8, 2025.
8. Guóchǐ, Bǎinián. 2019. "Century of National Humiliation." *The Centre for Strategic Translation.* https://www.strategictranslation.org/articles/from-the-rise-of-populism-to-the-return-of-history. Accessed on March 4, 2025.
9. Metcalf, Mark. 2020. "The National Humiliation Narrative: Dealing with the Present by Fixating on the Past." *Association of Asian Studies.* Fall. https://www.asianstudies.org/publications/eaa/archives/the-national-humiliation-narrative-dealing-with-the-present-by-fixating-on-the-past/. Accessed on March 4, 2025.
10. Wade, George. 2013. "China's Six Wars in Next 50 Years." *The Strategist,* November 26, https://www.aspistrategist.org.au/chinas-six-wars-in-the-next-50-years/. Accessed on February 21, 2025.
11. Chang 2024, Ibid., pp. 92-93.
12. Ibid., p. 93.
13. Wade, Ibid.
14. Chang, Ibid., p. 99.
15. Metcalf, Ibid.
16. Ibid.
17. Communist Party of China. 1999. "Article 55 of the Common Program of the People's Republic of China 1949-1954." commonprogram.science, http://commonprogram.science/art55.html#. Accessed on March 9, 2025.
18. Chey, Ong Siew. 2008. *China Condensed; 5000 Years of History and Culture.* Edited by Melvin Neo. Singapore: Marshall Cavendish Editions, p. 58.
19. Ibid., p. 60.
20. Ibid., p. 60.
21. Lang, Wang Jian. 2016. *Unequal Treaties and China.* Edited by Li Tong and Phoebe Poon. Translated by Li Tong. Vol. 1. Beijing: SilkRoad Press. pp. 2-15.
22. Ghosh, S K. 1977. "Sino-Soviet Border Talks." *India Quarterly* (Sage Publications) 33(1): 57-61, https://doi.org/10.1177/097492847703300105, pp. 57-58. Accessed on March 10, 2025.

23. Ibid., pp. 57-58.
24. Chang, Ibid., pp. 90-92.
25. Lang, ibid. p. 6.
26. Ohno, Kenichi. 2018. *The History of Japanese economic Development; Origins of Private Dynamism and Policy Competence*. London and New York: Routledge; Taylor and Francis Group, p. 44.
27. Iriye, Akira. 1989. "Japan's Drive to Great Power Status." Edited by Marius B Jansen. *The Cambridge History of Japan; The Nineteenth Century* (Cambridge University Press) 5: 721-782, p. 767.
28. Lang, Ibid., pp. 5-9.
29. Pike, John. 2012. "Annam Tributary to China." *GlobalSecurity.org*. April 3, https://www.globalsecurity.org/military/world/vietnam/annam-tributary.htm#:~:text=The%20name%20Annam%20is%20Chinese%2C%20from%20the%20term,Tang%20collapsed%2C%20it%20remained%20a%20Chinese%20tributary%20state. Accessed on March 12, 2025.
30. Communist Party of China, Ibid.
31. Ibid.
32. Ibid.
33. Chey, Ibid. p. 71.
34. Liu, Joie. 2024. "Mountains of Resistance: The Past and Present of Tibet's Quest for Independence." *Harvard International review.* November 6, https://hir.harvard.edu/mountains-of-resistance-the-past-and-present-of-tibets-quest-for-independence/. Accessed on March 13, 2025.
35. Rastogi, Nina Shen. 2008. "Why Does China Care about Tibet." *SLATE.* March 28, https://slate.com/news-and-politics/2008/03/why-does-china-care-about-tibet-and-when-are-monks-allowed-to-get-violent.html. Accessed on March 13, 2025.
36. Japan-Guide.com. 2002. "Taisho and early Showa Period (1912-1945)." *Japan-guide.com,* June 9. https://www.japan-guide.com/e/e2129.html. Accessed on March 14, 2025.
37. stratfor.com. 2014. "Japan's Territorial Expansion 1931-1942." *RANE WORLDVIEW.* https://worldview.stratfor.com/article/japans-territorial-expansion-1931-1942. Accessed on March 14, 2025.
38. Chinasage. 2024. "Qing or Manchu Dynasty 1644-1911—the End of Emperors." *Chinasage,* October 2, https://www.chinasage.info/qing-dynasty.htm#. Accessed on March 3, 2025.
39. Wade, Ibid.
40. Chang, Ibid., pp. 90-92.
41. Danxu, Yang. 2024. "From 1949 to the present, the growth of China's territorial area is detailed." *LaiTimes,* July 4, https://www.laitimes.com/en/article/6x6dn_7dinc.html. Accessed on March 15, 2025.
42. Xiao, Yiyang. 2025. "Heritagization of the Colonial Period in Dalian." *The Palgrave Encyclopedia of Cultural Heritage and Conflict*, February 19: 1-14, https://doi.org/10.1007/978-3-030-61493-5_123-1. Accessed on March 19, 2025.

43 Danxu, Ibid.

44. Knowledge of India. n.d. "The Day India Took Revenge of 1962: The Cho La Incident." knowledgeofindia.com, https://knowledgeofindia.com/the-cho-la-and-nathu-la-border-fight/#:~:text=The%20answer%20to%20all%20these%20questions%20is%20the,India%20and%20China%20after%20the%20war%20of%201962. Accessed on March 17, 2025.

45. Iriye, Ibid., p. 767.

46 Vogel, Ezra F. 2019. *China and Japan; Facing History.* Cambridge, London: The Belknap Press of Harvard University Press. pp. 133-135, 144.

47. Pike, John. 2013. "Deng Xiaoping's 24—Character Strategy." *GlobalSecurity.org*. December 28, https://www.globalsecurity.org/military/world/china/24-character.htm. Accessed on March 14, 2025.

48. Mastro, Oriana Skylar. 2021. "Chinese Grand Strategy." https://www.researchgate.net. May, file:///C:/Users/naren/Downloads/2021_ChineseGrandStrategyOrianaSkylarMastro.pdf.p6. Accessed on March 20, 2025.

49 BBC. 2022. "Hong Kong's handover: How the UK returned it to China." *BBC*. July 1. https://www.bbc.com/news/world-asia-china-40426827. Accessed on March 17, 2025.

50. FP Explainers. 2024. "25th anniversary of Macau handover: When Chinese rule returned to city." *FirstPost*. December 20, https://www.firstpost.com/explainers/25th-anniversary-macau-handover-chinese-rule-13846034.html. Accessed on March 17, 2025.

51. Council on Foreign Relations. 2025. "1895 – 2024; China's Maritime Disputes." *Council on Foreign Relations,* https://www.cfr.org/timeline/chinas-maritime-disputes. Accessed on March 19, 2025.

52. Mastro, Ibid., pp. 10-11.

53. Lee-Brown, Bec Strating and Troy. 2023. "Tensions in South China Sea continue, but ASEAN states successfully resolve maritime disputes." *The Jakarta Post*. May 3, https://www.thejakartapost.com/opinion/2023/05/03/tensions-in-south-china-sea-continue-but-asean-successfully-resolves-maritime-disputes.html. Accessed on April 9, 2025.

54. Global Institute of National Capability. 2024. "CN China's Grand Strategy." *Global Institute if National Capability.* September 24, https://www.ginc.org/chinas-grand-strategy/#:~:text=This%20article%20dissects%20the%20components%20of%20China%E2%80%99s%20Grand,Military%2C%20Economic%29%20framework%2C%20regional%20focus%2C%20and%20resource%20allocation. Accessed on Mar 14, 2025.

55. Ibid., p. 5.

56. Wesley-Smith, Terence. 2013. "China's Rise in Oceania; Issues and Perspectives." *Pacific Affairs* 86 (2): 351-372. wvcwinterswijk.nl. 2024. Map of Japan during WW II - United States Map. https://wvcwinterswijk.nl/map-of-japan-during-wwii/., p. 353. Accessed on March 21, 2025.

57. ANI Reporter. 2020. "China's grand strategy and how it intends to attain it." *The Economic Times*. October 20, https://economictimes.indiatimes.com/news/defence/chinas-grand-strategy-and-how-it-intends-to-attain-it/articleshow/78765054.cms. Accessed on April 5, 2025.

58. Mastro, Ibid., p. 19.

59. James McBride, Noah Berman and Andrew Chatzky. 2023. "China's Massive Belt and Road Initiative." www.cfr.org. February 2, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative. Accessed on March 20, 2025.
60. Murray, Caitlin. 2022. "An analysis of China's Belt and Road initiative and its neo-colonial ambitions." *Routes; The Journal for Student geographers* 2 (3): 176-182, https://routesjournal.org/2022/04/07/r2099/.p176. Accessed on March 20, 2025.
61. Ibid., p. 176.
62. Ibid.
63. Graceffo, Antonio. 2024. "An Insight into China's Six wars." *Taipei Times*, July 17: 8-8. https://www.taipeitimes.com/News/editorials/archives/2024/07/17/2003820902. Accessed on April 2, 2025.
64. Dangwal, Ashish. 2024. "From India To Mongolia—Six Wars That China Will Fight To Regain "Lost Glory" By 2060: Chinese State Media." *The Eurasian Times*. May 25, https://www.eurasiantimes.com/ne-from-india-japan-to-mongolia-six-wars/. Accessed on March 22, 2025.
65. Graceffo, Ibid.
66. Wade, Ibid.
67. Ibid.
68. Pierce, Logan. 2025. "5 Key Reasons Why Does China Want Taiwan for Reunification." *DefenceFeeds.com*. February 19, https://defensefeeds.com/analysis/why-does-china-want-taiwan/. Accessed on April 4, 2025.
69. Ibid.
70. Thomson, Jono. 2025. "Global support for China's stance on Taiwan increases." *Taiwan news*. January 16, https://www.taiwannews.com.tw/news/6016993. Accessed on April 4, 2025.
71. Ryan, Mick. 2025. "hina's Lightning Operation Around taiwan." *Futura Doctrina*. April 4, https://mickryan.substack.com/p/chinas-lighting-operation-around. Accessed on April 5, 2025.
72. Centre for Strategic and International Studies and Asia maritime Transparency Initiative. 2025. "South China Sea Energy Exploration and Development." *Centre for Strategic and International Studies and Asia maritime Transparency Initiative*. https://amti.csis.org/south-china-sea-energy-exploration-and-development/. Accessed on April 5, 2025.
73. FP Explainers. 2023. "Why does China keep claiming Arunachal Pradesh and Aksai Chin?" *Firstpost.com*. August 29, https://www.firstpost.com/explainers/why-does-china-keep-claiming-arunachal-pradesh-and-aksai-chin-13054082.html. Accessed on April 5, 2025.
74. Ibid.
75. Ibid.
76. Ibid.
77. Lee, Joyman. 2011. "Senkaku/Diaoyu: Islands of Conflict." *History Today*, May. Accessed April 5, 2025. https://www.historytoday.com/archive/senkakudiaoyu-islands-conflict.

78. Goldman, Corrie. 2015. "Stanford scholar illuminates history of disputed China Sea islands." *Stanford Report*. August 5, https://news.stanford.edu/stories/2015/08/islands-chiang-diaries-080515. Accessed on April 5, 2005.
79 Brar, Aadil. 2024. "China Eyes Russia's Far East as Putin's 'History Lesson' Backfires." *Newsweek*. February 13, https://www.newsweek.com/china-russia-vladivostok-lesson-far-east-backfires-1869327. Accessed on April 5, 2025.
80. Graceffo, Ibid.

Taiwan's Military Strategy: Adapting to an Asymmetric Threat

Tushar Mittal

Abstract

Taiwan's security environment is defined by the overwhelming military superiority of the People's Republic of China (PRC) and its People's Liberation Army (PLA). Confronted with an adversary that leverages rapid modernization, multi-domain capabilities, and a diverse array of non-kinetic tools, Taiwan has recalibrated its defence strategy away from conventional force-on-force engagements toward an asymmetric posture. This paper explores the evolution of Taiwan's military strategy, including the adoption of a "porcupine strategy," the development of robust coastal and air defences, and the hardening of cyber and information domains to deter aggression and sustain resilience in a contested Indo-Pacific. In addition, the paper analyses the vital role of international partnerships, particularly with the United States and like-minded democracies, and discusses the strategic challenges that Taiwan must overcome. Through a detailed examination of emerging PLA threats and Taiwan's corresponding military responses, the paper provides a comprehensive look at how asymmetric warfare can level the strategic playing field.

Colonel **Tushar Mittal** is Senior Fellow at the Centre for Land Warfare Studies (CLAWS), New Delhi. Views expressed are personal.

Introduction

Taiwan's strategic environment is inherently complex. While the island's democratic values and economic dynamism have allowed it to flourish, these very qualities have simultaneously rendered it a focal point of strategic competition between China and the broader international community. The People's Liberation Army (PLA) has, over the last decade, executed a series of military reforms under the leadership of Xi Jinping, emphasizing advanced capabilities such as power projection, joint operations, and amphibious assault preparedness (Tossi, 2023). Given the significant disparity in conventional military power between Taiwan and the PRC, Taiwan's defence establishments have increasingly turned to an asymmetric military strategy designed to complicate and deter any potential Chinese military incursion.

This paper examines Taiwan's evolving military strategy, which is underpinned by three core elements: deterrence, resilience, and asymmetric warfare. In particular, Taiwan's "porcupine strategy"—a doctrine built around the deployment of cost-escalation measures and flexible, decentralized tactics, that aims to render any PLA aggression (Bursi, 2023). The paper is structured to first assess the strategic context, outlining the growing threat from the PLA; next, it details the specific elements of Taiwan's asymmetric response including developments in missile and drone warfare, coastal and air defences, cyber capabilities, and the fortification of international alliances. Finally, the paper identifies key challenges and future directions for Taiwan's defence planning.

Strategic Context: The PLA's Growing Threat

Over the past decade, PLA has undergone transformative changes, designed to expand China's regional influence and deter external interference. Several aspects of PLA modernization are especially relevant to Taiwan's strategic calculus:

A2/AD Capabilities

China's anti-access/area denial (A2/AD) strategy is a critical element of its military modernization. By deploying advanced missile systems, long-range bombers, and sophisticated naval assets, the PLA seeks to establish a robust zone of denial around its periphery, effectively preventing US intervention in the Taiwan Strait (CRS, 2024). This capability forces potential adversaries to reckon with a layered defensive perimeter that complicates rapid reinforcement or relief operations. Taiwan's defence planners are well aware that any successful PLA campaign would not be limited to a swift invasion but would also involve extensive missile barrages and integrated joint operations designed to paralyze the island's ability to defend itself.

Amphibious Assault Readiness

Central to China's military strategy is the enhancement of amphibious warfare capabilities. The expansion of the PLA's amphibious transport fleet including the commissioning of Type 075 landing helicopter docks, significantly increases the likelihood of a forceful amphibious landing on Taiwanese shores (Kartik Bommakanti, 2024). This readiness to launch large-scale, multi-domain assaults means that Taiwan must develop effective countermeasures, such as mobile coastal defences and minefields, to disrupt PLA landing operations and mitigate rapid force projection.

Grey Zone Warfare

In addition to conventional threats, the PLA's evolving grey zone tactics pose a subtler but no less significant challenge. Grey zone warfare refers to actions that fall short of traditional open conflict, including cyberattacks, disinformation campaigns, economic coercion, and persistent airspace violations. These operations are designed to erode public confidence in Taiwan's institutions and undermine the island's ability to mobilize both

politically and militarily (Saxena, 2024). By exploiting ambiguity, grey zone tactics can destabilize Taiwan without triggering a full-scale military response—a tactic that has compelled Taiwanese defence planners to invest in robust cyber defences and rapid information countermeasures.

Blockade Strategy

Another critical facet of the PLA's strategic repertoire is the potential to implement a blockade. A naval blockade, if executed effectively, could choke off Taiwan's maritime supply lines, disrupt trade, and force political concessions without the need for an outright invasion (Jestrab, 2023). This strategy leverages China's growing naval capabilities and its ability to project power across the Indo-Pacific. Taiwan's limited geographic area intensifies the risk of such a blockade, making the development of resilient maritime countermeasures and rapid reaction forces a top priority. Given these converging threats, Taiwan has embarked on a series of strategic reforms aimed at complicating any PLA operational calculus. The emphasis is no longer on matching the Chinese military in a symmetric, conventional contest; rather, it is on creating a defence structure that exploits Taiwan's unique advantages, forces PLA decision-makers into uncertainty, and maximizes the costs of any attempted aggression.

Taiwan's Evolving Military Strategy

Recognizing the clear asymmetry between its own capabilities and those of the PLA, Taiwan's military strategy has evolved significantly over recent years. Instead of preparing for a direct, conventional confrontation, Taiwan has shifted its focus toward an approach that emphasizes asymmetric deterrence, multi-domain operations, and rapid adaptability.

Transition from Conventional to Asymmetric Deterrence

Historically, Taiwan's defence doctrine was centred on the belief that conventional military superiority would secure its sovereignty. However,

the rapid pace of PLA modernization and the advent of multi-domain operations necessitated a paradigm shift. Taiwan's leadership now acknowledges that matching China's advanced missile systems or amphibious warfare assets head-on is both impractical and strategically unsound. Instead, the island's military planners have embraced an asymmetric strategy designed to inflict disproportionate damage on any invading force, making the cost of aggression prohibitively high.

The "Porcupine Strategy"

Central to this new doctrine is what analysts have termed the "porcupine strategy." Much like the 'animal that deters predators with its quills,' Taiwan's approach is to embed its military with a multitude of inexpensive but highly effective defensive measures that complicate PLA operations. The strategy encompasses several key components:

- **Missile and Drone Warfare**: Taiwan is modernizing its indigenous missile systems, such as the Hsiung Feng series of anti-ship missiles, which are designed to target and neutralize Chinese naval vessels (Wu, 2023). Additionally, the development of loitering munitions commonly known as "suicide drones" like the Chien Hsiang, provides Taiwan with a flexible, low-cost option for targeting high-value enemy assets (Dangwal, 2023).
- **Swarming Tactics**: By deploying a large number of small, fast missile boats and unmanned aerial vehicles (UAVs), Taiwan seeks to overwhelm and disrupt PLA operations (Rosenbach, 2025). This "swarming" approach not only saturates enemy defences but will also force the PLA to allocate resources to counter a multitude of threats rather than focusing on a singular invasion force.
- **Mobile Defence Units**: In recognition of the vulnerability inherent in static defence systems, Taiwan is training and equipping highly mobile units capable of engaging in anti-armour and anti-air operations (Revels, 2023). These agile forces are designed to operate

in urban and rugged terrains, making it difficult for occupying forces to establish secure footholds.

- **Decentralized Command Structure**: A modern battlefield is characterized by rapid changes and faces constant threat of disruption to centralized command and control. To mitigate this risk, Taiwan is restructuring its military operations around a decentralized command philosophy. By dispersing key command nodes and embedding decision-making at lower echelons, Taiwan aims to ensure that its military can continue to operate effectively even if parts of its command infrastructure are targeted (Yeo, 2021).

The porcupine strategy is emblematic of Taiwan's broader shift towards an agile, resilient, and cost-effective defence posture. Rather than relying on a few high-cost platforms, the island is investing in a network of systems and tactics that, together, pose significant challenges to any adversary seeking to impose its will by force.

Strengthening Coastal and Air Defences

Given the PLA's focus on amphibious assault and air superiority, Taiwan has prioritized the reinforcement of its coastal and air defences. These initiatives are designed to complicate PLA operations across multiple domains and ensure that Taiwan's defensive perimeter remains robust even in the face of an intense first strike.

Coastal Defences and Anti-Landing Measures

The PLA's amphibious assault readiness is a well-recognized threat, and Taiwan's response has been to invest in measures that can deter or delay landing operations:

- **Smart Mines and Naval Minefields**: Taiwan is deploying smart mines along likely amphibious landing zones. These mines are integrated with advanced sensor networks that can be deployed in

shallow water, to boost its defences against a potential invasion by China. The new type can be deployed closer to the coastline and be more effective in warding off enemy landings (Taipei Times, 2012).

- **Coastal Missile Systems**: In addition to minefields, Taiwan is installing coastal defence missile systems designed to target and neutralize approaching PLA amphibious vessels. These systems are intended to create a layered defensive barrier that complicates enemy planning and increases the operational risks associated with a landing operation (Casimiro, 2024).

Air Defence Upgrades

Control of the air domain is a central element of PLA strategy, which has prompted Taiwan to enhance its own air defence capabilities:

- **SAM Upgrades**: Taiwan's acquisition of advanced surface-to-air missile (SAM) systems, including the US-origin Patriot PAC-3 as well as indigenous Sky Bow III systems, is intended to counteract the PLA's efforts to secure air superiority (Cuhng, 2025). These systems are integrated into a multi-layered air defence network designed to intercept incoming missiles and aircraft, thereby protecting critical assets and command centers.
- **Hardened and Dispersed Airfields**: Recognizing that modern warfare places a premium on the survivability of its air force, Taiwan has invested in the hardening of its airfields. This includes development of underground hangars and the dispersal of aircraft across multiple, strategically located sites (SHUGART, 2025). These measures are designed to minimize the impact of a first-wave missile barrage and ensure that Taiwan retains operational air power even under sustained attack.

The emphasis on both coastal and air defences represents a comprehensive effort by Taiwan to deny the PLA easy victories that

would result from overwhelming either domain. By hardening critical infrastructure and creating overlapping fields of fire, Taiwan seeks to force the PLA into a costly, drawn-out campaign where every advancement is met with stiff resistance.

Cyber and Information Warfare

In the modern battlespace, physical defence is inseparable from the protection of information and digital networks. Taiwan's experience with PLA grey zone tactics has underscored the need for robust cyber and information warfare capabilities. Disinformation has become a key instrument in modern hybrid warfare. The PLA is known to employ coordinated efforts to undermine public trust and destabilize democratic institutions through the spread of misleading or false information. Taiwan's strategy includes deployment of artificial intelligence (AI)-based tracking systems that monitor and identify Chinese influence operations (Nanda, 2024). By rapidly debunking and countering disinformation narratives, Taiwan seeks not only to protect its domestic political environment but also to maintain the international community's confidence in its governance and resilience. The dual focus on cyber and information warfare reflects a broader understanding that future conflicts will be fought as much in the digital realm as on traditional battlefields. Taiwan's investments in these areas are aimed at ensuring that its decision-making processes, as well as those of its allies, are not compromised by stealthy, non-kinetic operations designed to sow discord and confusion.

Enhancing Deterrence through International Partnerships

While Taiwan's internal military reforms are essential, only one element of a broader deterrence strategy relies on international partnerships. Given its strategic vulnerability, Taiwan has actively sought to fortify ties with key allies who share similar concerns over China's regional ambitions.

US Military Support

The United States has long been recognized as Taiwan's most important security partner. US military support manifests in several key takeaways:

- **Arms Sales**: Arms sales have provided Taiwan with advanced defensive systems, including AMRAAM Extended Range surface to air missiles. These acquisitions not only bolster Taiwan's self-defence capabilities but also serve as a tangible sign of US commitment to the island's security.
- **Naval Presence in the Indo-Pacific**: US Navy Freedom of Navigation Operations (FONOPs) in the Taiwan Strait have been a critical signal of US resolve. These operations underscore the broader strategic message that the international community will not acquiesce to unilateral changes in the status quo imposed by force.
- **Training and Advisory Programs:** In addition to hardware, US military training and advisory programs have been instrumental in modernizing Taiwan's armed forces. By adopting interoperability tactics and modern command and control procedures, Taiwan is better positioned to coordinate its defence efforts with US forces in a joint or multinational setting (Yeager, 2022).

Expanding Defence Ties Beyond the United States

Taiwan has also been active in forging closer ties with other regional and European democracies:

- **Japan's Strategic Shift**: Japan has indicated a growing willingness to support Taiwan, aligning its own strategic interests with those of the island in maintaining stability of the Taiwan Strait (NG, 2024). Japan's increased military posturing and potential for joint exercises with Taiwan underscore a regional recognition of the need for a coordinated response to Chinese coercion.
- **QUAD and Regional Security Initiatives**: Although Taiwan is not a formal member of the Quadrilateral Security Dialogue (QUAD),

the strategic focus of this grouping, comprising the United States, Japan, India, and Australia, on countering China's assertiveness in the Indo-Pacific indirectly benefits Taiwan. The shared values and strategic interests among these nations help create a broader security environment that constrains PLA aggression.

- **European Engagement**: European countries such as Lithuania, the United Kingdom, and Germany have increasingly demonstrated diplomatic and defense interest in Taiwan. This growing engagement is indicative of a broader international trend in which democracies are seeking to balance China's expanding global influence through enhanced political and military cooperation.

The international dimension of Taiwan's defence strategy is not merely about securing military hardware or training support; it is also a critical component of deterrence. By deepening alliances and forging new partnerships, Taiwan ensures that any potential PLA aggression would occur within an environment of collective international scrutiny and rapid allied response. Such a deterrence network serves to increase the political and economic costs for China should it choose to use force.

Challenges and Future Military Strategy

Despite significant progress in adapting to an asymmetric threat environment, Taiwan's military strategy faces several inherent challenges that must be addressed to sustain long-term deterrence and resilience.

Manpower and Recruitment Challenges

Taiwan's transition from a conscription-based system to a professional military force has introduced recruitment challenges. With a smaller pool of eligible recruits, the island faces a potential shortage of manpower. In response, Taiwan has reintroduced a one-year mandatory military service to broaden its reserve base and ensure that it retains

sufficient personnel to man its decentralized defence structures (The Hindu, 2022).

Budgetary Constraints

Although, Taiwan has increased its defence spending to over 2 per cent of its GDP, this level of investment remains modest compared to China's vast military expenditure. Budget constraints necessitate careful prioritization of resources, compelling Taiwan to invest in cost-effective, asymmetric capabilities rather than expensive, high-end systems that could be outmatched by the PLA's numerical superiority. The focus on indigenous systems and low-cost countermeasures is a pragmatic response to these fiscal limitations

Geographic Vulnerability and Strategic Depth

Taiwan's limited geographic size poses a significant challenge. The island's compact territory means that a first strike by the PLA could potentially degrade critical infrastructure before adequate mobilization or international assistance is possible. To mitigate this vulnerability, Taiwan is investing in hardened shelters, dispersal of military assets, and rapid-reaction forces that can be quickly deployed to counter an incursion (Kramer, 2024). The challenge lies in creating sufficient strategic depth within a geographically constrained environment.

Integration of Multi-Domain Capabilities

Modern warfare demands seamless integration across multiple domains viz. land, sea, air, cyber, and space. Taiwan's defence planners are tasked with significant challenges of ensuring that these diverse capabilities operate in concert. The development of a robust, decentralized command and control network is critical, but it requires overcoming both technical and organizational hurdles to achieve interoperability among different branches of the military.

Evolving PLA Capabilities and the Need for Continuous Adaptation

Perhaps the most dynamic challenge facing Taiwan is the continuously evolving nature of the PLA's capabilities. As China invests heavily in advanced technologies, including hypersonic missiles, artificial intelligence, and electronic warfare systems, Taiwan must be prepared to adapt its doctrine and procure new capabilities at a rapid pace. This requires not only sustained investment in research and development but also an adaptive organizational culture that can quickly respond to emerging threats.

The future of Taiwan's military strategy will likely involve an ongoing process of recalibration. As the PLA refines its operational doctrines and expands its multi-domain capabilities, Taiwan's asymmetric approach must also evolve. This will involve deeper integration with international partners, a greater focus on hybrid warfare including both kinetic and non-kinetic domains and continuous improvement of its indigenous defence technologies

Conclusion

Taiwan's military strategy, in the face of an asymmetric threat from the PLA, is a multifaceted and evolving doctrine. Confronted by an adversary with overwhelming conventional capabilities and a penchant for grey zone tactics, Taiwan has shifted its focus from direct, symmetric confrontation to an agile, decentralized, and cost-escalation approach. The "porcupine strategy" built on missile and drone warfare, swarming tactics, mobile defence units, and a resilient, decentralized command structure illustrates Taiwan's commitment to making any PLA incursion extremely costly.

At the same time, reinforcement of coastal and air defences, coupled with investments in cyber and information warfare capabilities, demonstrates Taiwan's recognition that modern conflict is as much about protecting digital infrastructure and public trust as it is about traditional

military engagements. Moreover, Taiwan's efforts to enhance deterrence through robust international partnerships most notably with the United States, as well as emerging ties with Japan, QUAD nations, and European democracies serve as critical multipliers of its own defence efforts.

However, the challenges remain significant. Manpower shortages, budget constraints, geographic vulnerabilities, and continuous evolution of PLA capabilities, all underscore the need for a dynamic and adaptable defence strategy. As Taiwan continues to refine its military posture, it must balance immediate defensive needs with long-term investments in technology, training, and international cooperation. Only by maintaining this balance can Taiwan hope to preserve its sovereignty and ensure that any attempt at coercion or military aggression by China will be met with a resolute and effective response.

In sum, Taiwan's strategic recalibration towards asymmetric warfare is a pragmatic and necessary response to the multifaceted threats posed by a modernized PLA. By leveraging its unique strengths, investing in innovative defence measures, and cultivating a robust network of international partnerships, Taiwan seeks not only to deter aggression but also to sustain its democratic way of life in an increasingly contested Indo-Pacific region. The continued evolution of this strategy will undoubtedly serve as a critical case study in modern asymmetric deterrence, with lessons that extend far beyond Taiwan's shores.

References

Ap. (2022, December 27). *Taiwan extends compulsory military service to one year*. The Hindu. https://www.thehindu.com/news/international/taiwan-extends-compulsory-military-service-to-one-year/article66310218.ece

Army University Press. (2023, September). *Xi Jinping's PLA reforms and redefining* "*Active defense*." Retrieved February 17, 2025, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2023/Active-Defense/

Bommakanti, K. (2024, October 1). *China's military modernisation: recent trends - 2024*. orfonline.org. https://www.orfonline.org/research/contemporary-trends-in-china-s-military-modernisation

Casimiro, C. (2024, October 2). *Taiwan Receives First Batch of Harpoon Anti-Ship Missile Systems From the US*. The Defense Post. Retrieved February 17, 2025, from https://thedefensepost.com/2024/10/02/taiwan-receives-harpoon-missile/

Chung, L., & Chung, L. (2025, February 11). Taiwan signs US$761 million deal for US NASAMS defence package. *South China Morning Post*. https://www.scmp.com/news/china/politics/article/3298261/taiwan-signs-us761-million-deal-us-nasams-defence-package

Congressional Research Service. (2024). *China Naval modernization: Implications for U.S. navy capabilities* (No. RL33153). https://sgp.fas.org/crs/row/RL33153.pdf

Dangwal, A. (2023, August 19). Suicide UAVs in action: Taiwan's chien Hsiang kamikaze drones make a rare appearance in new video. *EURASIAN TIMES*. https://www.eurasiantimes.com/ukraine-conflict-spurs-taiwans-interest-in-kamikaze-drones/

Gomez, E. (2023). *Taiwan's urgent need for asymmetric defense*. CATO. Retrieved February 17, 2025. https://www.cato.org/policy-analysis/taiwans-urgent-need-asymmetric-defense

Lewis, J. A. (2024). *Cyberattack on civilian critical infrastructures in a Taiwan scenario*. https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario

Mason, S. (2022, January 7). *Reestablish the U.S. Military Assistance Advisory Group-Taiwan—War on the rocks*. War on the Rocks. https://warontherocks.com/2022/01/reestablish-the-u-s-military-assistance-advisory-group-taiwan/

Nanda, P. (2024, January 14). Taiwan Uses Artificial Intelligence to Puncture China's Info War; Beijing's Plan of 'Threat Unification' Thwarted. *EURASIAN TIMES*. https://www.eurasiantimes.com/taiwan-uses-artificial-intelligence-to-puncture-chinas/

Ng, K. (2024, September 26). *Japan joins patrols through Taiwan Strait - reports*. https://www.bbc.com/news/articles/cm28yd04xxno

Protecting the porcupine: Why Taiwan matters. (2023, April 14). Epicenter. https://epicenter.wcfia.harvard.edu/blog/protecting-porcupine-why-taiwan-matters

Ratiu, A. (2024, July 1). *Strengthening Taiwan's resiliency - Atlantic Council*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/strengthening-taiwans-resiliency/

Revels, M. (2023, April 24). *Denying command of the Air: the future of Taiwan's air defense strateg*. Air University (AU). Retrieved February 17, 2025, from https://www.airuniversity.af.edu/JIPA/Display/Article/3371516/denying-command-of-the-air-the-future-of-taiwans-air-defense-strategy/

Saxena, A. (2024, June 15). *China's 'grey-zone' warfare tactics against Taiwan | Explained*. The Hindu. https://www.thehindu.com/news/international/chinas-grey-zone-warfare-tactics-against-taiwan-explained/article68286636.ece

Shugart, T. H., III, Walton, T. A., & Hudson Institute. (2025). *Concrete Sky: Air base hardening in the Western Pacific*. Hudson Institute. https://s3.us-east-1.amazonaws.com/media.hudson.org/Concrete+Sky+-+Air+Base+Hardening+in+the+Western+Pacific+-+Shugart+-+Walton.pdf

Slad. (2023, December 12). *A maritime blockade of Taiwan by the People's Republic of China: A strategy to defeat fear and coercion - Atlantic Council*. Atlantic Council. https://

www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/a-maritime-blockade-of-taiwan-by-the-peoples-republic-of-china-a-strategy-to-defeat-fear-and-coercion/

Su Wu, S. (2006). Taiwan's Asymmetrical Defense: Policies and alternatives Taiwan's Asymmetrical Defense: Policies and Alternatives. *Journal of Strategic Security*, 16(4). https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2101&context=jss

Taipei Times. (2012, November 30). *Military to produce 'smart' mines for invasion defenses.* https://www.taipeitimes.com/News/taiwan/archives/2012/11/30/2003548984. Retrieved February 17, 2025, from https://www.taipeitimes.com/News/taiwan/archives/2012/11/30/2003548984

The Autonomous Arsenal in Defense of Taiwan: Technology, Law, and Policy of the Replicator Initiative. (2025, February 3). The Belfer Center for Science and International Affairs. https://www.belfercenter.org/replicator-autonomous-weapons-taiwan

Yeo, M. (2022, August 19). Taiwan unveils Army restructure aimed at decentralizing military. *Defense News.* https://www.defensenews.com/global/asia-pacific/2021/05/17/taiwan-unveils-army-restructure-aimed-at-decentralizing-military/

"Project Tiger": Revitalising the Roar

G Sunil Kumar

The role of a Commanding Officer (CO) in the Indian Army is critical to maintaining discipline, operational effectiveness, and the welfare of troops. However, the status and authority of a CO have faced challenges in recent years due to bureaucratic constraints, legal scrutiny, and evolving leadership dynamics. Strengthening the position of a CO is essential for ensuring swift decision-making, enhancing morale, and upholding the traditions of the armed forces. This article explores key measures to improve the status of a CO, including policy reforms, enhanced training, and a balanced approach to accountability, ultimately reinforcing the leadership structure crucial for national defence.

The "Tiger"

CO : An institution

The CO is a pivotal institution in the Indian Army, representing the highest level of leadership at the unit level. This institution embodies the ethos of the Indian Army, where authority is balanced with responsibility, and leadership is built on trust, respect, and decision-making under pressure. The CO is not just an individual but an institution that upholds traditions, values, and combat effectiveness of the Army. Over time, the

Colonel **G Sunil Kumar** is Senior Fellow at the Centre for Land Warfare Studies (CLAWS), New Delhi. Views expressed are personal.

role has evolved, requiring continuous adaptation to modern warfare, legal frameworks, and organizational changes while maintaining its fundamental role as the backbone of military leadership. Strengthening this institution is essential to ensuring the Indian Army's operational excellence and cohesion. The "Paltans" are the "Cutting Edge" of the Indian Army and the CO is the "Cutting Edge" of the "Paltan".

Naam Nishan Namak

The ethos of *Naam, Nishan, Namak*—honour, identity, and loyalty—forms the foundation of the Indian Army's values, guiding every soldier's commitment to duty. *Naam* (honour) represents the legacy and reputation of a unit, *Nishan* (identity) symbolizes the pride associated with regimental traditions and insignia, and *Namak* (loyalty) signifies unwavering allegiance to the nation and service. The Commanding Officer plays a crucial role in upholding these values by leading with integrity, fostering regimental pride, and ensuring discipline within the ranks. Through personal example, fair leadership, and unwavering commitment to duty, the CO instils these principles in soldiers, thus strengthening their dedication to the Army's mission. By preserving these core ideals, the CO not only maintains operational effectiveness but also reinforces the Indian Army's rich heritage and unity. In many instances, the CO himself becomes the *Nishan* of the unit, exemplifying its spirit, valour, and sacrifice. This is evident in the tales of COs who led from the front, embodying the unit's ethos, and made the ultimate sacrifice for their men and their regiment (discussed subsequently).

The Tiger

In the Indian Army, the Commanding Officer (CO) is often referred to as the "Tiger" as a mark of respect and authority. This nickname symbolizes strength, fearlessness, and leadership, much like a tiger in the wild. The CO is expected to lead from the front, make tough decisions, and protect

his troops, embodying the courage and dominance associated with the tiger. Over time, this title has become a tradition within regiments, reinforcing the CO's absolute authority and inspiring soldiers to follow his command. It serves as a reminder of the warrior spirit, boosting morale and emphasizing the crucial role of the CO as both a leader and protector of his unit.

Throughout history, Commanding Officers (COs) have exemplified leadership by leading from the front, inspiring their troops with courage and determination. In the Kargil War (1999), Colonel Lalit Rai, CO of 1/11 Gorkha Rifles, led his men in capturing Khalubar Ridge despite being wounded, refusing evacuation until victory was secured. Similarly, in the 1962 Sino-Indian War, Lieutenant Colonel Shaitan Singh, the CO of 13 Kumaon, fought bravely at Rezang La, leading his men until his last breath, earning a Param Vir Chakra posthumously. Another remarkable example is Colonel Hoshiar Singh, CO of 3 Grenadiers during the 1971 Indo-Pak War, who personally led assaults on enemy positions in the Battle of Jarpal, securing a decisive victory and earning the Param Vir Chakra. More recently, Colonel Santosh Yashwant Mahadik, SC, SM, CO of 41 Rashtriya Rifles, displayed exceptional bravery in counter-terror operations in Jammu & Kashmir in 2015, making the supreme sacrifice while leading from the front. Similarly, Colonel B. Santosh Babu, CO of 16 Bihar Regiment, fearlessly led his men during the 2020 Galwan Valley clash against Chinese forces, sacrificing his life in defence of the nation and posthumously receiving the Maha Vir Chakra. These instances reflect the ethos of the Indian Army, where COs do not merely command from behind but stand alongside their soldiers in battle, thus demonstrating unparalleled courage and selflessness.

A Diminished Roar

In recent times, there is a growing perception that the stature of Commanding Officers in the Indian Army have diminished compared

to earlier eras due to increased bureaucratic oversight, legal constraints, and higher-command intervention. Earlier, COs had greater autonomy in decision-making regarding operations, discipline, and logistics, but today, approvals from higher headquarters often delay swift action. Legal scrutiny and human rights concerns, particularly in conflict areas like Jammu & Kashmir and the Northeast, have further restricted COs, making them more cautious in executing operations due to potential legal repercussions, as seen in cases like the Shopian firing incident (2018). Additionally, higher headquarters now closely monitor and sometimes micromanage unit operations, reducing the CO's role from an independent leader to more of an executor. The widened gap, in age and experience, between COs and Commanders/Staff at higher HQ tend to aggravate the situation further.

Furthermore, advancements in technology, including real-time surveillance and digital communication, have enabled senior commanders to directly oversee tactical decisions, limiting a CO's battlefield autonomy. In earlier wars like 1965 and 1971, COs had the authority to make real-time decisions, whereas today, strict operational doctrines often require them to wait for clearance before initiating aggressive actions. While these changes have made the Army more structured and accountable, they have also reduced the flexibility and swift decision-making once enjoyed by COs, altering the nature of battlefield leadership. We would now look at some of the reasons for this diminished roar.

Limited Unit Tenures

The lowering of the promotion age for the rank of Colonel and increasing commitments to staff and instructional appointments have resulted in officers spending less time with their units, impacting leadership continuity and unit cohesion. Earlier (Pre-Kargil period), officers would serve longer tenures within their battalions before taking command as a Commanding Officer (CO), allowing them to develop deep bonds with their troops

and gain extensive regimental experience. However, with promotions to Colonel rank now occurring at a younger age—often in the mid to late 30's age, officers are quickly moved to staff roles, instructional assignments, or higher headquarters, limiting their time in command roles at the unit level. Additionally, career progression now demands officers to attend various staff courses, foreign assignments, and deputations to remain competitive for further promotions, further reducing the duration spent on leading troops in operational units.

This frequent movement affects the continuity of leadership, as officers often take command of a unit for a shorter duration before being reassigned, leading to a scenario where soldiers and junior officers experience multiple COs in a short span. While this system ensures broader exposure and career growth for officers, it also challenges the traditional regimental bonding and field experience that were once considered the backbone of effective military leadership. There is no substitute for hands-on experience gained through meaningful tenures within the unit at various levels to foster true regimental spirit and develop effective leadership skills. Neither books, staff appointments, nor courses can replicate the depth of understanding, camaraderie, and battlefield decision-making that come from serving alongside troops in real-world conditions. Limited tenures weaken bonding with troops, increasing friction and doubt for both the CO and soldiers, especially during tough decision-making.

Perils of Younger Age

Early promotion to the rank of Colonel in the Indian Army has led to concerns about reduced maturity and experience among COs compared to earlier times. Previously, officers took command of a battalion in their early to mid-40's, after years of extensive regimental service, frontline experience, and leadership roles in various capacities. This longer grooming period allowed them to develop deeper tactical

acumen, decision-making skills, and a strong understanding of their men. However, with accelerated promotions, officers now assume command in their mid to late 30's, often with relatively fewer years of hands-on combat experience and leadership exposure. As a result, some COs may lack the same depth of battlefield wisdom and crisis-handling ability that their predecessors had. Additionally, with a shorter command tenure before moving to staff or higher headquarter roles, there is less time for them to refine their leadership through prolonged field service. While younger COs bring dynamism, adaptability, and modern perspectives, the reduced time spent honing regimental and tactical skills before command can sometimes affect decision-making in high-stakes situations, leading to a perceived decline in battlefield maturity compared to earlier generations of military leaders. A "Younger" CO results in early removal of non-empanelled officers from the unit, reducing experience and strength at the battalion level while inflating staff and higher HQ numbers, forcing stringent oversight.

HR Management Policies

The Indian Army's career management policies seem to be favouring staff and instructional roles over command tenures, placing excessive emphasis on course gradings and selection marks. The additional 1.5% weightage for DSSC/DSTSC, along with the resultant boost in value judgment scores during promotion boards, creates a significant disparity between officers with these qualifications and those without. However, these courses primarily assess academic aptitude and suitability for staff roles, rather than command potential and battlefield leadership. The policies further skew the command-to-staff ratio, as 'the QR of good course' gradings lead to more Extra Regimental Employment (ERE) postings, keeping these officers, who are more likely to Command the unit, away from their parent units for extended periods.

Excessive exposure to staff and instructional roles alters the temperament of Commanding Officers, making them risk-averse and career-conscious, rather than deeply invested in their units. Earlier, longer regimental tenures fostered strong unit-first leadership, but today's system encourages a broader, at times, career-oriented mindset, where COs may prioritize "self-preservation/safety first" approach over battlefield initiative. Unlike past leaders who took bold risks alongside their troops, modern COs may hesitate due to concerns over legal, administrative, and career repercussions. While structured leadership and adherence to protocols have their place—this shift may have led to an erosion of the selfless, unit-first ethos that once defined regimental leadership. However, this change is not a failure of the individual officer but rather a consequence of organizational HR policies, where prolonged exposure to non-Regimental roles naturally shapes a more cautious leadership approach.

Lack of support from Senior Officers and Higher HQs

Commanding Officers seem to be receiving diminishing support from senior officers/higher HQs, largely due to self-preservation instincts and the widening service gap between Colonels and Brigadiers. With early promotions to Colonel, officers assume command younger, but the long wait for Brigadier (nearly a decade) creates a stark difference in experience, maturity, and leadership outlook. This gap often leads either in timid acquiescence/immature friction between COs and higher commanders, who, having spent longer time in staff and headquarter roles, may also become increasingly disconnected from unit-level realities.

As a result, COs facing operational, legal, or administrative challenges may often find themselves isolated, with senior officers/ Higher HQs prioritizing a "Safe/Hands Off" approach, over protecting subordinates. Unlike the past, when organisational considerations

ensured COs were shielded from excessive scrutiny, today's system places full accountability on them, exposing them to legal, media, and bureaucratic pressures. The problem is further worsened by a top-heavy structure, especially at the staff level in higher HQs, where additional senior/staff level posts are created to accommodate officers who are already non-empanelled or awaiting promotion, adding unnecessary oversight and pressure on battalions. The growing burden of Standard Operating Procedures (SOPs) and rigid compliance protocols further restricts COs, forcing them into a risk-averse leadership style that undermines battlefield initiative and decisive action.

Change in Troops Profile

The increased social media exposure and the changing profile of troops—from predominantly rural, less literate backgrounds to a more modern, educated force—are posing new challenges for Commanding Officers in the Indian Army. Earlier, troops relied primarily on direct interaction with their leaders, fostering a close-knit regimental culture built on trust and experience. However, widespread access to social media has led to faster dissemination of information, unchecked rumours, and external influences, sometimes undermining the traditional chain of command. Additionally, today's additionally aware and digitally connected soldiers are more likely to question orders, compare conditions across units, and even escalate grievances beyond the battalion level, reducing the CO's ability to resolve issues internally. The shift from a hierarchical obedience model to a more individualistic mindset also makes discipline enforcement and morale management more complex. While a more literate and informed soldier brings advantages in tactical adaptability and skill development, the challenge for COs lies in balancing authority, addressing evolving expectations, and maintaining unit cohesion in an era where external narratives increasingly shape perceptions within the ranks.

Media Glare and Public Perception

Increased media scrutiny and a shifting public perception of the Indian Army—from a revered "holy cow" to just another government arm—have created significant challenges for COs, especially in active-duty areas. Every operation, decision, or casualty is now subject to intense media coverage, political discourse, and legal scrutiny, often without understanding the on-ground realities. This heightened attention forces COs to operate under constant pressure, where even justified actions in combat or counter-insurgency roles can be misinterpreted, sensationalized, or legally challenged. The fear of negative media portrayal, human rights allegations, or administrative repercussions discourages bold decision-making, making operations more defensive than proactive. Additionally, social media amplification can spread misinformation, erode troop morale, and expose operational strategies, further complicating command challenges. This evolving landscape demands a delicate balance between operational effectiveness, legal prudence, and public perception management, making a CO's role more complex than ever before.

Revitalising the Roar

We need to seriously look at means to restore the centrality of COs in unit leadership, strengthen their decision-making authority, and ensure they remain deeply connected to their troops, ultimately enhancing combat effectiveness and regimental ethos. Based on the challenges discussed, the following suggestions outline measures to strengthen the authority, effectiveness, and leadership impact of COs in the Indian Army:

(a) **Restoring Command Primacy Over Staff Appointments**

- Reduce/eliminate the undue weightage given to DSSC/DSTSC gradings in promotion boards. Meritorious officers may not need extra marks as a crutch to attain the rank of Colonel—stellar regimental service and individual merit on its own should suffice.

- Ensure command/unit tenures are prioritized over staff/ instructional roles (although important) for career progression.
- Maintain a balanced command-to-staff ratio in service profiles of officers to prevent excessive detachment from field leadership.

(b) **Strengthening Regimental Continuity and Hands-On Experience**

- Increase unit tenures at junior levels to build strong regimental bonds and leadership skills. Frequent Extra Regimental Employment (ERE) postings often detach officers from their battalions for extended periods, thus weakening their regimental ties and command experience. To address this, the qualification requirements for staff tenures should be made less stringent, particularly in terms of course gradings, ensuring a more equitable distribution of staff and command exposure. Officers with lower course gradings should still have opportunities to gain staff experience, while those with higher gradings should not be overburdened with repeated staff roles at the expense of unit tenures. This balance would allow for greater regimental continuity, stronger leadership development, and a more well-rounded officer cadre.
- Ensure longer command tenures to allow COs to deeply engage with their troops (at least 3 years).

(c) **Bridging the Experience Gap Between COs and Senior Commanders**

- Reduce the promotion gap between Colonel and Brigadier to ensure better alignment in experience and leadership perspective. Officers should assume command only after at least 18 years of service (early to mid-40s) and must have at least four to five meaningful unit tenures of at least two years each to develop strong regimental ties and battlefield leadership skills before taking charge as COs.

- Implement mentorship programs, where senior officers actively guide COs in operational and administrative challenges. More as "mentors" and "Partners" than "Assessors" and "Superiors".

(d) **Enhancing Senior Leadership Support for COs**

- Develop a more supportive command environment, where higher commanders are more inclined to support unit-level decisions.
- Reduce excessive legal and bureaucratic scrutiny on COs, allowing greater operational flexibility. It's easier for Higher HQs to build effective ties with civil administration and police authorities and these should be leveraged to lend support to the COs and the units as and when needed.
- Encourage a culture of backing bold battlefield leadership, rather than risk-averse decision-making.
- Encourage direct interaction with COs rather than over-relying on staff inputs, which may be biased or lack ground realities. This will enhance confidence, reduce pressure, and enable faster, more informed decision-making.

(e) **Reducing Bureaucratic and Compliance Burden**

- Simplify Standard Operating Procedures (SOPs) to help COs focus on training and combat readiness. SOPs should enhance efficiency and uniformity, not just fix blame or create scapegoats. They must streamline processes, prioritize practicality over complexity, and use clear, simple language instead of unnecessary academic jargon.
- Avoid creating SOPs for mundane tasks, as this increases rigidity and stifles innovation.
- Reduce administrative paperwork to free up time for leadership and unit engagement. Embracing digitization and shifting mindsets to accept digital records as valid correspondence will be a key step in this direction.

- Prevent excessive oversight from additional HQ structures that burden COs. Raising the promotion age for Colonels and relaxing staff posting criteria would ensure more officers at the unit level, thus reducing the current imbalance where overzealous/additionally qualified staff officers micromanage limited and relatively much younger unit officers.
- Avoid overloading units with excessive, rigid KRAs/Directions and frequent feedback mandates, as each unit is unique, and COs must have the flexibility to prioritize combat readiness. Instead, higher HQs should provide broad guidelines, allowing COs greater autonomy to formulate KRAs that balance regimental needs with organizational goals.

(f) **Adapting Leadership to Changing Troop Profiles and Social Media Influence**

- Train COs in modern leadership approaches to effectively manage more educated, socially aware troops.
- Establish clear guidelines for social media use within the unit to prevent misinformation and breaches of discipline.
- Encourage interactive leadership styles that balance authority with engagement to maintain morale and cohesion.

(g) **Promoting Bold and Decisive Leadership**

- Shift the promotion and evaluation criteria to reward field leadership, risk-taking, and operational effectiveness.
- Provide legal and institutional protection for COs making tough battlefield decisions in good faith especially while writing the ACR.
- Encourage a command culture that values initiative, rather than excessive adherence to protocol.

(h) Effective Media Engagement and enhancing Positive Public Perception.

- To counter increased media scrutiny and shifting public perception, COs need stronger legal and institutional backing, ensuring protection from undue litigation and scrutiny.
- A proactive media strategy with trained spokespersons and real-time counter-misinformation efforts can prevent false narratives from gaining traction.
- Better coordination with civil authorities will reduce unnecessary interference, while greater operational autonomy will allow COs to make bold decisions without fear of backlash.
- Media Engagement and Perception management need to be covered in greater depth and extent in army courses especially at the higher levels.
- A change in perception from "Fear of media" to an 'Enabler/ Facilitator' is necessary and its important to train our officers to do this effectively.
- Strengthening internal communication and troop morale through direct engagement and regimental traditions will further reinforce confidence and cohesion, enabling COs to lead effectively despite external pressures.

Conclusion

The Commanding Officer remains the cornerstone of unit leadership in the Indian Army, embodying the ethos of *Naam, Namak, and Nishan*. However, evolving operational challenges, bureaucratic constraints, and shifting leadership dynamics have steadily eroded the CO's autonomy and authority, affecting their ability to lead with conviction.

To restore the "Tiger's Roar," systemic reforms are imperative—ensuring longer and more stable command tenures, reducing bureaucratic interference, strengthening senior leadership support, and adapting to modern realities like evolved troop profile and social media scrutiny.

By reaffirming the primacy of battlefield leadership and reinforcing regimental traditions, the Indian Army can empower its COs to lead with courage, decisiveness, and unwavering commitment.

A strong and independent CO is not just essential for unit effectiveness but for the overall strength, cohesion, and operational excellence of the Indian Army. If we do not act now, we risk transforming the once-majestic Leader and Protector of the battlefield into an 'emaciated pet behind bars in a zoo'—an echo of its former glory rather than 'the fearless guardian of its domain'. It is time to revitalize the Tiger's Roar, as for the strength of the forest (the Indian Army) depends on it.

Use of Battlefield Equalisers to Include Innovations, Technology to Counter the Conventional Superiority in Russia-Ukraine Conflict

V S Salaria

Abstract

The Russia-Ukraine War is a classical case study for employment of Battlefield Equalisers leveraging technologies to bridge the asymmetry between unequal protagonists. The conflict has become catalyst and incubator for technological revolution exploiting the diffusion of dual use technologies through close collaboration between civilian developers and military end users bypassing the mainstream approaches towards capability building. Insights from this regional war have critical lessons and actionable takeaways for India especially for harnessing innovations, emerging, disruptive technologies and most importantly its adaptation on the battlefield as Battlefield Equalisers.

Brigadier **Virender Singh Salaria**, SC, SM is a Special Forces officer. An alumnus of NDA, the Officer has attended prestigious Command and General Staff Course (CGSC) from USA where he was adjudged 'Master Strategist.' The Officer has served in varied terrains, operational environments, Military Operations Directorate and as Defence Attache in Italy. Presently, the Officer is commanding Siachen Brigade. Views expressed are personal.

Modern warfare has continuously evolved with technological advancements shaping its conduct. Critical technologies like autonomous weapons, artificial intelligence and cyber etc., are giving birth to new war fighting tools along with traditional methods witnessing a resurgence. These changes have brought greater lethality, destruction and blurred the lines of conflict with direct warfare amalgamated with hybrid warfare and grey zone tactics. The battlefield has transformed with critical and emerging technologies that have made it a complex and interconnected ecosystem with the convergence of the physical and virtual domains. These technologies have emerged as battlefield equalisers to bridge the asymmetry between protagonists of which Russia-Ukraine conflict is a classic case study.

At the beginning of the Russia-Ukraine war, Ukraine was outmatched on every traditional defence metric. In 2021, Ukraine's defence spending was $4.7 billion compared to Russia's $45.8 billion. Russia outnumbered Ukraine in personnel, aircraft, armoured vehicles, maritime vessels and almost every element of conventional warfare. To offset Russian asymmetry in conventional warfare, Ukraine's smaller force with support from West had to become agile leveraging novel uses of technologies to even the playing field. Ukraine's use of modified commercial aerial and naval drones, new satellite and artificial intelligence capabilities and social media has given Ukraine an edge which has implications for current and future conflicts. The Russia-Ukraine conflict has emerged as a laboratory for latest military technologies making Ukraine the world's tech R&D lab. Russia-Ukraine theatre is surfing the wave of a military technological revolution exploiting the diffusion of dual use technologies through close collaboration between civilian developers and military end users.[1] This paper outlines innovative technological applications used by Ukraine and explores key lessons for India.

Commercial Aerial Drones

To defend along an 800-mile front, Ukraine needed quickly deployable reconnaissance capability and adaptable weaponry. Low-cost commercial drones nearly immediately filled that gap and have played a crucial role in limiting Russia's advances. While aerial drones have been used in military operations since the Vietnam war, Ukraine has made large-scale unprecedented use of commercial drones, quickly modified for use on the battlefield. Additionally, apart from more conventional applications like reconnaissance, Ukraine has employed these drones to guide artillery fire and to execute attacks by dropping munitions or flying them into enemy targets.[2]

As per open-source intelligence, Ukraine loses thousands of drones per month to Russian electronic jamming and maintenance issues. However, even with the short life span, the low-cost of these drones allows Ukraine to quickly replenish stocks and maintain capability. The most common drone has been the Chinese produced DJI-Mavic, available for just $2,000. Ukraine has been increasing procurement and domestic production by two parallel efforts namely the Army of Drones initiative and removing trade barriers to drone imports. The Army of Drones initiative seeks to bolster Ukrainian forces with drone capability through donations from the private sector and individuals. Donors can choose to donate money to specific drone purchases or send in new or used private drones in good working order. In its first three months, the initiative enabled the procurement of 1,400 drones, both commercial and military, and facilitated training for pilots. To support this, Ukraine simplified regulations around the import of drones, and removed VAT and import taxes to expedite getting drones into the country.[3]

In Ukraine's ongoing counteroffensive, drone operations continue to play a pivotal role. Operating close to the front line, working in

tandem with traditional tank units, drones provide reconnaissance and small munitions in the tech enabled 21st century trench warfare. Efforts on the front lines are also complemented by more traditional small unmanned aircraft systems (sUAS), which have been used for deeper penetration.

Naval Autonomous Systems

Russia's traditional naval strength posed a significant threat to Ukraine with Russia achieving early victories on the seas and imposing a naval blockade. Ukraine first countered Russian sea power with traditional naval weapons, bringing down the Russian flagship Moskva in April 2022 with anti-ship cruise missiles. But as Russian assets started operating further from the Ukrainian coastline, Ukraine turned to unconventional naval systems on the surface and subsurface to attack and deter the Russian forces. The underlying technology is far from advanced weaponry, with the simplest models appearing to consist of a water jet from a sea jet ski packed with explosives and communication devices. In October 2022, a fleet of such systems attacked Russian ships in Sevastopol, damaging three vessels.[4]

Ukraine is also making advances in underwater unmanned vehicles (UUV). Brave 1, a Ukrainian public-private defence collaboration recently revealed its new UUV Tolka TLK-150. At only eight feet long, it minimizes the risk of detection and is Ukraine's first self-developed UUV. Public donations are again key to funding these capabilities with Ukraine's fundraising materials offering to name unmanned vessels after significant donors. Maritime autonomous systems are already making an impact during Ukraine's ongoing counteroffensive. Recently, Ukrainian surface drones attacked the Kerch bridge—the critical link between Crimea to mainland Russia. This demonstrated the range of unmanned vehicles (about 440 miles) and that USVs can strike a breadth of targets, including infrastructure and other surface vessels.[5]

Satellite Communication

After Russian hackers successfully disrupted more existing traditional satellite communications in the early days of the conflict, Ukraine immediately pivoted to using Starlink, a SpaceX-owned network of thousands of low-earth-orbit satellites that provides high speed internet with minimal ground infrastructure. As further offensive strikes destroyed or degraded much of Ukraine's traditional internet infrastructure, this cutting-edge commercial technology became critical to the military effort. With Starlink, the Ukrainian military and civilians are able to access the internet through small portable terminals that connect to the satellites. There is essentially no alternative to Starlink in Ukraine, as its portability, cost, and ability to resist jamming make it uniquely resilient to disruption efforts.[6]

The most visible roles for these companies have been in the field of internet connectivity (Starlink/SpaceX) and in cloud computing and cyber (Amazon, Microsoft, Google). Other companies have provided hardware such as drones (DJI), or software to improve legacy systems. Amazon helped Ukraine move data to the cloud in the first days of the war. This included the provision of 'snowball' devices—suitcase-sized computer storage units to help store data, as well as room in the cloud.

However, Starlink also revealed a key vulnerability of reliance on commercial technology with Mr Elon Musk at times threatening to withdraw free access and company executives announcing that they would curb the use of Starlink for offensive purposes. Finally supported by Pentagon funding, Starlink remains a critical part of Ukraine's war effort, enabling command and control as well as the use of aerial and naval drones, social media, and AI for military purposes.

Artificial Intelligence

Speed of analysis will always offer a tactical advantage on the battlefield. Outnumbered by Russia, Ukraine leveraged AI to enhance decision-

making. From quickly sifting through drone footage, to empowering targeting solutions, AI underlies much of the technology Ukraine is leveraging on the battlefield.

Ukraine is using AI-enhanced software Palantir, which synthesizes knowledge of friendly force weaponry and ranges and then makes recommendations for targeting solutions. It uses commercial data, including satellite imagery, to give a near real-time picture of a given battle space. Palantir's software integrates that information with commercial and classified government data, including from allies, which allows military officials to communicate enemy positions to commanders on the ground or decide to strike a target, hence completing the digital Kill Chain.[7]

Additional uses of AI in the battlespace include the US company Primer analysing Russian radio. Traditional surveillance relied on humans to translate intercepted signals and then decode the code words and colloquialisms, which takes substantial time and personnel. AI trained and adapted on unencrypted Russian radio are quickly getting actionable intelligence into the hands of war-fighters. AI has also been used for facial recognition. Beginning in March 2022, Ukraine has been using Face Recognition company viz. Clearview's AI to vet individuals at checkpoints and identify deceased soldiers. Clearview has also provided tools to Ukrainian officials to identify Russians as well as Ukrainian collaborators.[8]

Platforms and Applications

Outmatched to Russia on every count, Ukraine had an urgent need to rapidly develop situational awareness to inform military decisions. First, user friendly designs were employed and made accessible at all levels. For direct military purposes, Ukraine developed Delta - a new platform to provide situational awareness of enemy and friendly forces into a real-time battle command application. This app layers satellite imagery and targeted information on top of more traditional battlefield position

tracking. Social media also feeds directly into Delta to display a more holistic picture of the battlefield. In addition, Ukraine employs Kropyva, a software that runs on simple Android tablets and enables more effective artillery targeting. Delta is only one of the several examples of sophisticated capability development projects initiated or delivered by non-governmental organisations and defence startups. These startup companies crowdsourced funds to develop, manufacture and field the Kropyva targeting software as well as Valkyria reconnaissance and Punisher strike drones. Interfacing directly with military units on the front, they developed techniques, tactics and procedures for reconnaissance and strike drone missions along with sophisticated target acquisition.[9]

Second, applications are engaging civilians directly as reconnaissance agents. Ukraine has leveraged an existing government app—Diia, which was previously employed for civil uses, such as paying taxes and applying for passports. With the updated version, Ukrainian forces are able to collect intelligence from everyday citizens. Diia is installed on 70% of smartphones in Ukraine, allowing the majority of Ukrainian citizens to quickly and easily report enemy movements via encrypted messages and provide real-time intelligence.

Third, Ukraine is able to act on raw social media information at an unprecedented speed. Intelligence and military agencies have long used open-source information to inform assessments but connectivity at all levels of the Ukrainian army is helping translate social media into swift action. For example, Ukrainian forces used the geolocation data from a Russian soldier's selfie posted on vKontakte—a popular Russian social media site for immediate battlefield damage assessments, confirming their strikes on an occupied position. Ukrainian companies like Molfar can find locations of Russian units within three hours of videos posted online. This approach has been leveraging gaps in Russian operational security.[10]

Lessons for India

Effectively leveraging emerging technologies has helped Ukraine hold its own in a war against Russia's traditionally superior military. Yet innovation cannot be static especially in face of a determined and well-resourced opponent. Already, Russia is counter adapting to Ukraine's innovations from jamming Ukrainian drones to experimental electronic warfare aimed at bringing down Starlink to investing in AI-powered weapons. It will be critical for Ukraine to continue to update and innovate. There is an opportunity for India to learn from Ukraine's experience. It is worth analysing following key lessons from Ukraine's innovations to inform India's approach in current and future conflicts.

Public Private Partnerships

Ukraine's agile public private partnerships have increased flexibility and responsiveness to a rapidly changing battlefield. Innovation works from multiple channels. Private industry needs a pathway to inject solutions and operational units need to be able to identify requirements. Ukraine is leveraging both mechanisms through innovation hubs like Brave1 and bottom-up with soldiers procuring off-the-shelf technology. Ukraine's nimble innovation architecture has enabled advancements in all warfare domains.[11]

The private sector has the risk-appetite, agility and market incentives to develop cutting edge innovations in a way that publicly funded institutions cannot match. The procurement process is also leading to lessening diversity in the Indian defence industry with many small and medium-sized companies not able to foot significant entry costs to the market. India should consider allowing more direct and flexible engagement with the private sector, including through streamlining regulatory requirements to leverage the full benefit of innovation for defence outcomes.

To guarantee smooth cooperation with the private sector, India shall consider including commercial systems, equipment and even personnel in military exercises to validate how new off-the-shelf systems can be integrated into the military with minimal bureaucracy and immediate impact.

Implications for Conventional Warfare

Emerging applications of technology are removing some of the asymmetric advantage between more established militaries and smaller forces. The importance of traditional military might, however, cannot be discounted. Russia's successful defensive entrenched positions rely on traditional conventional warfare like mines, tanks, snipers, and layered lines of defence. To attempt to break through Russian lines, Ukraine has merged innovative technology with conventional warfare: small drones conducting reconnaissance for tanks and Starlink connecting units along the front lines. But Ukraine's desperate need for tanks in the counteroffensive shows traditional warfare has a role and sheer numbers still matter. Both Russia and Ukraine are employing a strategy of attrition, slowly and steadily degrading the enemy's personnel and supplies. Technology and traditional warfare are even more linked in the current battle space.

Role of Civilians

Technology has enabled and motivated the involvement of individuals in this conflict to a degree that would likely be replicated in future. Local civilians represent increasingly valuable partners to military forces. Ukraine has showcased the power of a mobilized civilian population armed with technology. The seamless integration of civilian intelligence and targeting shows real potential to shape future conflicts. Leveraging this resource will require both support of local populations and ways to ingest and

action new sources of data. Soft power will continue to be a critical component of any effective military campaign, alongside the technology solutions that can bring civilian forces into the fight. Hobbyist drone unit Aerorozvidka worked closely with Ukrainian military sending tips regarding incoming Russian forces through apps or telegram chatbots. As part of Information Warfare effort, civilians equipped with technology were also employed to prosecute alleged war crimes using its analysis of vast troves of data to link allegations of war crimes to pieces of evidence, including satellite imagery, troop movements, and open-source data like photos and videos uploaded by Ukrainians on social media.[12]

An engaged citizenry is an overall positive development but it can add to polarisation, be instrumentalised by opponents, or lead to pressures that could hamper international diplomacy. India should be proactive and establish mechanisms to coordinate and make use of civilian volunteers who can boost capacities. One promising example is to cultivate individuals' involvement in cyber defence in order to engage individuals who might otherwise conduct cyber vigilantism with little positive impact on military strategic goals. The idea of using civilians as an intelligence resource might also be an option. Here, again, India can learn from Ukraine which has been exceptionally good at positively directing individuals' engagement.

Innovative Model to Harness Technologies

Ukraine's model of grassroots innovation exhibits several key features with valuable lessons. First, the focus is placed on capabilities rather than technologies. Effects attainable through the augmentation of tactics, improved situational awareness or combinations of systems are preferred to material solutions for reasons of cost and time. Second, tasking is focused on clearly defined combat missions, enabling the orchestration of multiple actors and systems to achieve the maximum combat effects. Third, minimally viable systems are deployed into battle even at relatively

low levels of maturity. Fourth, immediate operational feedback is used for continuous improvement. Fifth, informal but evolved network between field commanders and civilians facilitates direct interaction of developers with end users. Sixth, donor funding minimises overheads and eliminates red tape enabling development at minimal expense. Finally, experts in acquisitions, engineering and operations work together in dedicated cross functional teams.

India must develop an accelerator program to harness the emerging technologies. The accelerator would introduce methods for approaching, assessing, validating, sourcing and fielding capabilities to meet urgent operational needs. It shall manage a portfolio of open innovation projects, implemented by task force teams of technology, military and industry specialists working directly with warfighting units. As a clearly defined programme with transparent governance, the accelerator would also set an example in terms of accountable allocation of resources to priorities. By bringing acquisition together with concept development and experimentation, the accelerator would not only tighten the loop between the defence and industry to accelerate iterative improvements but address attributes like performance, security, interoperability, maintainability and other qualities necessary for adoption and transition at early stage of development through stakeholder engagement. India must optimise existing programmes like iDEX and must also consider collaborative accelerator programmes with friendly countries to pool in resources, research and talent.

Conclusion

The Russia-Ukraine War has not yet ended and therefore, this paper provides just a first overview of how emerging technologies have been used in this war so far especially to offset the military superiority, augment and compliment traditional weapon systems. Countermeasures could change the relevance and impact of certain weapon systems and new

uses of technologies might be developed. Even so, this paper shows that there is plenty for India to learn amid the uncertainty. Outsized influence of private companies in war, their coordination and collaboration with government and military will have a major impact on warfighting. This war also teaches that in military, the mass still matters and new technologies and traditional systems need to work in an integrated and complimentary manner. The Government of India also needs to prepare for the enabling nature of new technologies in both formal and informal security assistance and acknowledge that controlling and channelising the engagement of individuals will be an opportunity and challenge in future conflicts. The paper also advocates that mainstream approaches to capability development are slow to harness emerging and disruptive technologies and these approaches must be supplemented by rapid capability development approach that serves the security needs of nation. In Russia-Ukraine War, the most impactful new technologies so far have been drones, space assets, AI enabled software defined systems and these are likely to play an increasing role in the future conflicts.

Notes

1. Dewan, Angela. "Ukraine and Russia's militaries are David and Goliath. https://www.cnn.com/2023/02/25/europe/russia-uktaine-military-comparisonintl/index.html
2. Paul Scharre, Army of None: Autonomous Weapons and Future of Warfare (New York: W.W.Norton & Company, 2018), pp 204-208
3. A Brief History of Drones."Imperial War Museums, https://www.iwm.org.uk/history/a brief -history-of-drones
4. Gunnery,Robert."The Meatgrinder:Russian Tactics in the Second Year of Its Invasion of Ukraine."RUSI, 19 May 2024, https://rusi.org/explore-our research/publications/special resources/meatgrinder-russian-tactics-second year-its invasion-ukraine
5. "Innovative Submarine Drone is Ukraine's New Weapon Against Russian Navy."Naval News, 10 May 2023, https://www.navalnews.com/naval news/2023/05/innovative-submarine-drone-is-ukraine's-new-weaponagainst- russian-navy
6. "Starlink Technolgy."Starlink,https://www.starlink.com/technology
7. Maceas,Bruno."Palantir and Future of Warfare in Ukraine."TIME, 10 Jul 2023, https://time.com/6293398/palantir-future-of-warfare-ukraine

8. "Mapping Software Used by the Ukranian Army."Army SOS, https://armysos.com.ua/defense-mapping-software
9. "Ukraine: Digitalization in Defence."Ukraine.ua,https://Ukraine.ua/investtrade/digitization/
10. O'Carroll, Lisa."Meet Diia: The Ukranian App Used to Do Taxes and Report Russian Soldiers." The Guardian, 26 May 2023, https://www.theguardian.com/world/2023/may/26meet-diia-the-ukranian-aapused-to-do-taxes-and-report- russian-soldiers
11. "Demystifying the Department of Defense." The MITRE Corporation, https://www.aida.mitre.org/demystifying- dod
12. Ukraine's Drone Warfare Capabilities. "Ukraine 24, https://u24.gov.ua/naval drones

Navigating Cyber Risks: Fortifying India's Space Infrastructure Against Emerging Threats

Biswajit Barick

Abstract

This paper discusses the emerging cybersecurity threats to space assets—focusing on the growing vulnerability of space systems due to advancements in technology and the commercialization of the space sector. India's achievements in space exploration, such as the successful Space Docking Experiment (SpaDex), Chandrayaan-3 and future space ambitions, highlight the need for robust cybersecurity measures, to protect critical space assets, which are essential to our nation for smooth functioning in contemporary scenarios. Cyber threats, including malware, social engineering, supply chain attacks, and denial-of-service attacks, pose significant risks to space missions and infrastructure. The paper analyses recent cyberattacks targeting space systems and suggests mitigation strategies, including comprehensive cybersecurity solutions, international cooperation,

Lieutenant Colonel **Biswajit Barick** was commissioned into the Corps of Army Air Defence in 2009. The Officer has served in the Counter Insurgency environment of Jammu and Kashmir as a General Staff Officer Intelligent Grade 2. Views expressed are personal.

cybersecurity training, and rigorous security testing protocols. It concludes with recommendations for India to strengthen its space cybersecurity frameworks, collaborate internationally, and prioritize the development of skilled cybersecurity professionals to safeguard its growing space sector from future threats.

Introduction

On 16 January 2025, India created history with a successful Space Docking Experiment (SpaDex)—entered into the elite group of nations and became the fourth nation to achieve this technological feat. This mission has showcased India's Technological prowess in spacecraft docking, undocking and rendezvous—a critical capability for future space operations.[1] A year ago India's Chandrayaan-3 also placed India among the elite nations to have achieved such fleet. During all these missions, data was being transferred from multiple locations across the globe; coordination and the command and control of satellites worldwide makes space-fairing nations vulnerable and easy targets for non-state actors.

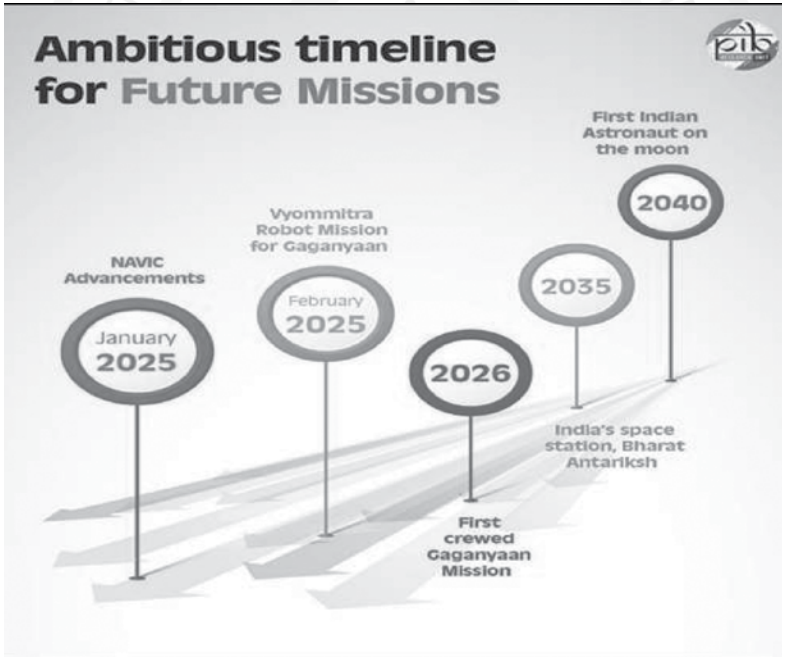
The modern society depends heavily on space infrastructure and hence to keep it safe becomes a pertinent responsibility. They must be protected, and protection of such assets from cyber threats is becoming a challenge.

There are many examples in the past of cyber attacks on satellites viz. Russian attack on Ukraine's Viasat KA-SAT network in 2022 to create communication outages during the commencement of Russian invasion, hacking and jamming of Starlink network[2] and introduction of malware to a host of satellite terminals in 2023 which rendered communications offline.[3] The cyber threat to satellites is a reality.

As per the Department for Promotion of Industry & Internal Trade (DPIIT) Startup India Portal, the number of Space Startups has increased from just one in the year 2014 to 189 in 2023.[4] The investment in Space Startups in India has increased to $ 124.7 Million in 2023. "India's space

economy currently accounts for around two per cent of the global space economy, but it has the potential to reach $44 billion by 2033 with about 8 per cent of the global share"[5] as per Space Economy Trends analysis. Rapid development in the space sector makes India a growing target for Cyber attacks on its space assets. The future missions in space, as released by the Press Information Bureau, are shown in Figure 1.[6] The increasing complexity and commercialization of space systems require further strengthening of security measures to address emerging cyber threats effectively.

Figure 1: Indian Missions in Space



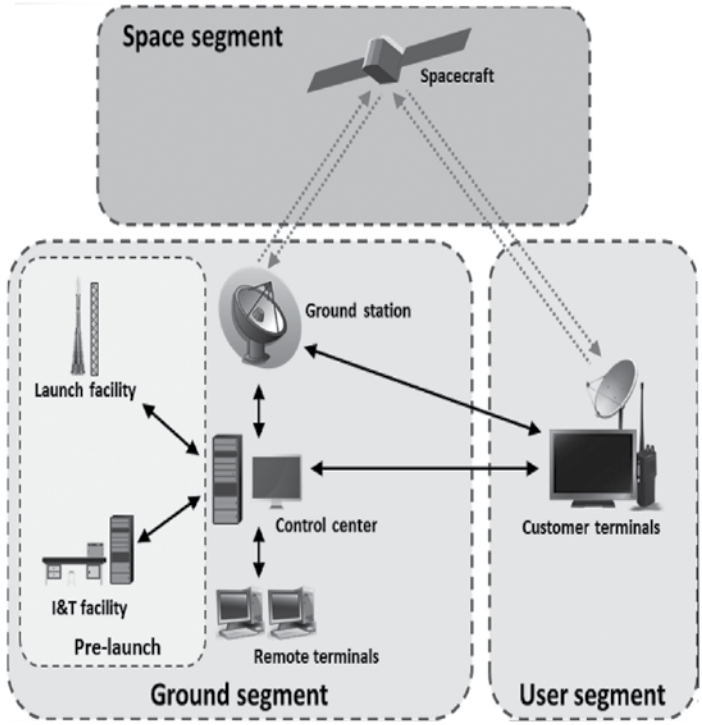
In this paper, we shall identify the threats emerging in the cyber domain and their impact on space assets. Towards the end, we shall analyse the existing cyber security mechanism in the Indian context and

suggest a model to adapt and excel in the space journey despite the cyber threats in the contemporary scenario.

Cybersecurity Landscape in Space Systems

Space Systems. The term "Space system" (Figure 2) includes all the systems and equipments involved in space activities from ground to orbit, sensors to signal data and payloads. This also includes critical technologies such as global positioning systems, communication and imagery systems and economic activities.[7] The two major roles of space systems are in national security and economic development, however, both are at risk of disruption today.

Figure 2: Space Systems



The challenge in the space systems lies in the long-term functionality of the hardware and software of space assets. These systems remain unchanged for up to 10-15 years due to lack of upgradation. Thus, they become easy targets for cyber threats as technology is advancing rapidly in the cyber domain.

Hack of United Kingdom's Ministry of Defence Satellites[8]: In 2023, a cyberattack compromised systems in the UK Ministry of Defence, including systems related to satellite control and communications. It was part of a broader series of state-sponsored attacks on critical infrastructure. While specific details remain classified, the breach raised alarms about the vulnerability of satellite communications and defense systems. This is one of the incidents that became news, however, thousands of cyber attacks occur across the globe on a daily basis. The space systems are not devoid of such attacks. With the enhancement of technology and reduced launch cost of space, the assets are increasing day by day and so are the multitude of threats.

The Indian Computer Emergency Response Team (CERT-In) has recently issued a stark warning about increasing cyber threats to satellite communications, cautioning that "each new satellite added to this intricate network is both an engineering marvel and a potential target for cyber threats". CERT-In issued an advisory on 04 February 2025 stating that "With satellites now deeply integrated into essential daily operations—from navigation to transaction synchronization—any disruption can lead to widespread repercussions."[9]

Threat Spectrum. The space systems function on the 'system of systems' concept—damage to one system will have a cascading effect on multiple systems. The threat spectrum to the systems is multiplying manifolds due to rapid development in this field and the collusive interplay of the public and private players in recent times. Firstly, the vulnerability to the space systems from the adversary is due to its vast importance for a nation. Secondly, the commercialization of the space

sector has enhanced the threat level owing to the lowering cost of space launch and utilisation of commercial off-the-shelf (COTS) components in satellites especially Cubesat. The entry of smaller teams in space operations leads to innovative technological demonstrations.[10] Thirdly, the main means of communication with space objects and ground stations are through the networks and vast numbers of interconnected networks of computers. The uplink and the downlink data of systems are not always encrypted. Thus the opportunity for data manipulation, distortion and disruption exists to the adversary. Fourthly, the vast volume of data collected, handled and communicated by satellites every day offers countless vulnerabilities that can be exploited by any cyber attack.

The Risks. Any cyber attack aims to minimize the exposure and maximize the impact. Having seen the ever-increasing vulnerabilities in space systems, the risks accompanying cyber attacks on these are listed below:

- Taking control of satellites physically and manoeuvring them to collide and destroy.
- Altering the orbits of satellites will render them incapable of performing the designated tasks.
- Deliberately lowering the orbit so that these satellites re-enter the atmosphere and get destroyed. In addition, by using cyber attacks, the control systems of the satellites are altered and causes irreparable damage.
- Jamming, spoofing and hacking of communication networks to target the mission packages. Jamming however is not a typical cyber, but spoofing is a major cause of concern as the user or receiver of the satellite data is unaware of the manipulated data that is being received post-spoofing by any cyber attack.
- Cyber attackers can target the ground systems which control the satellites in space and destroys them.

- The risk to space systems from cyber attacks can emerge from one state to another or military actions.

Types of Cyber Attacks/Threats to Space Assets

Cyber attacks in today's scenario gets easily detected and policies exist to take suitable actions against the defaulters. However, deniability and ambiguity in pinpointing the perpetrator still exist. If we reflect on history 'the Max Headroom' hack remains the gold standard: its content was bizarre, its motives were mysterious, and its perpetrators was never caught'.[11] The types of cyber attacks which occur in the typical IT industry also affect space operations as the systems used are the same.

- ***Malware Attack.*** The most common type of cyber attack is a ***Malware*** (acronym of Malicious Software) attack which includes viruses, trojans, worms, ransomware and spyware. The malware enters the space system through any link on an untrusted email, website or by downloading unauthorized software. Once it enters the computer system, it deploys on the target systems and starts collecting sensitive data, blocks network components and disrupts system functioning by switching off the entire system itself.[12]
- ***Social Engineering Attack*** involves deceiving users into providing an access point for malware. The user unknowingly gives out sensitive data or installs malware on the device as the attackers pose as genuine entities. Main types of social engineering attacks include phishing, baiting, pretexting, Voice Phishing (Vishing), SMS phishing (Smishing), Tailgating and Piggybacking.
- ***Supply Chain Attacks*** are innovative types of cyber threats, to developers and vendors associated with space operations, as it infects genuine applications and dispenses malware by means of source code and software update mechanisms. These attacks are dangerous as the compromised applications are certified by trusted vendors. The entire

supply chain gets infected as the supplier of the systems is not aware that the application has already been compromised since its inception. The type of such attacks include compromising the build tools and code signing procedures; malicious codes are generated during auto updates and embedded in the hardware/software.

- ***Man in the Middle (MitM)*** attack involves interference and interception of the communication between two ends such as the user and application. The attacker gets into the system and steals sensitive data by impersonating and eavesdropping the network. The means used are Wi-Fi eavesdropping, email hijacking, IP, HTTPS & DNS spoofing.
- In a ***Denial of Service (DoS)*** attack, the system gets overloaded with huge data traffic and its normal operations are stalled. If the DoS attack is involved in multiple devices then it is known as Distributed DoS (DDoS). The techniques are SYN flood DDoS (TCP sequence), User Datagram Protocol (UDP) flood DDoS, HTTP flood DDoS and Network Time Protocol (NTP) DDoS.
- An ***Injection Attack*** involves inserting malware into the code of a web application through identified vulnerabilities. Once the attack is successful, sensitive data exposed, the DoS attack is executed and systems are then compromised. The methods of these kinds of attacks are Structured Query Language (SQL) injection, Code injection, Operating System injection, Lightweight Directory Access Protocol (LDAP) injection and Cross-site Scripting.

The list of cyber attacks on space systems in the year 2024 is given in Table 1 below. One of the recent studies by the *Center for Security Studies, at ETH* Zurich that *identified 124 cyberattacks against the space sector*—Distributed Denial of Service (DDoS) attacks constituted 65 per cent, intrusion attacks was 11 per cent and 9 per cent were hacking and leak operations.

Table 1. List of Cyber Attacks on Space Systems in 2024[13]

Month	Year	Type of target	Country targeted	Target	Attacker	Type of attack
February	2024	Company	Luxembourg	SES	Phoenix	DDoS
April	2024	Company	Russia	Astra	IT Army of Ukraine	DDoS
April	2024	Company	Russia	Altegrosky	IT Army of Ukraine	DDoS
March	2024	Company	Russia	Gazprom Space Systems	IT Army of Ukraine	Intrusion
March	2024	Company	Russia	RSCC	IT Army of Ukraine	Intrusion
January	2024	Agency	Russia	Far Eastern Scientific Research Center of Space	BO Team	Intrusion
March	2024	Company	Poland	Floris	NoName 057(16)	DDoS
July	2024	Company	Italy	Leonardo	Cyber Dragon	DDoS
January	2024	Company	Russia	Special Technology Center	GUR	Data breach
July	2024	Research	Russia	Military Training Center at BMSTU	Cyber Resistance	Data leak
June	2024	Research	Netherlands	SRON	62IX GROUP	DDoS
March	2024	Company	Ukraine	Unknown	Pharanos Cyber Army	Intrusion
January	2024	Company	Russia	GPS Update.ru	Anonymous Italia	DDoS

July	2024	Company	USA	TrafficView	LulzSec	DDoS
January	2024	Company	Russia	Sev-Sat	HimarsD DoS	DDoS
June	2024	Company	Ukraine	JSC Kyiv Radar Plant	NoName 057(16)	DDoS
July	2024	Company	Ukraine	JSC Kyiv Radar Plant	Cyber Army of Russia	DDoS
January	2024	Agency	Ukraine	UCRF	Cyber Army of Russia	DDoS
September	2024	Agency	USA	NOAA	CyberVolk	Data leak
April	2024	Company	USA	Starlink	Ukraine (unspecified)	Software cracking
May	2024	Company	Italy	Avio	NoName 057(16)	DDoS
September	2024	Company	France	Safran	JustEvil	Data leak
September	2024	Company	Ukraine	JSC Kyiv Radar Plant	NoName 057(16)	DDoS
September	2024	Company	Ukraine	JSC Kyiv Radar Plant	NoName 057(16)	DDoS
September	2024	Agency	USA	US Geological Survey	CyberVolk	Data breach extorsion
September	2024	Company	Ukraine	Arsenal	NoName 057(16)	DDoS
September	2024	Company	Sweden	Hexagon	User1	Intrusion
September	2024	Unknown	Ukraine	Cell phones (GPS data)	Unknown	Malware

The Wiper malware used in Viasat hack was an unique type of attack and no other operation of that type was observed so far. Thus, we can safely say that most operations against the space systems were unsophisticated attacks with temporary and recoverable consequences.[14]

Nowadays, the hacktivists are taking sides in armed conflicts as evident from the Russia-Ukraine war as also the Israel-Palestine conflict wherein they targetted space systems. Recently, India has announced the launch of multiple satellites to enhance the space based surveillance program. The sources in military establishments told leading newspapers during Aero India 2025 that "The first lot of satellites under the third phase of the space-based surveillance (SBS-3) program will be launched by 2027-28. A total of 52 satellites will be launched under the program".[15] If this is the case then, securing the space systems from cyber threats, needs to be taken seriously. This trend needs to be flagged and mitigation measures need to be implemented as it will heavily impact future operations in space sectors.

Cyber Security Challenges in Space Industry

The concept of cyber security applies broadly to all systems that relies on digital and cyber resources, however, space systems have unique factors that vividly differentiates them from terrestrial complements. Securing space systems against cyber threats poses extraordinary challenges due to operational constraints, environmental factors, and the critical nature of based assets. The major challenges are as follows:

- **Remote & Inaccessibility.** The satellites once launched, are not easily accessible for upgradations physically. Regular maintenance and security enhancements of terrestrial systems are not possible due to their inaccessibility.
- **SWaP constraints and Legacy Systems.**[16] The space systems in orbit are highly controlled by weight, size and power limitations which levy substantial design trade-offs. In terrestrial systems, robust hardware security modules can be incorporated. In addition, due to requirements of lighter weight and low power solutions, employment of legacy technology is selected which is susceptible to modern cyber threats.

- **The lifespan of Satellites**: The average life of a satellite is 15-20 years, thus it becomes difficult to keep pace with ever-evolving cyber threats and cyber security standards.
- **Communication Distances**: Owing to long-distance communication, to and fro signals from satellites are susceptible to interception and manipulation.

Global Strategies to Address Cybersecurity Challenges

An Executive Order (EO) was signed by President Biden on 'Strengthening and Promoting Innovation in the Nation's Cybersecurity'.[17] The order includes detailed measures to protect systems involved in space operations. Section 3, "Improving the Cybersecurity of Federal Systems," and Section 8 "National Security Systems and Debilitating Impact Systems," of EO highlight the actions need to be taken by agencies towards cybersecurity measures to be adopted in the space systems. Also, strict adherence to the cybersecurity protocols by the private players in space operations and implementation of cyber defences on government procures space national systems, have also been highlighted. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has invited experts to revise the Tallinn Manual 'to review legal and policy challenges related to cyber war'.[18] Thus, these global efforts emphasise the importance of an integrated approach to maintaining the security of space infrastructure amidst ever- expanding cyber challenges.

A few strategies that are being implemented/explored to navigate through the challenges globally are:

- **Data and Signals Encryption**: All the agencies involved in space operations need to ensure that all data and signals transmitted to and from satellites are encrypted. This will enhance the protection from interception and tampering. This is akin to the existing model of using advanced encryption protocols in military satellites to secure communication channels.

- **Authentication and Access Control**: Implementation of strong authentication and access control mechanisms to prevent unauthorised access to space systems. These measures apply to both ground systems and the assets in the orbit.
- **Redundant and Fail-Safes Mechanism**: The process of building redundancy of space assets ensures that if one component is compromised, backup systems are available to take over—this will minimize the downtime and impact.
- **Artificial Intelligence(AI) based Detection Systems**: Incorporation of AI and machine learning in space assets to detect unusual activities, such as unauthorized access attempts or abnormal signal patterns, that indicate a cyber threat.
- **Quantum Technology**: Quantum cryptography is an emerging technology with potential applications in satellite communication. This could enhance the encryption key standards that are theoretically impossible to intercept without detection.
- **Hardening Firmware and Software**: Inception of cybersecurity measures to include hardened firmware and software, helps protect satellites from malware. The option of remote updates and rigorous testing, to avoid vulnerabilities, should also be incorporated.
- **International Collaboration and Policies:** Keeping in view the global nature of space, organizations such as the International Telecommunication Union (ITU), United Nations Office for Outer Space Affairs (UNOOSA), European Space Agency (ESA) and other space-faring nations, play a crucial role in establishing cybersecurity standards and promoting collaboration.

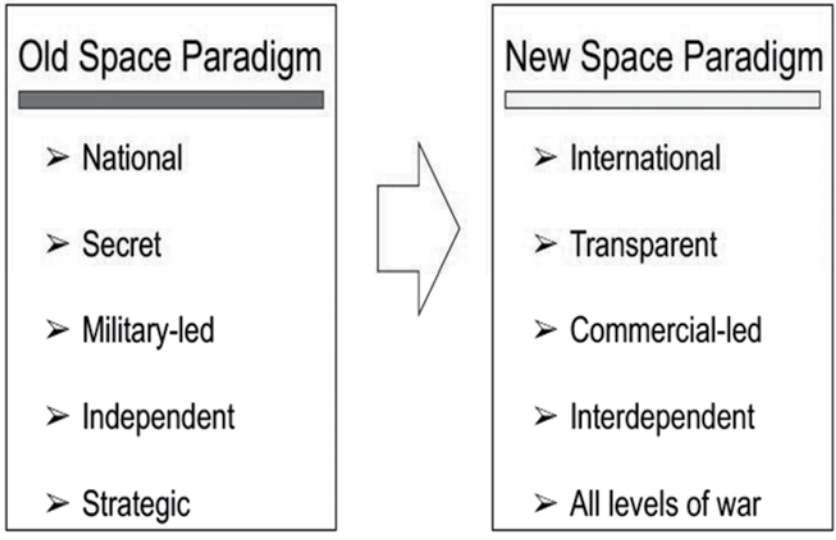
Indian Space Navigating through Cyber Risks

In the space era before the year 2000, the space industry relied on security through obscurity, as the players in the sector were limited. However, the new space era (Figure 3) has opened up to new players and technologies,

thus the previous approach to security needs to be revisited and revamped keeping in view the ever-changing landscape in the cyber domain. Thus, it is clear that threats to space systems exist and at an appropriate level, the following questions must be asked and answered to arrive at critical security measures before deployment of any space systems that may have nationwide impact in the long run.

- Do cybersecurity measures in the nation have collection assets, systems or networks to identify cyber attacks in Space Systems?
- Could disruptions to critical space systems impact national security, economic security, public health or safety?
- Does existing policies, mechanisms or governance structures address defaulters once identified?
- Do systems involved in the space domain incorporates security measures since the inception stage?
- Are the people handling the systems in the space domain adequately trained to avoid any kind of major impact inadvertently?

Figure 3: Old and New Space Paradigm



Existing Mitigation Measures. The Indian Space Research Organisation (ISRO) has made significant strides in space technology and gained worldwide recognition and acclaim. As we continue to make our mark in the global space arena, the necessity for robust cybersecurity measures becomes paramount. The cybersecurity aspect is taken very seriously at ISRO. The cybersecurity framework has been designed to be robust, adaptive, and in line with international best practices. It includes a combination of technical measures, policies, and expertise of certified ethical hackers.[19]

Suggested Measures. The cyber security landscape changes faster than imagined. Thus, India as a nation needs to regularly assess existing means to address cyber threats to its space assets and in addition, incorporate latest solutions available globally. The solutions which are relevant and can be adopted into the realms of cybersecurity of space systems in the Indian context are covered in succeeding paragraphs.

- ***Comprehensive Cyber Security Solutions.*** These are the tools that any organisation/agency should incorporate into systems to defend against cyber threats and accidental damage to sophisticated and sensitive systems. The security solution is available for Application, Network, Cloud and Endpoint devices. The Internet of Things (IoT) security and the Threat Intelligence, are few important aspects that need to be considered by the space systems.
- ***International Collabrations.*** No one country can effectively protect its space assets from contemporary cyber security challenges in isolation. The United Nations Organisation for Outer Space Affairs (UNOOSA) has initiated a discussion on these aspects. All the nations including India can play a crucial role in collaborating and coordinating the existing measures and futuristic means to face challenges and mitigate the same. A successful example of international cooperation is the establishment of the Space Data Association (SDA), an international organization that promotes sharing of data on space

object movements to prevent collisions and mitigate risks. The SDA's collaborative approach serves as a model for addressing cybersecurity threats wherein sharing threat intelligence and best practices can enhance the collective security of space missions.[20]

- ***Cyber Security Training***. The space industry needs cybersecurity training akin to any IT Industry. As of May 2023, a report published by the Business Standard newspaper stated that, 'the industry had about 40,000 open opportunities, indicating the growing demand for skilled cybersecurity professionals. However, the demand-supply gap stood at 30 per cent, projecting a major skill challenge in the industry, according to the study by tech staffing firm TeamLease'.[21] Atmanirbhar Bharat mission should also focus on the training of youth and professionals working in the Space domain to build an ecosystem of homegrown software and skilled cybersecurity workers. The number of skilled cyber security professionals has increased from one lakh in 2021 to three lakhs in 2023, however, we still need to focus on investing on latest technologies.
- ***Rigorous Security Testing Protocols***. The software and hardware being developed or assembled in India should undergo rigorous Security Testing Protocols before it is deployed in any system. Most of the space projects today are kind of prototype projects that lack required security protocols. However, the same systems are studied in detail by the threat actors who may utilise it in the future against the target nations. Hence, all efforts at the apex level need to be initiated to address the vulnerabilities. The same can be achieved by sharing existing technologies with novice players and interchanging the technologies to build resilience space systems to face cyber threats.
- ***Zero Trust Security Architecture for Space Systems***. The Space Systems Command (SSC) in the US is partnering with industries to develop and integrate a Zero Trust security solution across the entire space assets—from ground systems to satellites and other

related systems.[22] Implementing zero-trust security mechanisms by ISRO can significantly enhance the security and resilience of its space missions and infrastructure. It helps in Protection of Sensitive Data, Enhanced Network Security, Real-Time Threat Detection, Secure Remote Access and Resilience Against Cyber Attacks.[23]

- ***Quantum Technology and AI***. Quantum technology has emerged as a potential solution to address the ever-escalating cyber threats across the globe. ISRO has made significant strides in quantum communication; employment of quantum key distribution for enhanced encryption will go a long way to mitigate the Cyber threats to space systems. With the advent of AI and machine learning, new dimensions have been added to cybersecurity, calling for a collective effort from all arenas including technology firms, academia, and cybersecurity experts. Thus, collaborative and cooperative measures will form a formidable force to reckon with, which will be essential to safeguard India's space systems from cyber threats.

Conclusion

Cybersecurity for space systems in future will be shaped by increasing reliance on satellite constellations and the accelerating speed of cyber threats. As the constellation grows, threat complexity will grow exponentially which will require seamless coordination and collaboration of multiple agencies to mitigate the challenges. Autonomous solution to the future anticipated threats will take centre stage.

Key Takeaways. Cybersecurity begins with improving encryption standards, encryption of the uplink and downlink communication between the satellite and the ground stations as well as implementation of cryptographic techniques like quantum encryption and end-to-end protocols. In addition, a comprehensive relook into the training of the workforce in dealing with the systems in space operations, is required.[24] The legal framework in cybersecurity-related aspects of space systems

will require continuous review not only by a particular nation but as a collaborative effort by all the space-faring nations.

A study was published by the Foundation for Defence of Democracies in April 2023 wherein it was recommended that space systems need to be designated as a critical infrastructure[25] sector keeping in mind the enhanced utility in our everyday lives. However, in the same study, it was also brought out that having identified the threats in the space domain, many years back, steps taken by the United States have been inadequate. To counter cyber threats in space, a combination, of regulatory frameworks, technological advancements and operational strategies must be implemented by space faring nations.

India, whose ambition in the space domain is taking a positive stride, needs to identify the threats and enhance collaboration with other space-faring nations and learn from their previous experiences and build a robust and resilient ecosystem to thwart away any challenges of cyber security. In addition, private player's infusion in the space domain is a welcome measure, but the protocols of cyber security should at no cost be compromised. As it is said, today's solutions may become tomorrow's problem—the speed of development in space systems undertaken today should not impede our path of navigation in this glorious space journey tomorrow due to cybersecurity aspects.

Notes

1. Srivastava, "SpaDeX Mission: Revolutionising Space Exploration Pioneering India's Future in Space."
2. "Russian Satellite Internet Downed via Attackers Claiming Ties to Wagner Group."
3. "India Needs Better Cybersecurity for Space Systems."
4. "Space Economy In India: Size, Opportunities, Regulatory Framework, And Government Initiates - PWOnlyIAS."
5. "Space Economy In India: Trends, Innovations, And Future Prospects - PWOnlyIAS."
6. Srivastava, "SpaDeX Mission: Revolutionising Space Exploration Pioneering India's Future in Space."
7. Cilluffo and Shields, "Time to Designate Space Systems as Critical Infrastructure."
8. "UK Military in Data Breach - and Other Cybersecurity News | World Economic Forum."

9. "CERT-In Warns of Cyber Threats to Satellites, Says Each New Satellite Is a 'Potential Target'."
10. Calabrese, "Space Oddity: Space Cybersecurity Lessons from a Simulated OPS-SAT Attack."
11. Serena, "The Max Headroom Incident And The Creepy Mystery Behind It."
12. Attacks, "Cybersecurity Threats What Are Cybersecurity Threats ? Common Sources of Cyber Threats Types of Cybersecurity Threats."
13. Poirier, "CYBERDEFENSE REPORT Hacking the Cosmos : Cyber Operations against the Space Sector A Case Study from the War in Ukraine."
14. Clémence Poirier, "Trawling Hacker Forums Uncovers Crucial Information on Space Cyber Attacks | November 2024."
15. "Aero Show 2025: First Batch of Satellites under New Space Surveillance Programme to Be Launched by 2027-28."
16. Shahzad et al., "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers."
17. "Cybersecurity Executive Order Includes Direction on Space Systems—Office of Space Commerce."
18. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations | National Security Archive."
19. "Safeguarding the Stars: A Deep Dive into ISRO Cyber Security Measures."
20. Antara Jha, "Cybersecurity in Space and the Challenges of International."
21. Business Standard, "Cybersecurity Jobs: India Suffering High Cybersecurity Skill Gap, 40k Open Positions: Report."
22. Agency, "Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment."
23. Agency.
24. "The Growing Threat of Cyberattacks on Space Assets | New Space Economy."
25. Cilluffo and Shields, "Time to Designate Space Systems as Critical Infrastructure."

References

"Aero Show 2025: First Batch of Satellites under New Space Surveillance Programme to Be Launched by 2027-28." Accessed February 19, 2025. https://www.deccanherald.com/india/karnataka/bengaluru/aero-show-2025-first-batch-of-satellites-under-new-space-surveillance-programme-to-be-launched-by-2027-28-3402717.

Agency, Infrastructure Security. "Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment," no. April (2024).

Antara Jha. "Cybersecurity in Space and the Challenges of International" Vol 18 Iss (2024): 1–8. https://www.defstrat.com/magazine_articles/cybersecurity-in-space-and-the-challenges-of-international-regulation/.

Attacks, Malware. "Cybersecurity Threats What Are Cybersecurity Threats ? Common Sources of Cyber Threats Types of Cybersecurity Threats," 2024, 1–8. https://www.imperva.com/learn/application-security/cyber-security-threats/.

Business Standard. "Cybersecurity Jobs: India Suffering High Cybersecurity Skill Gap, 40k Open Positions: Report," 2024. https://www.business-standard.com/technology/tech-news/india-suffering-high-cybersecurity-skill-gap-40k-open-positions-report-123062100397_1.html.

Calabrese, Matteo. "Space Oddity: Space Cybersecurity Lessons from a Simulated OPS-SAT Attack," 2023.

"CERT-In Warns of Cyber Threats to Satellites, Says Each New Satellite Is a 'Potential Target.'" Accessed on February 19, 2025. https://www.moneycontrol.com/technology/cert-in-warns-of-cyber-threats-to-satellites-says-each-new-satellite-is-a-potential-target-article-12943940.html.

Cilluffo, Frank, and RADM (Ret.) Mark Montgomery Sharon Cardash Kelsey Shields. "Time to Designate Space Systems as Critical Infrastructure," 2023. https://www.fdd.org/analysis/2023/04/14/time-to-designate-space-systems-as-critical-infrastructure/.

Clémence Poirier. "Trawling Hacker Forums Uncovers Crucial Information on Space Cyber Attacks | November 2024." interactive.satellitetoday.com, n.d. https://interactive.satellitetoday.com/via/november-2024/trawling-hacker-forums-uncovers-crucial-information-on-space-cyber-attacks.

"Cybersecurity Executive Order Includes Direction on Space Systems – Office of Space Commerce." Accessed on February 19, 2025. https://www.space.commerce.gov/cybersecurity-executive-order-includes-direction-on-space-systems/.

"India Needs Better Cybersecurity for Space Systems," n.d. https://www.darkreading.com/ics-ot-security/india-cybersecurity-space-critical-infrastructure.

Poirier, Clémence. "CYBERDEFENSE REPORT Hacking the Cosmos: Cyber Operations against the Space Sector A Case Study from the War in Ukraine," no. October (2024). https://doi.org/10.3929/ethz-b-000697348.

"Russian Satellite Internet Downed via Attackers Claiming Ties to Wagner Group." Accessed on February 14, 2025. https://www.darkreading.com/cyberattacks-data-breaches/hackers-claiming-wagner-group-ties-down-russian-satellite-internet-comms-.

"Safeguarding the Stars: A Deep Dive into ISRO Cyber Security Measures." Accessed on February 20, 2025. https://www.linkedin.com/pulse/safeguarding-stars-deep-dive-isro-cyber-security-giridaran-e/.

Serena, Katie. "The Max Headroom Incident and The Creepy Mystery Behind It," 2021. https://allthatsinteresting.com/max-headroom-incident.

Shahzad, Syed, Keith Joiner, Li Qiao, and Felicity Deane. "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers," 2024, 1–23.

"Space Economy In India: Size, Opportunities, Regulatory Framework, And Government Initiates - PWOnlyIAS." Accessed on February 14, 2025. https://pwonlyias.com/current-affairs/space-economy-in-india/#space-economy-in-india.

"Space Economy In India: Trends, Innovations, And Future Prospects - PWOnlyIAS." Accessed on February 14, 2025. https://pwonlyias.com/editorial-analysis/space-economy-india/.

Srivastava, Santosh Kumar/ Gouri S/ Vatsla. "SpaDeX Mission : Revolutionising Space Exploration Pioneering India s Future in Space," 2025. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jan/doc2025116486201.pdf.

"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations | National Security Archive." Accessed on February 20, 2025. https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations.

"The Growing Threat of Cyberattacks on Space Assets | New Space Economy." Accessed on February 20, 2025. https://newspaceeconomy.ca/2025/02/13/the-growing-threat-of-space-based-cyber-attacks/.

"UK Military in Data Breach - and Other Cybersecurity News | World Economic Forum." World Economic Forum, 2024. https://www.weforum.org/stories/2024/05/cybersecurity-news-lockbit-scattered-spider/.

Strengthening the Core: Building Input Material Foundations for Ammunition Self-Sufficiency

Biju Jacob

Abstract

India's goal of turning itself into a superpower in defence manufacturing hinges upon the availability and usability of materials for ammunition production. The current status of key material, such as metals, explosives, chemical stabilizers, and smart component is comprehensively reviewed with focus on their sourcing patterns, their import dependence and the vulnerability of their supply chain. Recent reforms and policy interventions under Atmanirbhar Bharat and the Defence Production and Export Promotion Policy (DPEPP) 2020 have not led too far, away from the dominance of imported strategic materials (such as RDX, HMX, tungsten and rare earth components) in the Indian supply chain. Major challenges including being short of domestic refining capacity, having fragmented procurement

Brigadier (Dr) **Biju Jacob**, VSM, commissioned in June 1994, is an alumnus of the National Defence Academy and Defence Services Staff College and has done the Higher Defence Management Course and Advanced Professional Programme in Public Administration. He is an ammunition expert and has vast experience in management of ammunition and missiles and has been involved in various studies on storage, disposal, proof, life extension and 'Make in India' initiative of ammunition.

system, technological gaps and geopolitical risks that might interrupt ammunition manufacturing are outlined in the paper. Based on the United States, China and Israel comparative insights, the paper suggests a multi-faceted Indian roadmap, including, indigenous mining, public-private partnerships, strategic stockpiling, advanced R&D and skill development. With a view to form a National Defence Material Grid (NDMG), the proposed formation of a material procurement, purchase, and traceability unification step is posited as a game changer among various means. India can secure its defence preparedness by strengthening the material ecosystem, reducing its import dependence and placing itself on the global stage of ammunition and defence manufacturing.

Introduction

A nation's readiness and autonomy for defence and its armed forces' capability relies on the manufacturing of ammunition. In addition to production of bullets, shells and missiles, is a highly industrialized process involving metallurgy, chemical engineering, electronics and advanced manufacturing techniques. Given India's large armed forces and growing regional security responsibilities, the supply of mobile, indigenous, high-quality ammunition is crucial since disruptions would be eminently embarrassing and destabilizing. The geopolitical context of the country—with long border tussles, cross border terrorism and strategic rivalry in Indo-Pacific region makes the need for a resilient and self-reliant defence industrial base still more redundant (Mukherjee et al., 2021).

India's historic ammunition manufacturing has largely remained in the state control of the Ordnance Factory Board (OFB) to promote efficiency, accountability and modernization, which had recently been corporatized into seven Public Sector Undertakings (PSUs). This

structure has worked, in a sense, to meet the basic necessities regarding the Indian Armed Forces but it has not been able to catch up with technological advancements, dynamic perceived threats, and rising smart ammunition and high technology munition requirements. A key factor behind this impasse is the country's reliance on imports of raw materials like metals, copper and tungsten, chemicals like RDX and HMX, and high-tech electronic components to manufacture precision guided ammunition (Kumar et al., 2023).

An 'Atmanirbhar Bharat Abhiyan' has recognized ammunition production as a strategic endeavour towards self-reliance on defence sector. The Defence Production and Export Promotion Policy (DPEPP) 2020 has ambitious targets for increasing indigenous content in defence production as well as reducing dependence on foreign suppliers, which provide evidence of the practice. Defensive Strategy of Atmanirbhar Bharat includes development of India as a global defence manufacturing hub by motivating private sector participation, FDI liberalization and pushing innovation through research and development (Rajan et al., 2022). Despite these policy efforts, however, there is a fundamental bottleneck related to the lack of adequate domestic availability as well as inadequate processing capabilities of essential input materials.

The lack of key input material is multifaceted in nature. India has huge mineral resources, but exploiting it is hampered by environmental restrictions, obsolete mining technologies, logistical snags, and lack of investment in modern material science. In addition, the defence sector needs high purity, defence grade materials such as special alloys, propellants, electronic sensors and almost none of this is available in India or cannot be manufactured in the country right now either. In addition, it increases the cost of production and carries very high risks to the country security with regard to geopolitical disruptions, trade sanctions, or war, (Sharma et al., 2020).

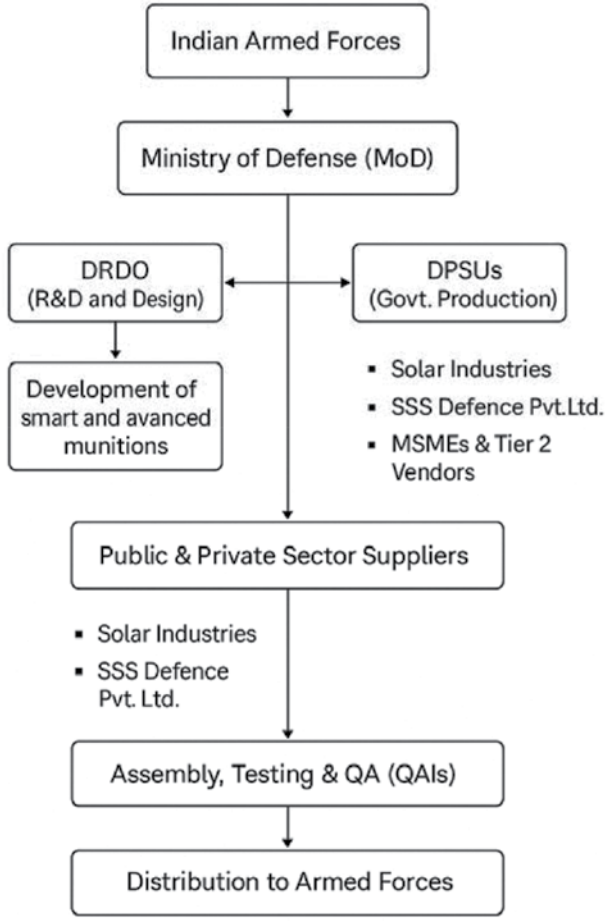
Therefore, there must be a comprehensive strategy aimed at securing and developing domestic sources of raw materials for ammunition manufacturing, which is to be self-reliant. These include building mining infrastructure, encouraging refining and processing technologies, providing incentive for the public-private partnership and integration of supply chains through defence corridor and industrial clusters. Additionally, indigenous material substitutes and the propagation of sustainability in the extraction and recycling of materials present long term solutions to constraints.

Given this context, a critical analysis of the availability of input materials for ammunition manufacturing in India is both timely and necessary. Such an inquiry must address key questions: What are the critical materials required for different types of ammunition? To what extent are these materials sourced domestically? What are the existing challenges in material procurement, processing, and integration into the defence supply chain? And most importantly, what policy, industrial, and technological interventions can pave the way for sustainable and strategic material self-sufficiency? By shedding light on this critical aspect of defence preparedness, the study contributes to the broader national goal of achieving technological and strategic autonomy.

Ammunition Manufacturing in India

Ammunition manufacturing in India is an essential part of its defence production capability, covering a broad spectrum of munitions such as small arms cartridges, artillery shells, air-dropped bombs, tank ammunition, rockets, and smart or precision-guided munitions. Each category of ammunition has its unique material requirements, production technologies, and supply chain complexities, all of which influence India's defence readiness and strategic autonomy.

Figure 1: Indian Ammunition Production Ecosystem



Small arms and ammunition includes bullets used in rifles, pistols, and machine guns—ranging in caliber from 5.56 mm to 12.7 mm. These are widely used by the Indian Army, paramilitary forces, and police services. The heavy firepower in the armed forces is based on artillery ammunition in 105 mm, 130 mm and 155 mm shells. The indigenous platforms such as Arjun MBT and T-90 come equipped with tank and anti-tank ammunition. Aerial bombs, mortar shells and rocket propelled

grenades are other important categories. However, in recent years, the interest has been pivoted to smart ammunition and guided munitions, that collectively consists of electronics and sensor for higher accuracy, lethality, and reduced collateral damage (Singh et al., 2023).

Traditionally, Ordnance Factory Board (OFB), as it was then known, constituted the largest manufacturer of munitions in India; it has been restructured into seven defence Public Sector Undertakings (DPSUs) under the Ministry of Defence. Among these, Advanced Weapons and Equipment India Limited (AWEIL) and Munitions India Limited (MIL) have been given the ammunition production responsibility. Currently, MIL is the biggest conventional ammunition producer in India and cater for all three services of the armed forces as well as of paramilitary and police forces (These DPSUs produce over 150 guns including small, medium, and high caliber rounds) [Mukherjee et al. 2021].

Along with the public sector, some private players have also entered the aperture of ammunition manufacturing in a liberal set of defence industrial policies of the government. One of the notable ones is Solar Industries India Ltd., a Nagpur based company that fast likes by its reach in domain of high energy materials, explosives and propellants. A close ally is SSS Defence in Bengaluru, which is into small arms and ammunition designed for the Indian terrain and operational requirements. DRDO and DPSUs, these companies are getting increasingly closer to Defence Research and Development Organisation with an aim to develop next generation munitions as well as to reduce the import dependence.

The establishing of Defence Industrial Corridors (DICs) in Uttar Pradesh and Tamil Nadu is a major enabler for this transition. The purpose of these corridors is to create an integrated ecosystem of defence manufacturing by providing infrastructure, policy encouragement and cluster-based development. Uttar Pradesh is being developed as key nodes around can also support ammunition and small arms manufacturing at Kanpur, Aligarh, Jhansi and Chitrakoot. DIC of Tamil Nadu includes

Coimbatore, Salem, Hosur and Chennai with component and special manufacturing units. It is also anticipated that these corridors will be able to indigenize critical components and input materials required in the production of ammunition (Rajan et al., 2022).

Flagship initiatives such as Make in India, Atmanirbhar Bharat Abhiyan and the defence production and export promotion policy (DPEPP) 2020 further bolster India's vision of self-reliance in defence. The goal of these initiatives is to enhance the indigenous content in defence production from the present 60–65% to more than 80 percent in coming decade. This means that not only will ammunition be manufactured both domestically, but capabilities along the upstream streams of material extraction, refining, propellant chemistry, and electronic sub-systems will be developed commensurate with the demands of the resultant ammunition products. Amongst them the government has identified various types of ammunition which are included in the Positive Indigenization list, thus prohibiting their import (Kumar et al., 2023).

Although such efforts have been made, inconsistencies, lack of quality control, and lowered global competitiveness are still challenges. However, the changing defence industrial landscape with increasing levels of foreign investment, private sector participation and R&D collaboration implies a positive trend towards achieving self-sufficiency in terms of ammunition manufacturing in India.

Key Input Materials for Ammunition Production

However, the manufacturing of ammunition is a very laborious process and it is highly depended on the availability of the value-added input materials. Included in these materials are metals and alloys of casing and penetrators, high energy explosives and propellants for charge and propulsion, chemicals and binders for stability and performance, and more recently advanced electronics and sensors for smart or guided ammunition. Ensuring a consistent and indigenous supply of

these components is fundamental to achieving self-reliance in defence manufacturing.

Metals and Alloys

Metals and alloys form the structural backbone of ammunition. **Brass**, an alloy of copper and zinc, is extensively used for cartridge cases due to its corrosion resistance, formability, and high ductility. India sources a significant portion of its brass from Hindustan Copper Ltd., although imports still supplement domestic production to meet defence-grade specifications (Kumar et al., 2023).

Copper, valued for its excellent electrical and thermal conductivity, is crucial not only for brass but also for electric primers and fuses in smart ammunition. **Steel,** particularly high-carbon and stainless variants, is used in projectile cores, bomb casings, and armour-piercing shells due to its superior mechanical strength and penetrative capability.

Tungsten, a dense and hard metal, is employed in kinetic energy penetrators and armour-piercing rounds. However, India lacks domestic tungsten reserves and relies almost entirely on imports, primarily from China and Russia, making it a strategic vulnerability (Rajan et al., 2022). **Aluminum,** known for its light weight and thermal resistance, is commonly used in aircraft-delivered munitions, missile casings, and pyrotechnic compositions. It also enhances the thermobaric effects of certain explosives.

The development of high-performance alloys combining the properties of two or more of these metals is also critical, especially in next-generation and smart munitions where weight, impact resistance, and thermal performance must be carefully balanced.

Propellants and Explosives

Propellants and explosives are the energetic materials responsible for launching the projectile and causing terminal effects on the target.

Among the most commonly used high explosives in Indian ammunition manufacturing are RDX (Cyclotrimethylenetrinitramine) and HMX (Cyclotetramethylene-tetranitramine). RDX is widely used due to its high detonation velocity and relatively safe handling characteristics, while HMX is reserved for high-performance military applications including warheads and shaped charges.

TNT (Trinitrotoluene), although older, remains a widely used explosive due to its balance between stability and explosive power. India has indigenous production facilities for RDX and TNT, although production of high-purity HMX remains limited and often depends on imports or joint ventures.

Nitroglycerine (NG) and **Nitrocellulose (NC)** form the core of single-base, double-base, and composite propellants used in artillery and tank ammunition. Glycerol and cellulose are synthesized through nitration; these are however very stringent to the environmental and process controls. Though India is capable of producing these materials, environmental restrictions and the degradation of the infrastructure have limited output volumes and consistency (Mukherjee et al., 2021).

Chemicals, Stabilizers, and Binders

Chemical, stabilizers and binders play vital roles exactly on the same level as the explosive materials in modern ammunition. Shelf life is improved, premature detonation is prevented, and performance is improved under various climatic conditions by these additives.

In nitrocellulose based propellants, stabilizers like Diphenylamine or Centralite are added in order to help retard degradation over time. These compounds retard the autocatalytic decomposition of energetic materials and are critical to prevent the occurrence of unsafe situations during storage and transportation.

Polymeric binders are made more flexible and the brittleness of explosives are reduced by the addition of plasticizers like tributyl citrate

and diethyl phthalate. Since HTPB (Hydroxyl-Terminated Polybutadiene) and GAP (Glycidyl Azide Polymer) binders have become very energetic, they are increasingly used as binders in composite propellants for missiles and rocket systems.

Generally, these chemicals are being imported because there are no big facilities for large scale, defence grade production in India. Thus, they also need to be procured within the international compliance frame of the Chemical Weapons Convention (CWC), further complicating the complexity.

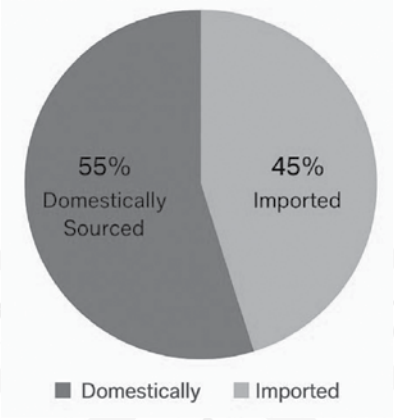
Electronics and Sensors for Smart Ammunition

Electronics in ammunition is indispensable with the progression of modern warfare, and the need for precision precursor strike. Miniaturised electronics enable smart ammunition such as guided artillery shells, loitering munitions and programmable airburst rounds to navigate, detonate and target.

MEMS (Micro Electromechanical Systems) sensors, gyroscopes, accelerometers, fuzes and programmable logic controllers are core components. The precision targeting, inflight trajectory correction, and optimized detonation enhances mission effectiveness.

With the exception of inputs such as silicon and copper, India currently does not possess domestic production capabilities for most of these advanced electronic components. But Bharat Electronics Ltd (BEL) and others have now started developing indigenous solutions; but it remains a heavily imported sector, with imports coming from the US, Israel and South Korea, among others (Singh et al., 2023). As part of the "Make in India" and Defence Electronics Policy, development of a robust ecosystem for defence microelectronics is therefore a key priority.

Figure 2: Key Input Materials in Ammunition and Their Sources



Sources and Supply Chains of Input Materials in India

A robust and resilient ammunition manufacturing industry is heavily reliant on the strength of its raw material sourcing and supply chain infrastructure. In India, the availability of input materials for ammunition—ranging from metals and explosives to electronics and chemical stabilizers—hinges on a combination of domestic mining and processing capabilities, the involvement of micro, small, and medium enterprises (MSMEs), foreign imports, and an array of regulatory and logistical frameworks. Understanding the intricacies of this supply chain is essential for charting the path towards strategic self-sufficiency in defence production.

Mining and Processing Companies

Though India is rich in natural resources, their application to defence purposes is somewhat limited because of technological, regulatory and policy constraints. Hindustan Copper Ltd. (HCL) is the lead state owned enterprise engaged in copper ore mining and smelting which is a critical metal for pistol cartridges as well as critical for electronic components. Despite being the only vertically integrated copper producer in the country, HCL fulfils only a fraction of India's defence requirements,

necessitating imports from countries like Chile, Zambia, and Indonesia (Kumar et al., 2023).

The **National Mineral Development Corporation (NMDC)** plays a pivotal role in the mining of iron ore, which is essential for producing steel used in shell casings, bomb bodies, and armour-penetrating ammunition. However, the conversion of iron ore into defence-grade steel requires specialized alloying and heat treatment processes, typically carried out by select public and private sector units.

The **Bhabha Atomic Research Centre (BARC)** is a key institution for the development of high-energy materials and rare-earth processing, especially those used in advanced munitions and smart ammunition electronics. While BARC has made substantial contributions to India's nuclear and missile programs, its capacity to scale and commercialize materials for conventional ammunition remains limited, requiring partnerships with manufacturing firms and defence PSUs.

Involvement of MSMEs and Local Industry

MSMEs form the backbone of India's industrial ecosystem and play a vital role in the defence supply chain, particularly in the supply of non-strategic components and sub-systems. These include cartridge clips, packaging materials, small mechanical parts, primers, and fuse components. Under the Defence Procurement Procedure (DPP), MSMEs have been encouraged to participate more actively in supplying to DPSUs and private ammunition manufacturers.

In addition, industrial clusters around **Pune, Hyderabad, Coimbatore, Kanpur, and Nagpur** have emerged as hubs for component manufacturing, machining, and chemical processing. Some of these MSMEs have received DRDO technology transfers for specific defence applications, such as thermobaric chemicals, plastic-bonded explosives, and additive manufacturing for fuse components (Rajan et al., 2022). However, MSMEs often face challenges related to finance,

certification for defence-grade quality, and long payment cycles from large procurement agencies**.**

Foreign Imports and Strategic Dependencies

Despite the availability of some raw materials domestically, India remains dependent on foreign suppliers for several critical inputs. A significant portion of high-purity **tungsten, copper, nickel, RDX, HMX,** and propellant stabilizers is imported due to inadequate local production or quality constraints. The primary countries from which India imports defence-grade materials include **China, Russia, Israel,** and the **United States.**

China is a dominant supplier of rare-earth elements and tungsten, but India's over dependence poses strategic vulnerabilities in light of ongoing border tensions. Advances in smart munitions and electronic fuzing systems are provided by both **Israel** and **Russia** in the explosives, propellant formulation, large caliber shell component areas. The **United States**, under bilateral defence cooperation agreements, supplies a wide range of energetic materials, precision electronics, and defence chemicals (Mukherjee et al., 2021).

The higher cost of procurement, as well as the risks to supply chain disruption in the case of geopolitical crisis, a global pandemic or a diplomatic dispute, increases the dependency on external imports. Additionally, the import of such materials can take on long lead times, complex international licensing and export control as in the case of export control regimes such as Wassenaar Arrangement.

Licensing, Environmental Regulations, and Logistical Constraints

Ammunition materials are highly regulated in India for procurement and production. The Explosives Act of 1884 governs the licensing of production, transport and storage of explosives and propellants of which the Petroleum and Explosives Safety Organisation (PESO) is the

supervisory agency. While all these regulations are necessary for national safety, they could also delay production timelines because of bureaucracy and inspection time.

The other layer of complexity is environmental regulations, particularly those that pertain to mining and chemical processing. As an example, the nitrocellulose and nitro-glycerine are extracted and refined from hazardous waste that must be dealt under the directives of the Ministry of Environment, Forest and Climate Change (MoEFCC). The many regulatory constraints tend to discourage private participation in capacity expansion and delay it.

The defence supply chain suffers from additional economic and logistical inefficiencies. There are strict security norms for the transportation of explosive materials—this includes restricted routes, restricted timings and constant police escort. Moreover, India's rail and road infrastructure continues to be optimized for the lower priority—more time insensitive requirements of defence logistics (Sharma et al., 2020).

Key Challenges in Material Availability

India's ambition to self-reliance in defence manufacturing, specifically ammunition production, depends on what input materials are available. Although policy initiatives, structural reforms and technological progress have been made to address the lack of sources, supply and technological integration of such materials, the ecosystem supporting their sourcing, processing and integration continues to be dilapidated. Below are the key challenges that limit the availability of material in India's ammunition manufacturing value chain.

Limited Domestic Production of Critical Metals and Explosives

The most urgent is lack of domestic production of vital metals and explosives used in ammunition. Although India has natural reserves of iron and bauxite, as well as copper, but it does not have shown reserves or

efficient extraction capability for a number of strategic materials, including tungsten, nickel, tin and rare earth metals which are vital for production of armor-piercing round, penetrators and other electronic components used in smart munitions.

High purity explosives such as RDX, HMX and CL-20 are produced domestically by very few defence laboratories and public sector units and are constrained by outdated equipment, exhausted processes, bottlenecks and environmental compliance. This increased reliance on import and growing shortages of supply during high demand scenarios is due to lack of ability to scale up production of these materials.

Technological and R&D Limitations

Another critical barrier is the lack of indigenous capacity in advanced materials research and development (R&D). Defence manufacturing demands materials that exhibit superior properties—such as high melting points, thermal stability, corrosion resistance, and energy density—under extreme operational conditions. India's public sector institutions like DRDO and BARC have made progress in niche areas, but the translation of laboratory-scale innovations to industrial-scale production remains limited (Singh et al., 2023).

Furthermore, private sector involvement in defence materials R&D is minimal due to high entry barriers, long gestation periods, and limited access to testing infrastructure. There is also lack of dedicated national centres for research in defence metallurgy, explosives chemistry, and smart materials, leading to technological dependence on foreign suppliers for high-performance alloys and precision electronics.

Import Dependency and Foreign Exchange Concerns

India continues to depend heavily on imports for several raw materials and semi-processed components such as tungsten carbide, beryllium, fuzing systems, optical fibers, and programmable guidance modules. While

global sourcing offers technological advantages, it also subjects India's ammunition supply chain to volatility in foreign exchange rates, tariff fluctuations, and supply chain markups.

Additionally, the procurement of such strategic materials from foreign vendors often involves complex compliance with international regulations, export control regimes (e.g. ITAR, Wassenaar Arrangement), and licensing requirements, which further delays procurement and increase costs (Mukherjee et al., 2021). This import dependency also creates an imbalance in India's defence trade posture, affecting long-term sustainability and national security.

Geopolitical and Pandemic-Induced Supply Chain Risks

Recent global events, such as the COVID-19 pandemic and geopolitical tensions with China, have exposed severe vulnerabilities in India's external supply chains. During the pandemic, the international movement of materials like high-grade copper, electronic sensors, and explosive precursors was significantly delayed due to lockdowns, port closures, and logistic disruptions. These delays impacted the timely production and delivery of ammunition for both training and operational readiness.

Furthermore, the strategic rivalry between India and China, of which the latter is India's major supplier of rare earth materials and electronic sub-components, constitutes a serious security risk. India runs the danger of losing access to crucial materials that are hard to substitute or rapidly replaced with complementary supply from non-Indian sources (Rajan et al., 2022). Similarly, the Russia–Ukraine conflict has disrupted traditional supply lines for military-grade metals and explosives, thus affecting global pricing and availability.

Lack of Integrated Procurement Framework

The current defence material procurement framework in India is fragmented across various departments, PSUs, and armed service

commands. The absence of a unified and digitized **National Defence Material Grid** results in poor forecasting, overlapping orders, and inefficient inventory management. Many ammunition manufacturers face delays due to non-availability of timely approvals, licenses, or supply chain transparency.

Procurement procedures under the **Defence Acquisition Procedure (DAP)** are also time-consuming and often not aligned with the fast-paced demands of modern ammunition production cycles. Additionally, there is limited interoperability and coordination between public-sector production units, DRDO laboratories, and private suppliers—resulting in delayed indigenization efforts and under-utilization of domestic capabilities (Sharma et al., 2020).

Skill Gaps in Material Science and Defence Metallurgy

A less visible but equally critical challenge is the **shortage of specialized human resources** in areas like **defence metallurgy, explosives chemistry, material formulation,** and **defence-grade electronics.** Most Indian technical institutions focus on general engineering disciplines, with limited exposure to defence-specific applications in materials science.

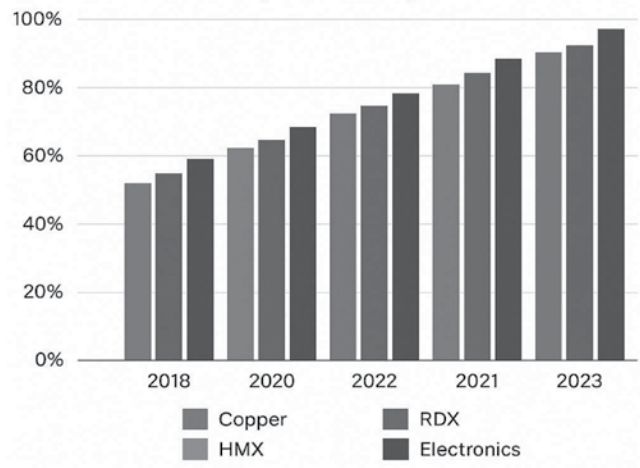
While premier institutes like **IITs, IISc**, and **DRDO centres** offer select programs, there is a glaring gap in vocational training and mid-level technical workforce for operating and maintaining explosive manufacturing facilities, metallurgical plants, and quality testing units. This lack of skilled manpower affects not only R&D but also the quality assurance and safety of finished ammunition products (Verma et al., 2021).

Global Best Practices and Comparative Insights

To strengthen its ammunition manufacturing capabilities and achieve material self-sufficiency, India can draw valuable lessons from the defence production strategies of other leading nations. Countries such

as the United States, China, and Israel have developed robust systems for managing strategic materials, thus ensuring seamless integration of industrial and military objectives. Their models offer insights into how India can restructure its policy, infrastructure, and innovation ecosystem to enhance indigenous capacity in ammunition manufacturing.

Figure 3: Import Dependence of Strategic Materials (2018–2023)



United States—Defence Industrial Base and Rare-Earth Policy

The United States maintains one of the world's most advanced defence industrial bases, supported by a well-orchestrated supply chain network and a strategic focus on critical materials. Through its **Defense Production Act (DPA)** and **National Defense Stockpile Program**, the US government ensures availability of essential raw materials such as rare-earth elements, titanium, beryllium, and high-performance alloys required for munitions and advanced weapon systems.

The **Defense Logistics Agency (DLA)** plays a key role in managing inventories and coordinating with private manufacturers to maintain strategic reserves of metals and chemicals. Furthermore, the **Office of**

Industrial Base Policy ensures that defence procurement decisions support domestic production and technological innovation (DoD, 2021).

To mitigate supply chain risks, especially from China, the US has prioritized the **reshoring** of rare-earth mineral processing and invested in public-private partnerships to develop alternative sources from allied nations such as Australia and Canada. These initiatives aim to secure long-term independence in critical material supply (Papp, 2020).

China–Integrated Military–Industrial Complex

China's success in defence manufacturing, particularly in material self-sufficiency, lies in its **civil-military integration (CMI)** strategy. Under this model, Chinese defence production is deeply embedded within its national industrial and scientific framework. State-owned enterprises such as **Norinco** and **China North Industries Group** manage end-to-end production of ammunition and explosives, sourcing materials directly from domestic mining and chemical industries.

China controls over 60% of the global supply of **rare-earth elements**, including neodymium and dysprosium, which are critical to guided missile systems and smart munitions. Through policies such as the '**Made in China 2025**' plan, the government provides massive subsidies and policy support for indigenous R&D in materials science and explosives engineering (Zhang et al., 2019).

Additionally, China has heavily invested in **automation, artificial intelligence**, and **nano-materials** in munitions development, creating high-performance, lightweight, and cost-efficient weapons. In particular, Indians involved in indigenization can draw from the experience of China in top-down integration on the industry-academia-defence services.

Israel–Innovation in Material-Efficient Smart Weapons

Israel's successful innovation-driven, defence manufacturing sector is particularly relevant for resource constrained countries and can be used

to develop a similar model. The development of smart ammunition using a reduced footprint of material, while maintaining lethality and precision, made history through companies such as Rafael Advanced Defense Systems, IMI Systems, and many more.

The strength of Israel's design is the ability to configure modular weapon systems using standardized components that are optimal for resource use and flexible manufacturing. Compact, fast and capable of firing a large number of shells or rockets, Israeli firms manufacture high impact munitions with minimal reliance on strategic metals using innovations in microelectronics, MEMS based sensors and lightweight composite materials (Levy et al., 2021).

On the other hand, Israel's defence system of R&D is an ecosystem that is characterised by close collaboration between the military, the universities, and the startups. SIBAT (International Defence Cooperation Directorate) helps the government agencies to promote indigenous technology and facilitate global partnership. This can be emulated by India by making stronger DRDO, IIT, and private industry linkages.

Policy Frameworks India Can Adopt

India stands to gain by selectively adapting policy frameworks from these nations:

- From the US, India could adopt **strategic stockpiling** of rare and essential materials and establish a **Defence Materials Authority** akin to the DLA.
- China's **civil-military integration model** can inspire India to establish defence-focused **industrial clusters** with dedicated material supply lines.
- Israel's **innovation incubation and modular design** philosophy could guide India's R&D model towards agility and cost-efficiency.

Additionally, India can also examine bilateral resource sharing and international research collaboration for diversifying sourcing and improve its strategic material supply chain. A globally competitive and self-reliant ammunition production ecosystem can be built with the correct combination of policy, investment and institutional coordination in India.

Recent Developments and Indian Initiatives

In the backdrop of many years of defence material self-sufficiency challenges and global supply chain vulnerabilities, India has evolved several strategic policies and initiatives that promote growth of indigenous defence manufacturing ecosystem. All of these measures converge with the national vision of Atmanirbhar Bharat (Self Reliant India), for the reduction in import dependency, improvement in industrial capability, and increase in export of defence products including ammunition and other related materials.

Defence Production and Export Promotion Policy (DPEPP) 2020

The Defence Production and Export Promotion Policy (DPEPP) 2020 is a comprehensive policy for indigenous defence production. According to the policy, annual turnover of INR 1.75 lakh crore and export revenues of INR 35,000 crore in defence manufacturing should be achieved by 2025. The MoD focuses on 3 criteria for DPEPP: development of critical technologies, decrease of import dependency on strategic materials, and expansion of domestic capacity through innovation and infrastructure investment (MoD, 2020).

It also establishes the mechanisms for indigenization of imported parts, classification of items for local production on the Positive Indigenization List and has mechanisms for supporting the startups and MSMEs in ammunition components development, raw materials and explosives development.

Strategic Partnerships and DRDO-Industry Collaboration

Within the last few years, the Defence Research and Development Organisation (DRDO) has partnered with both public and private industry players to speed up production of ammunition and smart munition payloads. Specially under the Strategic Partnership Model, Indian private firms are being given the nod to partner with DRDO, and foreign OEMs (original equipment manufacturers) for the co-development and manufacture of high technology defence products.

It resulted in transfer of technologies (ToT) for high energy materials, propellant systems, electronic fuzing, metal alloys, to companies including Solar Industries, SSS Defence and Bharat forge. Apart from that, DRDO also provides handholding while testing prototypes, licensing and quality standardization.

Defence Testing Infrastructure Scheme (DTIS)

The Defence Testing Infrastructure Scheme (DTIS), announced in 2020, is taken as the groundwork of a good quality assurance system. Under the public-private partnership, DTIS would spend an allocation of INR 400 crore to set up state-of-the-art testing facilities for defence equipment and materials.

These facilities are especially useful for the qualification of the performance and safety of ammunition materials such as explosives, stabilizers, metals, and fuzing systems. In DTIS program, the testing infrastructure is being set up at various key defence manufacturing clusters which are reducing the dependency on limited number of government labs, and shortening the product validation cycles (Raksha Mantri Report, 2021).

Technology Development Fund (TDF)

The **Technology Development Fund (TDF),** administered by DRDO, is designed to finance the development of defence technologies by Indian

startups, MSMEs, and academia. TDF supports projects with high-risk, high-reward potential in fields of **energetic materials, composite metallurgy, pyrotechnics,** and **defence electronics**.

Through TDF, several indigenous materials and components used in ammunition—such as thermobaric explosives, lead-free primers, and composite casings—are currently under development. The initiative encourages innovation and ensures that small-scale developers can contribute meaningfully to defence self-reliance without being hindered by financial constraints (DRDO, 2022).

These policy interventions and programmatic developments underscore a paradigm shift in India's defence production strategy—moving from state-controlled to a **collaborative, innovation-driven ecosystem** focused on building long-term resilience in material sourcing and ammunition manufacturing.

Recommendations and the Way Forward

To achieve long-term self-reliance in ammunition manufacturing, India must address the foundational gaps in its material availability and production ecosystem. While significant progress has been made through recent policies and institutional reforms, sustainable and scalable development demands a multi-dimensional approach. The following recommendations outline strategic interventions aimed at building a robust domestic ecosystem for input materials, fostering innovation, and enhancing national defence preparedness.

Indigenous Mining and Advanced Refining Facilities

The first and foremost priority is to expand and modernize **domestic mining and refining capabilities** for key input materials such as copper, tungsten, nickel, aluminum, and rare-earth elements. India must move beyond ore extraction to **value-added processing**, which is essential for producing defence-grade raw materials.

Existing public sector companies such as **Hindustan Copper Ltd., NMDC**, and **IREL** should be provided with policy incentives and technology upgradation support to increase output and reduce wastage. At the same time, private players should be encouraged to invest in **rare-earth separation plants, metal purification,** and **high-performance alloy processing** through tax incentives and simplified environmental clearances (Kumar et al., 2023).

Public-Private and International Joint Ventures

To reduce technology gaps and foster innovation, India should actively promote **public-private partnerships (PPPs)** and **international joint ventures (JVs)** in ammunition material development. DRDO and defence PSUs can collaborate with domestic private companies in areas such as **explosives chemistry, fuzing systems,** and **microelectronics** through co-development and co-production models.

Additionally, JVs with countries like **Israel, France, South Korea, and Japan** can help acquire technologies for high-purity energetic materials, advanced binders, and precision guidance components. These collaborations should focus on **long-term technology transfer, localization of supply chains,** and **export-oriented production** to maximize strategic and economic benefits (Rajan et al., 2022).

Strategic Material Stockpiling and Warehousing

India should establish a centralized mechanism for **strategic material stockpiling**, especially for high-dependency and high-cost materials like **RDX, HMX, tungsten, rare-earth magnets,** and **high-purity metals.** These stockpiles should be managed under a proposed **National Defence Material Authority,** akin to the US Defense Logistics Agency.

Such facilities can ensure **buffer reserves during conflicts, supply chain disruptions, or emergency procurement delays**. Geographic

diversification of warehouses and integration with defence industrial corridors (e.g. UP and TN DICs) will enhance logistical efficiency and inventory security (Mukherjee et al., 2021).

Boosting Research in Energetic Materials and Smart Components

Targeted R&D support must be extended to academic institutions, startups, and industry for developing **next-generation energetic materials, eco-friendly propellants, lead-free primers, programmable fuzes,** and **miniaturized smart components**. Special emphasis should be placed on **dual-use materials** that can be repurposed for both military and civilian applications.

Programs under **Technology Development Fund (TDF)** and **IMPRINT** should be scaled up and aligned with global trends in smart ammunition and nanomaterial-based explosives. Establishing **Centres of Excellence in Defence Materials** at premier institutes such as IITs, IISc, and NITs will foster interdisciplinary innovation and practical applications (Singh et al., 2023).

Formation of National Defence Material Grid (NDMG)

A unified and digital **National Defence Material Grid (NDMG)** should be established to centralize procurement, inventory management, and inter-agency coordination. This platform would provide real-time insights into the availability, consumption patterns, and projected demand of critical input materials across all defence units.

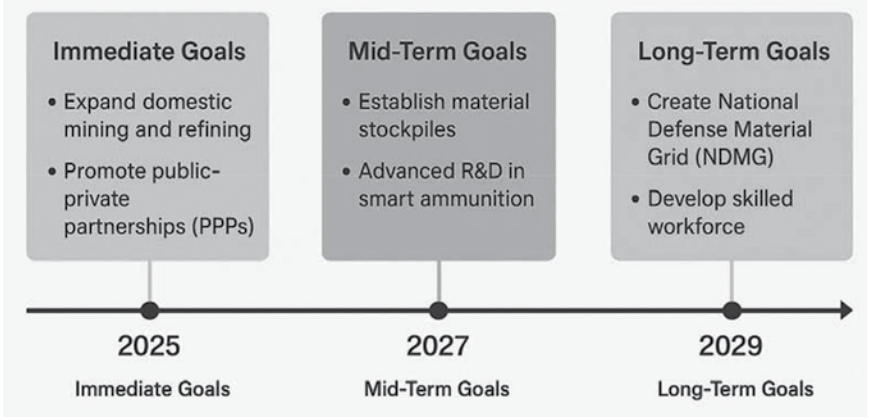
The NDMG should link stakeholders across the value chain—from raw material suppliers and manufacturing units to logistics providers and quality control agencies—ensuring **supply chain transparency, reduced redundancy,** and **better planning**. It can also serve as a single-window system for licensing, tenders, and compliance tracking (Sharma et al., 2020).

Capacity Building and Skill Training for Material Scientists

In order to create a workforce capable of grooming a future ready defence metallurgy, materials science, explosives engineering and defence electronics, India must invest in human capital development in these areas. It can be put into place through the introduction of specialized diploma and postgraduate programmes, short-term certification and on-the-job training modules in collaboration with DRDO, academia and industry.

IIT Madras, IISc Bengaluru, DIAT Pune can very well establish niche programs in high performance materials and safety engineering at institutions like it. Moreover, industrial training institutes (ITIs) located near the defence industrial corridors could incorporate such special modules as propellant handling, quality testing, and material safety protocols (Verma et al., 2021).

Figure 4: Roadmap for Material Self-Reliance in Defence Manufacturing (2025–2030)



Conclusion

India's efforts for self-reliance in ammunition manufacture is at a cusp, influenced by its in-house and outside realities. The country has, in many ways, been commendable in developing a 'pull' from within,

with indigenization of weapon platforms and extending private sector presence. However, critical input materials availability continues to remain a fundamental bottleneck. Vulnerability of India's defence supply chain lies in its dependence on imports to supply strategic metals, high energy explosives such as RDX and HMX, and smart components such as microelectronics and sensors making India vulnerable for defence procurement.

These material constraints are basically strategic constraints, rather than just logistical constraints. However, on the occasion of geopolitical unpredictable disturbances, trade embargo, or global supply recessions (like COVID-19 and ongoing conflicts), India's capability to fulfil the operational requisite of its armed forces can get severely curtailed. First of all, the dispersed nature of the domestic material ecosystem is joined by insufficient R&D capability for defence grade materials and a shortfall in mining and refining infrastructure that carries along with systemic delays as well as increase in costs and restricted innovation.

In this respect, achieving self-sufficiency in ammunition materials is not a goal, but a strategic necessity. It enables the country to function with full operational independence, shield themselves from these supply chain shocks, and reduce their need for foreign vendors for this critical wartime resource. Besides, an auto-reliant defence material ecosystem can serve as a spur for industrial growth, employment generation and export competitiveness, thereby ensuring both India's national security and economic resilience in general.

Therefore, there is a critical imperative for a consolidated national endeavour by the public and private sectors, as well as academia, scientific institutions and strategic partners. This strategy should include all the elements of developing a National Defence Material Grid (NDMG), the establishment of indigenous facilities for mining and advanced refining, R&D support in energetics material and smart munition devised, and structured skill development programs.

India's concept of Atmanirbhar Bharat in defence manufacturing will always be incomplete without material sovereignty. By empowering India's ammunition manufacturing capabilities, this will also provide a robust and resilient material ecosystem for India to strengthen its position as a global defence manufacturing hub of the future.

References

Department of Defence. (2021). *Annual Industrial Capabilities Report to Congress.* U.S. Department of Defence.

DRDO. (2022). *Technology Development Fund Guidelines.* Defence Research and Development Organisation. https://tdf.drdo.gov.in

Kumar, P., Reddy, V. K., & Nair, S. (2023). *Strategic materials in India's defence manufacturing: Challenges and opportunities.* Defence Technology Review, 18(2), 122–135.

Levy, G., Barkat, R., & Mizrachi, A. (2021). *Smart Ammunition in the Age of AI: Israel's Experience*. Journal of Defence Innovation, 6(1), 58–73.

Ministry of Defence. (2020). *Defence Production and Export Promotion Policy (DPEPP) 2020.* Government of India.

Mukherjee, A., Sharma, T., & Singh, R. (2021). *Evaluating the transformation of India's ordnance factories: A supply chain perspective.* Journal of Defence Studies, 15(4), 45–60.

Papp, J. F. (2020). *Rare Earth Elements: Supply Chain in the United States.* U.S. Geological Survey.

Rajan, M., Gupta, D., & Joshi, P. (2022). *Atmanirbhar Bharat and defence sector reform: The road ahead*. Indian Journal of Public Policy, 10(1), 89–104.

Raksha Mantri Report. (2021). *Annual Report on Defence Initiatives.* Ministry of Defence, Government of India.

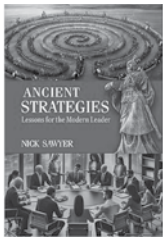
Sharma, R., Tripathi, N., & Mahapatra, B. (2020). *Self-reliance in defence manufacturing: Issues and policy recommendations.* Policy Perspectives, 7(3), 101–117.

Singh, A., Verma, N., & Das, P. (2023). *Smart ammunition and modern warfare: Trends in India's defence innovation*. Journal of Military Technology and Innovation, 9(1), 65–78.

Verma, R., Das, A., & Nayak, S. (2021). *Bridging the skills gap in India's defence sector: A strategic imperative.* Indian Journal of Technical Education, 28(3), 78–85.

Zhang, Y., Liu, Q., & Chen, H. (2019). *Military–Industrial Integration and Innovation in China*. Asian Defence Journal, 27(3), 89–104.

Ancient Strategies: Lessons for the Modern Leader
By Nick Sawyer



New Delhi: Pentagon Press, 2025, Price 1495/-,
Hardcover, pp. 400, ISBN: 978-81-980002-1-7

Review by Harjeet Singh

Project Udbhav, initiated by the Indian Army in 2023, endeavours to unearth the profound Indic heritage of statecraft and strategic wisdom embedded within ancient Indian texts on statecraft, warfare, diplomacy, and grand strategy. A valuable addition to the literature on India's past is *Ancient Strategies: Lessons for the Modern Leader***.** The author, Brigadier Nick Sawyer is an alumnus of India's National Defence College and served as UK's Defence Attache to India from 2022-2024.

The book analyses the works of six ancient strategists and draws out the key lessons articulated by each. These lessons are then contextualized and contemporized for the modern leader into an easy to absorb and easy to apply set of guidelines. Common lessons from across ancient works are also extracted to provide the ageless fundamentals of effective strategy. The eclectic choice of ancient works analyses Asian strategies and writings, with Julius Caesar being an outlier.

Part 1 of the book looks at developing a strategic mindset and studies the works of Miyamoto Musashi, especially The *Book of Five Rings*, and the Indian epic—*The Mahabharata*. The first essential requirement for successful strategy is for the senior leader to have a strategic mindset. Before any analysis, planning or process can be applied to a complex

Colonel **Harjeet Singh** (Retd) is a defence analyst and author of several books, monographs and articles on military matters. Views expressed are personal.

problem, the strategic leader must be in the right frame of mind. This can take a lifetime to develop as experience counts a lot. Both can be used to help create the strategic mindset for senior leaders that is so critical for tackling complex problems in the 21st Century.

Part 2 looks at what the author calls 'adopting a strategic approach.' It is the cultural approach opted within the highest levels of a government or organisation on the 'tradecraft' of strategy rather than how to deal with a specific problem or situation. It looks at the Kautilya *Arthashastra* which covers statecraft, governance and warfare. It also looks at the *Purananuru*, a collection of works that gives advice to kings on how to manage their subjects and lands, and offers some thoughts on adopting strategic approaches to complex problems, besides analyses of the Tamil concept of valour. Beyond its importance for understanding the development of South Asia's history, culture, religion, and linguistics, the *Purananuru* is a great work of literature, reflecting accurately and profoundly the life of southern India 2,000 years ago. It is a collection of 400 heroic poems about kings, wars and public life, of which two are lost and a few have survived into the modern age in fragments. The collected poems were composed by 157 poets, of which 14 were anonymous and at least 10 were women. It is indeed a hidden gem of world literature.

Finally, Part 3 analyses the works of Sun Tzu and Julius Caesar and presents some strategic toolsets to assist with developing and implementing specific strategies. Strategy is very different to simple plans and tactics as it needs creativity and flexibility. Sun Tzu's *Art of War* and Julius Caesar's *Commentaries on the Gallic War* give some useful toolsets that can help senior leaders and their teams devise a successful strategy to deal with a specific problem set which are designed more as a checklist and prompt rather than a rigid set of rules.

The study of history by professional military personnel is important, if for no other reason but to further educate themselves. By studying history, we can identify our strengths, weaknesses, and those of our enemies. The

battlefield and technology will continue to change but there are many ancient verities that deserve study to draw relevant lessons.

Spanning a comprehensive spectrum and eliciting useful lessons for the modern leader in a very readable and pellucid prose, the book presents the ancient texts in an engaging manner. The straightforward language to highlight relevance retains the readers' interest. With a vision to integrate ancient wisdom into modern military pedagogy, the book provides insights drawn from centuries-old principles to navigate today's intricate strategic landscape. The book provides a valuable addition to the literature on the subject and offers insights and lessons for military professionals, diplomats, business leaders and students of the ancient past.

It is clear that ancient military history has come a long way. Nevertheless, there is much work remaining to be done. While war was a central part of ancient cultures and civilizations, it is still rare to see a military historian who studies the Classics. The book's relevance and clarity are likely to resonate strongly as it represents an additional arrow in the quiver of knowledge and find its application in myriad ways. The book is well researched and provides some thought provoking insights worthy of imbibing.

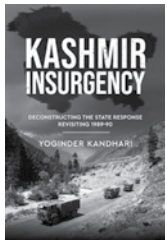
Ancient military history has always been popular, and this remains the case. One can study the subject also on television, on the internet and in documentaries (of course of varying quality). It would be difficult to overstate the importance of warfare and military institutions in the ancient world. Beyond the prevalence of warfare itself, nearly every facet of life in the ancient world viz. art, literature, music, religion, trade, agriculture, manufacturing, gender roles, architecture, education, and science—influenced, and was influenced by warfare and the military institutions tied to it. Hence, it is not surprising that warfare and the military have been important components of historical narratives for as long as they have existed. All successful military leaders did not expect a plan of operations to survive beyond the first contact with the enemy. They set only the

broadest of objectives and emphasised seizing unforeseen opportunities as they arose. Strategy is not a lengthy action plan—it is the evolution of a central idea through continually changing circumstances.

The book fills a critical gap in the literature on the subject and will be of keen interest not only to military formations and units but also to the diplomatic community and academic institutions as also individual researchers and readers. It has a useful bibliography which will be of interest to those who wish to study the subject further. This book is highly recommended for professionals and scholars alike who seek to comprehend the application of ancient military strategies to their modern context.

As both war and national security became topics of increased public participation, officers, defence analysts, and academics turn to the past to support or critique virtually all national security topics, including doctrine, force structure, reform, and strategy. The past can certainly inform the future and it will be unwise to not take advantage of such accumulated experiences.

Kashmir Insurgency: Deconstructing the State Response Revisiting 1989–90
By Yoginder Kandhari



White Falcon Publishing, 2025, Price 626/-,
Hardcover, pp. 308, ISBN: 978-9349311237

Review by RC Patial

Why do I settle down to review "*Kashmir Insurgency: Deconstructing the State Response Revisiting 1989–90*" by Yoginder Kandhari, especially over 30 years after that historically turbulent time? Particularly now, when India has moved ahead with assertiveness, as seen post the 22 April 2025 Pahalgam attack on innocent Hindu tourists—paraded, identified, and shot at point blank range in front of their families. I happened to be in the Valley during that period, doing '*Jungle Bashing*' based on intelligence inputs rooted in the past rather than forecasting the future. Reading Kandhari's detailed study took me back down my memory lane.

The author, Yoginder Kandhari a retired Indian Army officer and a Kashmiri Pandit offers a deeply informed view of the 1989–90 insurgency in Kashmir, when Kashmir believed "*Azadi was round the corner.*" The book captures the confused ground situation during that time from a security and administrative perspective. Drawing on his extensive Counter Insurgency (CI) experience, Kandhari delivers an in-depth analysis of the

Colonel **RC Patial**, SM, FRGS, PhD is a retired Infantry officer of 11 GR. He possesses unique experience of serving in active CI Ops across the country and in Sri Lanka. Has served with the NSCS as a Senior Defence Specialist and in NTRO as OSINT Chief Editor. He is a regular writer on military matters, mountaineering, travelogues and international relations. The veteran is a keen mountaineer and a trekker. Presently, he is the Principal of Amity Indian Military College, Manesar.

events surrounding the forced exodus of the Kashmiri Pandit community and the state's faltering response—a subject close to every Kashmiri Pandit's heart.

The book is organized into four main chapters—*Looking the Other Way*, *Subversion Within*, *Blindfolded*, *Army Pushed into Crucible*, and *The Kashmiri Pandits*—the latter occupying a significant portion in terms of volume and importance.

Col Bhanwar Singh, a commanding officer at the time of a Gorkha Battalion, laments: *"We were silent spectators to the Pandit's departure from the valley. We heard Masjid loudspeakers blurting out threats to them. We had no time for the Pandits."* That single statement encapsulates institutional indifference. He further recalled that "*by the end of 1989, the State police had given upon countering the insurgents and almost abandoning their posts*".

Brigadier Mahalingam, the Commander of the newly inducted Brigade from Nagaland, recalls that "*No one at the Helm knew What was Happening*!" The first task allotted to this Brigade by the Corps Commander was to remove loudspeakers and anti-India banners under *'Op Banner'*.

The Govt of India handled the Rubaiya's kidnapping case in a very meek way which led to an avalanche of abductions and Farooq had forewarned of the consequences. *JeI* had published a booklet in Urdu '*Hizbe Islam*' (Virtues of Islam) a near outline plan of Pakistan's 'Op Topac'.

Sharing from personal experience—on de-induction from Sri Lanka aboard a military special train to Nagaland, we expected the battalion would be diverted to J&K given the brewing crisis in the Valley. That didn't happen immediately, but three months later, the Brigade rushed to Kashmir. General VN Sharma, at the Badami Bagh Corps HQ Helipad in early 1990, briefed us to "*Train and Prepare for an*

Offensive to Go Across!" (Pg 126). What followed is well documented in the book—never part of a permanent CI grid, we operated as floaters in the Valley. Two future Army Chiefs were commanding formations then.

The Author examines the administrative and security failures in detail, highlighting flawed response mechanisms during a period of escalating internal collapse. The narrative is enriched with firsthand accounts, official documents, and ground-level observations, offering a multifaceted perspective of the insurgency's early days and the socio-political factors that fed it.

The ideological backdrop is stark. Pakistan's deep-seated belief that India seeks '*Akhand Bharat*' (Greater India) was countered by General Zia-ul-Haq, who declared: "*Islam is our goal. Quran is our constitution. Jihad is our path. War till victory—God is great.*" He further outlined Pakistan's intent to liberate Kashmir and subvert India through political intrigue and religious radicalisation.

The book delivers an unflinching account of how Pakistan-backed Jihadism, aided by growing radicalisation, collided with an Indian state caught flat-footed. Yet, beyond the cross-border terrorism narrative lies a harsher truth—of political apathy, collapsed intelligence networks, and moral failure during a humanitarian crisis. All of it happened in plain sight, as a "Lackadaisical Ostrich Approach" prevailed—open borders Highway enabled Kashmir's youth to be converted into so-called Jihadis by the proxy war machinery operating from PoK.

Today, India has shed much of the strategic confusion that marked the 1989–90 period. The silver lining is clear: Contemporary India is assertive, not expansionist. Prime Minister Modi's '*Operation Sindoor*' marked a shift in doctrine. No longer will India tolerate cross-border provocations without a decisive and proportionate response. The operation signaled India's commitment to regional stability and national

honor. Yet, while this new assertiveness is welcome, we must remain vigilant—'Pakistan's Proxy War' has not ended with *Operation Sindoor*.

"*The Proxy War against India by Pakistan has No Fronts, No Rules of the Game and is Not Time Bound Anymore*!"

The work "*Kashmir Insurgency: Deconstructing the State Response Revisiting 1989–90*" with detailed historical background stands out. Based on three years of meticulous research and built on firsthand interviews with officials, politicians, civil society, and common Kashmiris, it paints a comprehensive picture of the covert Jihadist crusade enabled by Pakistan and abetted by Indian institutional inertia. Courageous, unbiased, and compassionate, this is essential reading for anyone seeking to understand the Kashmir conundrum—a land betrayed and people abandoned.

A must-read for those who lived through the insurgency, Security Forces who fought aimlessly, the Kashmiri Pandit community across generations, and all serious Kashmir watchers.

Notes for Contributors

General

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

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

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

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

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

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

Mandatory Certificates

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

Style of the Journal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mailing Address: All manuscripts should be addressed to:

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

CLAWS JOURNAL

Journal of the Centre for Land Warfare Studies

CLAWS JOURNAL

Journal of the Centre for Land Warfare Studies

CLAWS JOURNAL

SUBSCRIPTION RATES

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

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

Please Print

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

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

Note: Kindly add Rs. 80.00 as postage charge

CLAWS JOURNAL

SUBSCRIPTION RATES

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

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

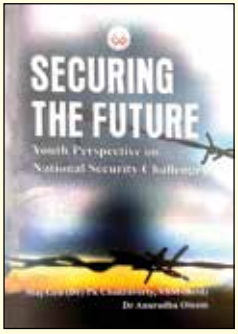
Please Print

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

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

Note: Kindly add Rs. 80.00 as postage charge.

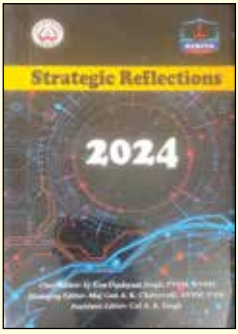
PUBLICATIONS



Securing the Future
Youth Perspective on National Security Challenges

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

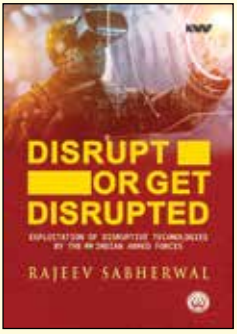
INR 695/- (PB)



Strategic Reflections 2024

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

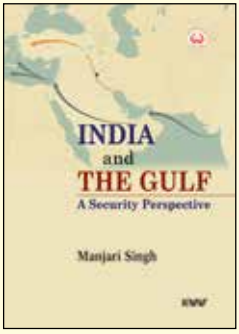
INR 1,495/- (HB)



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

Rajeev Sabherwal

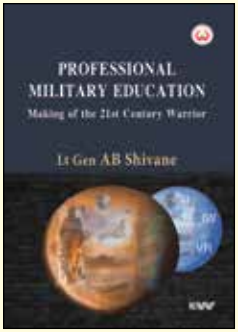
₹ 2580/- (HB)



India and the Gulf
A Security Perspective

Manjari Singh

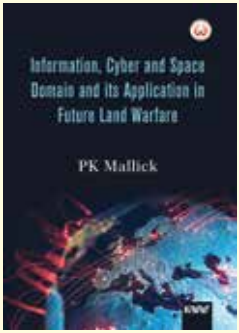
₹ 1880/- (HB)



Professional Military Education
Making of the 21st Century Warrior

Lt Gen AB Shivane

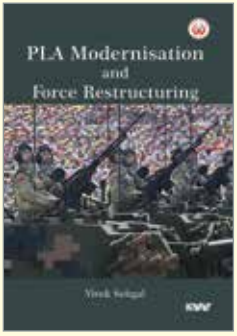
₹ 1680/- (HB)



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

PK Mallick

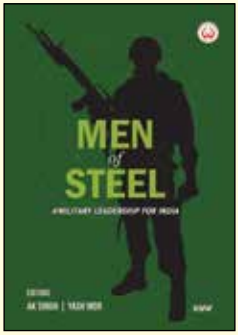
₹ 1580/- (HB)



PLA Modernisation
and
Force Restructuring

Vivek Sehgal

₹ 1680/- (HB)



Men of Steel
#Military Leadership for India

AK Singh | Yash Mor (Eds.)

₹ 680/- (PB)