CIVIL MILITARY FUSION FOR INTEGRATED STRATEGIC DETERRENCE AND INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE

Brig Anshuman Narang*

Abstract

Civil Military Fusion (CMF) is no new West innovated approach or Communist Party of China's (CPC) "Whole of Nation" approach with Chinese Characteristics. National security requires a coherent CMF approach since defence forces are not the sole guarantors of a country's peace and stability. Apropos, Indian civil agencies and military forces are equal stakeholders for ensuring Integrated Strategic Deterrence (ISD) to prevent war and provision of accurate and synthesized Intelligence Surveillance and Reconnaissance (ISR) to negate strategic surprises. The 'Sanjay' of Mahabharat and repeated strategic signalling to Karan by Krishna aptly highlight the DIME (Diplomatic Information Military Economic) approach for ISD and ISR from ancient Indian epics. This essay will focus on adoption of a synergised CMF approach for ensuring ISD and ISR.

Introduction

The ancient Indian civilization boasts of CMF right from the epics of Ramayana and Mahabharat, Vedas and Upanishads to Kautilya's Arthshastra. Dr (Mrs) Manju Narang in her book "Sanskrit Wangmaya Mein Sainya Vyavastha" (Military Systems in Sanskrit Literature) aptly highlights Indian original thoughts of CMF. In order to revive our 'Golden Bird' era, it is utmost essential for India to implement two visions

simultaneously 'GATI SHAKTI' and 'SAINYA SHAKTI' for a strong 'ATMARNIRBHAR-BHARAT 2047'.

21st century was predicted as the end of long-drawn conventional wars. Most NATO countries had drastically curtailed their defence expenditures. The Armenia-Azerbaijan war first and then Russo-Ukrainian war of 2022 has blown off all such predictions. The determination of Ukrainian populace, military and government together have shown the tremendous achievements of actual fused CMF strategy. Closer home, China is a nation in perpetual war state. The CPC General Secretary Xi Jinping's repeated video addresses including latest ones in 2023 ask for war preparedness from forward troops in Western Theatre Command as also CMF in ensuring People's Liberation Army (PLA) becomes a world class army by 2049.

The longest drawn Sino-Indian standoff peaked at Galwan clash in 2020 has neither faded nor remain restricted to one sector with latest clashes in Yangtse sector in December 2022. Two essentials stand out clearly- the failure of Integrated Strategic Deterrence (ISD) despite possession of nuclear weapons and importance of multi-domain ISR in timely anticipating military build-up and predicting adversary's courses of action and places of combat power application.

Integrated Strategic Deterrence (ISD)

The Chinese Science of Military Strategy (SMS) 2020 adopts Henry Kissinger's formula of calculating Deterrence as a product of Capability/ Strength, Intent/ Determination and Adversary's assessment of capabilities/ Strategic Information Transmission. The product in any multiplication is zero if any of the input is a zero. The three years of Sino-Indian standoff and ever-increasing aggressiveness against Taiwan has continuously shown Chinese practical CMF approach in climbing seven out of eight steps of its escalation ladder[1]. Whereas, the conversion of anticipated Russian short special operation into elongated attrition war has shown the dismal failure of synergy within Russian defence forces itself and an appreciable 'Whole of Ukraine' national resolve duly enabled by multi-nation NATO support. The Chinese Cs of modern-day grey zone coercion and compellance approaches adopted by our

adversaries need to be matched by the Ds of Deterrence together by the national civil and defence structures.

Grey Zone Cs / Stages	Recommended Indian Ds for Enhanced ISD	China's Escalation Ladder Steps[2]	Recommended CMF for Disrupting Escalation Ladder	
Co-exist / Collaborate / Cooperate			Civil Field	Military Field
Compromise / Constraint	Stage short of crisis		Convergent Confidence Building Measures	
Crisis	Deter	1. Create an atmosphere of war	Diplomatic manoeuvring & Strategic Signalling	Prepare, enhance capability, display strength
Communicate	Diminish the bluff / Discourage	2. Show advanced weapons	Develop technology, Narrative building	Visualise, Induct, train & update doctrine
Compete	Disturb & Display Cohesiveness	3. Holding military exercises	Academic wargaming with allied think tanks	Joint exercises – with and without allies
Contest	Dislocate / Deny	4. Adjust military deployment	Infrastructure development	Rebalance to plug vulnerabilities
Confront	Dissuade / Deceive	5. Raising the level of combat readiness	Enhance manufacturing capacity; Cognitive hardening	Display Operational Preparedness & Equipment Effectiveness
Coerce	Disorder & Decapacitate	6. Implementing information attacks	Sanctions; QPQ counter & harden to deny; Develop redundancy	Deny recce, develop counters & Strike

| Compel | Delay, Disrupt & destroy | 7. Restrictive military operations | DIME Narrative 'Depict Adversary as aggressor' | Defend disputed areas strongly & counter-attack decisively |
| Combat Provocation | Defeat Decisively to force de-escalation | 8. Warning military strikes | Multi-domain National Resilience | Harden to prevent damage; Defeat ISR & precision; Assured counter-strike |

Table 1: Disrupting Adversary's Grey Zone Coercion Escalation Ladder

An Indian CMF approach to ISD thus requires a cross-domain display of all three inputs - Capability, Intent and Strategic Signalling to punitively deter our adversaries from misadventures, Salami-slicing, Coercion or Compellance. The first part of this essay will thus focus on CMF to achieve ISD in Diplomatic, Information / Cognitive, Cyber, Military, Space, Technology, and Economic domains.

Diplomatic. Negotiations with Chinese is an art which can only be developed by aggregating diplomatic, political, and military lessons. The two varieties of Chinese negotiators, PLA's local Commanders and Diplomats, have limited manoeuvrability with remote control in the hand of CPC's boss. The continuity of Chinese negotiators also ensures an institutionalized knowledge of contentious issues facilitating timely identification of weak spots of adversaries' negotiation plan or historical fault line. Hence, any lack of coherence amongst Indian diplomats, frequently changing Military Commanders and five-yearly elected democratic governments can lead to negative fallout right from international UNSC resolution to Strategic negotiations and even tactical level border talks. A repeatedly displayed coherent messaging of 'One-India' stance with corresponding range of diplomatic manoeuvres will only deter a cunning adversary. The key CMF pillars in three stages of negotiations are illustrated below.

Stage	Pre-Negotiation	Negotiation	Post-Negotiation
Fused Actions	Common narrative – Core interests; Deny Adversary's hidden friendly traps; Identify possible additional demands; Deny ambiguity to adversary.	Common stand; Display endless patience & resilience; Avoidance of any gifts / unfavourable overtures.	One Voice; Clarity of Next course of action.
Government	Archive of previous negotiations; Identify national core interests; Publish White-paper justifying historical rights; Evolve favourable agenda.	Selection of best negotiating team; meticulous record keeping.	Multi-lingual media release for international understanding.
Military	Accurate ground survey; Profiling of Adversarial Military Commanders; Institutional archive of military negotiations; Maximise strengths for bargaining; Contingency planning for surprises.	Identify & draw out differences between opposing military & political bosses; Analyse minutest issues in Mandarin drafts	Translate the negotiation outcome to on-ground deployment without any scope for surprises.
Para-military forces	Involvement in the planning stage to highlight their patrolling problems.	One common stance with respective counterpart	Maintain strict vigil over to maintain territorial integrity
Local populace	Highlight their historical rights / grazing areas etc; establish connect with relatives across	Prevent any untoward incident	Exploit grazing areas and project revised border development requirements
Political Parties	Multi-party discussions to build common narrative; Deny adversary political manoeuvring space; Provision of experienced advice.	Display trust in the negotiators	Healthy & constructive parliamentary discussion on available courses of actions for favourable resolution

Stage	Pre-Negotiation	Negotiation	Post-Negotiation
Academia / Think Tanks / Military and government veterans	Exploit old existing interpersonal & organisational linkages; Identification of sympathetic adversarial officials from previous experiences; Provision of detailed background material.		Critically analyse the outcome to provide honest advice for the next step
Legal Experts	Provision of legal advice; Legally vet draft agenda & negotiation plan		Analyse the agreement from legal perspective
Historians	Strengthen historical claims & linkages to disputed areas		
Media	Display commonality of stance & national unity; Complete silence on negotiation plans; Present India as the aggrieved party.	Linguistic experts to translate pre-planned media releases	Multi-lingual media release world over highlighting own positives & adversarial negatives

Table 2: CMF Approach for Negotiations
(Some Ideas taken from Vijay Gokhale[3] and Rand Corporation Study[4])

Information/Cognitive. National Cognitive strength, in the Informatisation era, is the sum of civilian population's Cognitive Resilience, clarity of Government's Narrative, National Media's sincerity to National Narrative, strength of Political Parties' convergence of agendas for 'One Strong and Secured Nation', military's Information Dominance capabilities, level of cognitive amalgamation of paramilitary and civil forces for common national objective and most importantly the Cognitive Strength of Civilian and Military leaders particularly at strategic levels. This definition itself clearly brings out the requirements of the desired CMF depth in the information domain to collectively counter adversarial agenda, strengthen national Cognitive resilience, exploit our ancient cultural power and stitch together a 'BHARAT SHAKTI 2047' narrative to reinvigorate our story crafting and narration capabilities.

Figure 1: National Cognitive Strength

Cyber. The cyber domain both on civilian and military front can be divided into offensive, defensive and reconnaissance fields. While China is strengthening its Great Firewall against American offensive capabilities, it has achieved maximum CMF in the cyber offensive and reconnaissance domain. The strength of Chinese cyber warriors run into millions with hardly any differences between its fifty-cent army, cyber criminals and Militia, semi-official cyber companies, State cyber entities and firms, and PLA's cyber forces in form of Strategic Support Force (SSF) at Strategic level and Information Support Brigades at operational and tactical levels. This wide array of Chinese cyber force, also classified as multitude of Advanced Persistent Threats (APTs) by USA, have repeatedly conducted converging deep attacks on Indian critical infrastructure adversely affecting functioning of a normal Indian. The disruptive array of Chinese attacks on Indian power grids, Aerospace, and defence firms, AIIMS and other hospitals, military communications networks, internet service providers, hotels and airlines has diversified and intensified during the ongoing standoff due to lack of retaliatory measures. This relentless series of Chinese cyber-attacks has become a 'New Normal' causing grave economic losses and thereby making an

accepted fete accompli sadly. A broad array of Chinese cyber-attacks since 2009 are elucidated below in Figure 2.
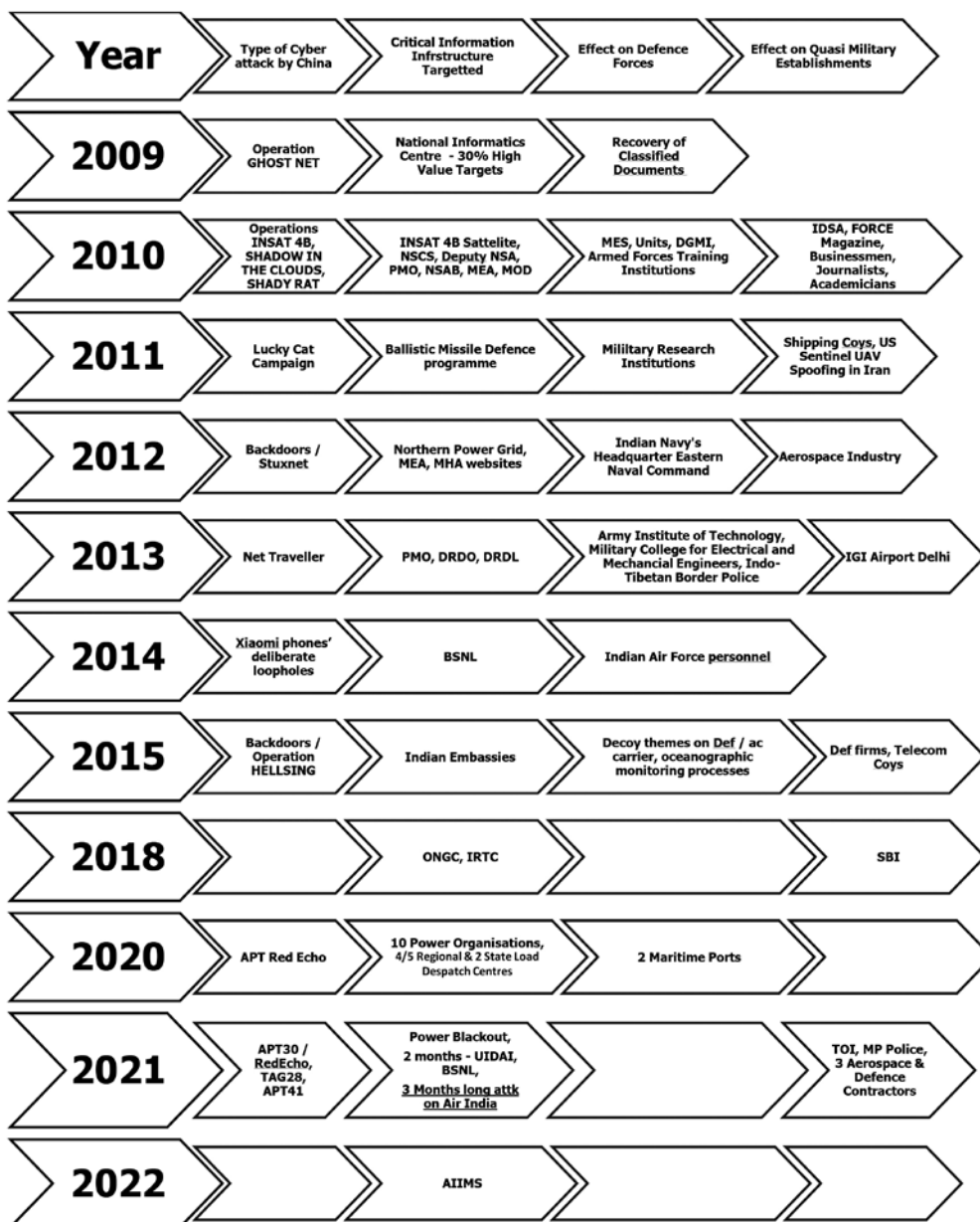
Year	Type of Cyber attack by China	Critical Information Infrstructure Targetted	Effect on Defence Forces	Effect on Quasi Military Establishments
2009	Operation GHOST NET	National Informatics Centre - 30% High Value Targets	Recovery of Classified Documents	
2010	Operations INSAT 4B, SHADOW IN THE CLOUDS, SHADY RAT	INSAT 4B Sattelite, NSCS, Deputy NSA, PMO, NSAB, MEA, MOD	MES, Units, DGMI, Armed Forces Training Institutions	IDSA, FORCE Magazine, Businessmen, Journalists, Academicians
2011	Lucky Cat Campaign	Ballistic Missile Defence programme	Mililtary Research Institutions	Shipping Coys, US Sentinel UAV Spoofing in Iran
2012	Backdoors / Stuxnet	Northern Power Grid, MEA, MHA websites	Indian Navy's Headquarter Eastern Naval Command	Aerospace Industry
2013	Net Traveller	PMO, DRDO, DRDL	Army Institute of Technology, Military College for Electrical and Mechancial Engineers, Indo-Tibetan Border Police	IGI Airport Delhi
2014	Xiaomi phones' deliberate loopholes	BSNL	Indian Air Force personnel	
2015	Backdoors / Operation HELLSING	Indian Embassies	Decoy themes on Def / ac carrier, oceanographic monitoring processes	Def firms, Telecom Coys
2018		ONGC, IRTC		SBI
2020	APT Red Echo	10 Power Organisations, 4/5 Regional & 2 State Load Despatch Centres	2 Maritime Ports	
2021	APT30 / RedEcho, TAG28, APT41	Power Blackout, 2 months - UIDAI, BSNL, 3 Months long attk on Air India		TOI, MP Police, 3 Aerospace & Defence Contractors
2022		AIIMS		

Figure 2: Array of CMF Enabled Key Chinese Cyber Attacks on India since 2009[5]

India has lost its advantage in the Information Technology, of having world's leading firms as shown in Figure 3, by not fusing cyber domain experts for protecting India's Cyber Sovereignty. A Cyber Balakot, aggressive cyber strike on adversarial weak points, optimally exploiting India's pool of cyber professionals in all domains is the essential imperative for proving our capabilities, displaying intent and significant strategic signalling. Reconnaissance of multitude of targets, infiltration into adversarial networks and execution of precise strikes with devastating effects requires Cognitive fusion and innovative integration of best cyber brains in India and abroad who can do it repeatedly with new advanced flawless techniques.
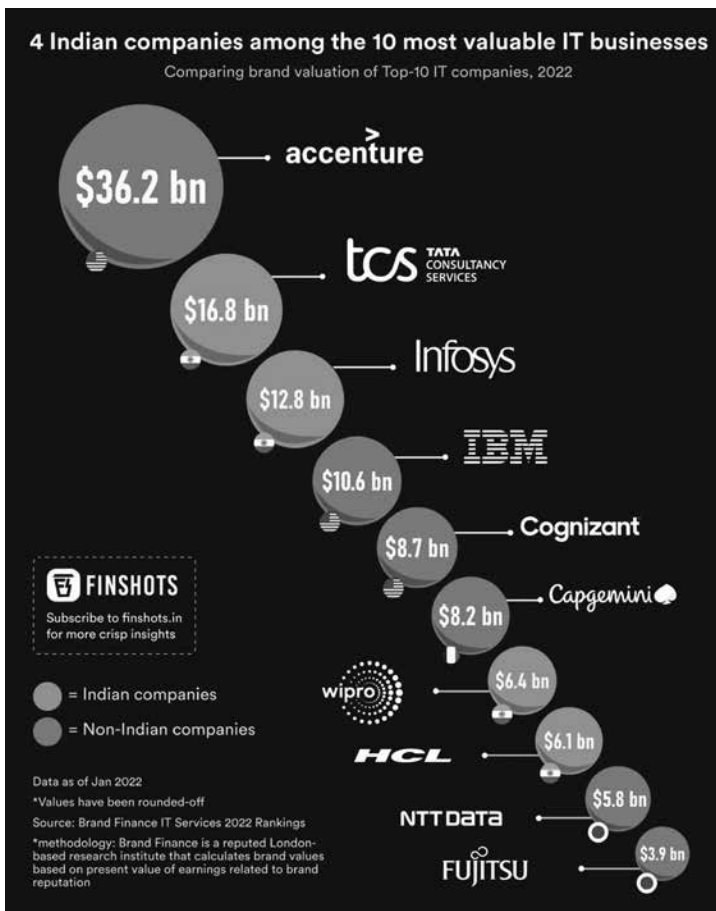

Figure 3: World's 10 Most Valuable IT Businesses [6]

The cyber-CMF approach must exploit the national patriotic fervour of every Indian Cyber expert, the Corporate Social Responsibility of leading Indian Cyber firms and evolve our own Cyber Million Talent Policy as further illustrated in Figure 4 below. Our defence forces and numerous government agencies need to integrate the multitude of compartments into a strong cyber force with punitive cyber strike capabilities.
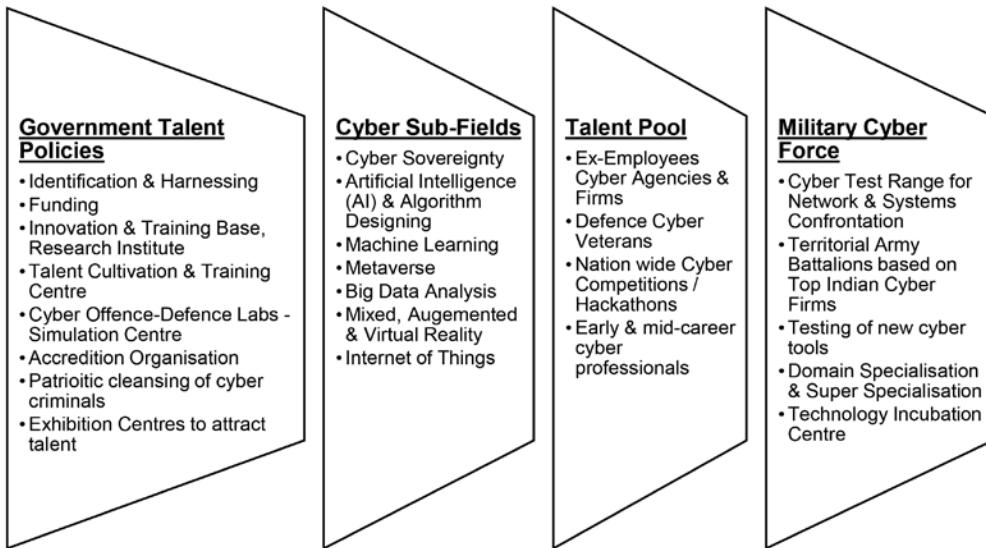
Government Talent Policies
- Identification & Harnessing
- Funding
- Innovation & Training Base, Research Institute
- Talent Cultivation & Training Centre
- Cyber Offence-Defence Labs - Simulation Centre
- Accredition Organisation
- Patrioitic cleansing of cyber criminals
- Exhibition Centres to attract talent

Cyber Sub-Fields
- Cyber Sovereignty
- Artificial Intelligence (AI) & Algorithm Designing
- Machine Learning
- Metaverse
- Big Data Analysis
- Mixed, Augemented & Virtual Reality
- Internet of Things

Talent Pool
- Ex-Employees Cyber Agencies & Firms
- Defence Cyber Veterans
- Nation wide Cyber Competitions / Hackathons
- Early & mid-career cyber professionals

Military Cyber Force
- Cyber Test Range for Network & Systems Confrontation
- Territorial Army Battalions based on Top Indian Cyber Firms
- Testing of new cyber tools
- Domain Specialisation & Super Specialisation
- Technology Incubation Centre

Figure 4: National 'Cyber Million' Talent Programme

Military. The biggest limitation of Indian conventional military Deterrence is the lack of jointness. It may be surprising but CMF is essential in the military domain too and most importantly to enforce jointness not only inter-service but intra-service and inter-ministry to ensure coherence of military aim of defeating enemy by combat power optimization amongst all uniformed forces. The increased budget allocation, clear national security policy, integrated public and private defence industry development are all essentials but joint doctrine and force structuring are the key requirements for projecting true Indian military capability with no budgetary requirements and actual manpower savings if planned correctly. The combat potential of largest numbers and most lethal

types too also does not translate into actual combat power if they are not stitched together as one cohesive force. The Chinese have learnt their lessons and undertaken suitable reforms of all their military, para-military, militia, and internal security forces to be placed under one joint integrated structure as shown below.
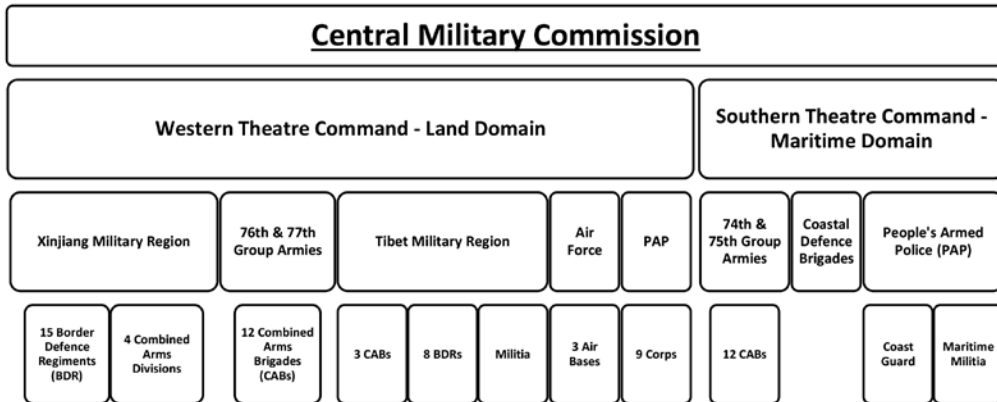

Figure 5: Chinese Integrated Theatre Structures – Land & Maritime Domains [7]

Similarly, India also needs to fuse its compartmentalised force structures under envisaged Theatre Commands, cutting across different ministries, for enhancing conventional deterrence on borders as elucidated below.
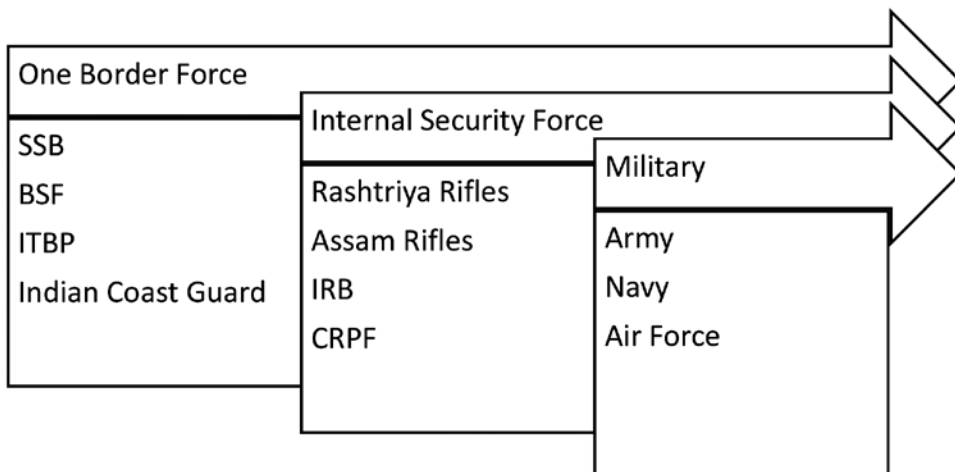
Figure 6: Fusion of Ministries for National Security under Theatre Command

The compartmentalized combat application of Russian defence forces has dented its conventional Deterrence drastically against a much weaker nearly one-tenth size Ukrainian defence force. The differences in response of Ukrainian and Russian civilian populace have manifested in a much larger Russian military struggling against nearly one-tenth size Ukrainian military. In the Indian context, the reactivation of Village Defence Committees in Jammu in 2022 is an example of CMF at tactical level. The latest Agniveer policy will eventually lead to a large quantum of military trained civilians who can be recalled anytime later. The essential CMF enabled imperatives for ensuring integration for combined arms warfare and jointness amongst services to ensure strengthened military capabilities are elaborated below.

Parameter	Civil Role	Military Responsibilities
Joint Vision & Systems Interoperability	Government – 'BHARAT SAINYA SHAKTI' Vision for 2047, Drafting National Security Strategy & Interoperability Standards for 'ATMANIRBHAR BHARAT' Indenisation; Defence Industry – Defence Visions – 2029, 2039 & 2047; Ensure system interoperability from design conceptualisation itself	Joint Capability Development Vision Documents – 2029, 2039 & 2047; Interoperability of Doctrine, Intelligence, Training, Networks, Communication, Policies, Protocols, Logistics etc.
Joint Training	Academia / Think Tanks / Veterans – Evolve a joint training curriculum	Joint Training Nodes by Lead Service / Arm with subject proficiency
Planning for Multi-Domain Intelligentised Precision Warfare	Government – Robot & Autonomous Systems Development Vision; AI industry and Veterans – Crafting of software for Joint Intelligence Preparation of Multi-Domain Battle-space (JIPMB); Quantum enabled C5I2SR (Command, Control, Communications, Computers,.	JIPMB doctrine & products – Theatre / Joint Commander's Priority Intelligence Requirement, Joint Targeting Lists, Sensor-Target-Weapon matched tasking orders, Joint Operations Order / Instructions with Contingency Plans, Multi-Domain Battle-space deployment,

Parameter	Civil Role	Military Responsibilities
	Cyber, Interoperability, Intelligence, Surveillance & Reconnaissance); Informatised & Intelligentised equipment development	and camouflage instructions
Multi-Domain Resilience for Long Attrition Wars	Think-Tanks / Veterans – Vulnerability analysis studies; Defence Industry – Development of Resilience tool-kits & Enhancing of Manufacturing Capacities	Integrated Air-Missile-Drone-Weapons Defence Umbrella; Electromagnetic cum cyber cum cognitive Resilience; Coherent & Automated physical security
Infrastructure Development	Government – 'GATISHAKTI' & Vibrant Villages Programme; Multi-purpose infrastructure development	Projection of Joint Infrastructure requirements; Asset Sharing protocols
Common Command for Border Management Posture	Government – Amalgamation of forces under different ministries under one ministry preferably Ministry of Defence for command & control for border management posture	Revised command & control, & strengthening of Border Security Force (BSF), Seema Suraksha Bal (SSB), Indo-Tibetan Border Police (ITBP) & Indian Coast Guard (ICG) etc

Table 3: CMF Enabled Integration for Combined Arms Warfare and Jointness

Space. Space Sovereignty is the new frontier for race from outer space resources to orbital spots, from Space Situational Awareness to orbital manoeuvrability and from spatial nomenclature to temporal firsts for national pride and most importantly Space based data independence. Thus, the space domain-based capability development, infrastructure resilience, resources exploitation and assured support requires effective Space Deterrence. This further necessitates close CMF encompassing clear government vision including policy and financial support; adequate R&D depth by both public and private institutions; energized, relentless and patriotic pursuit by Indian Civil industry; scalable military force structuring; generation of nationalist fervour particularly by media; and most importantly best talent provision and development. The dual-purpose requirements are plenty but are surely achievable- own

navigation system; assured satellite communication; redundant Space Situational awareness; multi-spectral accurate remote sensing with less than hour revisit; interplanetary resources exploration and offensive capabilities just to list a few.
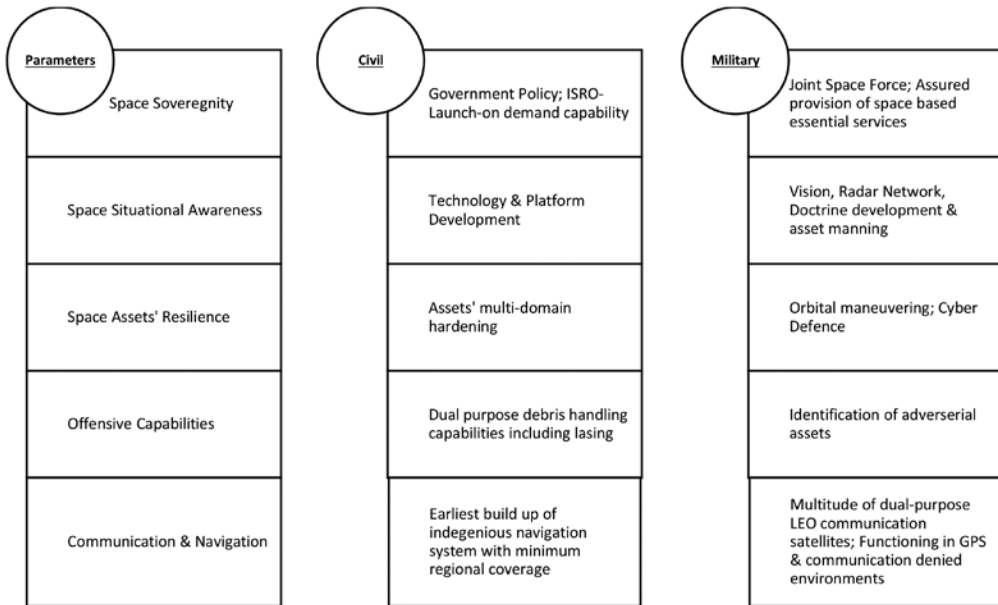

Figure 7: CMF Pillars for Space Deterrence

Technology. China has focused its CMF completely to develop technology as the core combat capability, talent as the most important strategic resource and innovation as the core concept. Despite American denial for decades, they accept that they have been outsmarted by the Chinese in many technological fields and sub-sets of Quantum, AI, Data analysis, unmanned platforms, Space, Cyber, and Robotics. The Chinese inferiority in most technologies is being overcome by quantity through massive production capacities. The biggest reality is that "Technology Indigenisation and Techno-nationalism" through CMF is the only solution available to India to transform from technology deprivation to the technologically self-reliant "Atmarnirbharat" thereby strengthening our technological deterrence. India, through CMF, needs to dominate the non-contact non-kinetic grey zone being dominated by Chinese disruptive technologies.

This requires best military brains to sit with our best scientists, wildest engineers, brightest civil academia, innovative defence start-ups, leading entrepreneurs and bureaucrats to crystal graze the future and clearly enunciate a dual-purpose technology development plan with achievable timelines. The most essential domain for CMF must cater for skipping few steps in between, if possible, to catch with the advanced nations. The dual-purpose nature of technology development, as explained below for few critical technologies, can facilitate advancements for both military and civil populace.
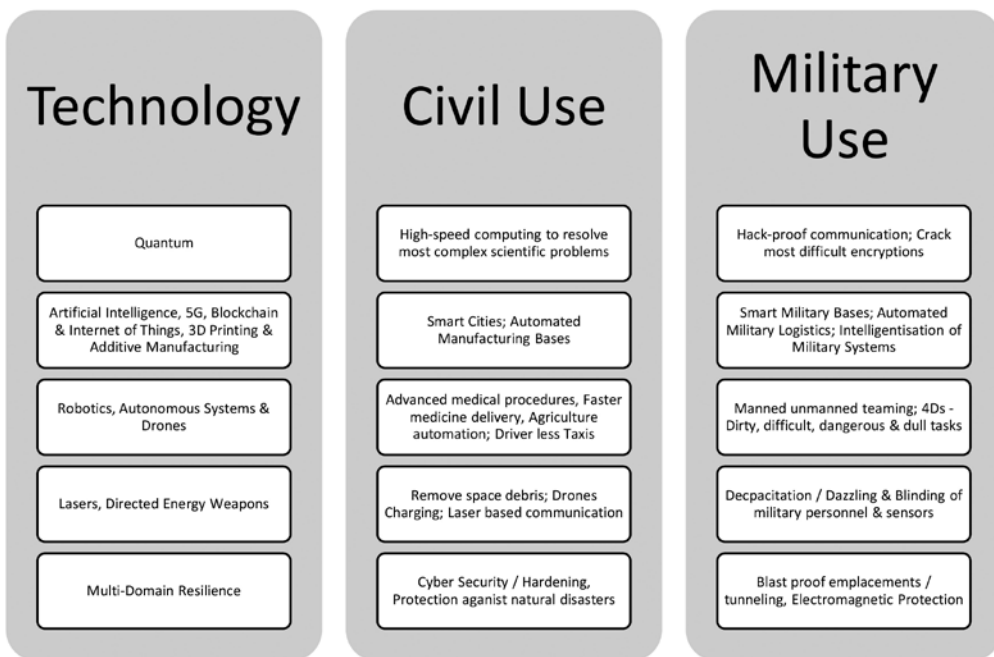
Technology	Civil Use	Military Use
Quantum	High-speed computing to resolve most complex scientific problems	Hack-proof communication; Crack most difficult encryptions
Artificial Intelligence, 5G, Blockchain & Internet of Things, 3D Printing & Additive Manufacturing	Smart Cities; Automated Manufacturing Bases	Smart Military Bases; Automated Military Logistics; Intelligentisation of Military Systems
Robotics, Autonomous Systems & Drones	Advanced medical procedures, Faster medicine delivery, Agriculture automation; Driver less Taxis	Manned unmanned teaming; 4Ds - Dirty, difficult, dangerous & dull tasks
Lasers, Directed Energy Weapons	Remove space debris; Drones Charging; Laser based communication	Decpacitation / Dazzling & Blinding of military personnel & sensors
Multi-Domain Resilience	Cyber Security / Hardening, Protection against natural disasters	Blast proof emplacements / tunneling, Electromagnetic Protection

Figure 8: Dual-Purpose Advantages of Essential Futuristic Technologies

Economic. Any nation can deter adversary only if economic threat seems achievable or sanctions initiated are comprehensively implemented. Ideal example is the current Sino-Indian standoff. Despite Indian government banning multitude of Chinese apps and diplomatic concerns of border resolution first, Indian imports from China and apropos trade deficit was the highest ever in 2022. This clearly shows lack of coherence between national security objectives and civilian economic trade requirements. Hence, CMF in economic domain

needs maximum strengthening and convergence of national security objectives for viable ISD. Every common Indian needs to be explained his power, role, and responsibilities for economic Deterrence.
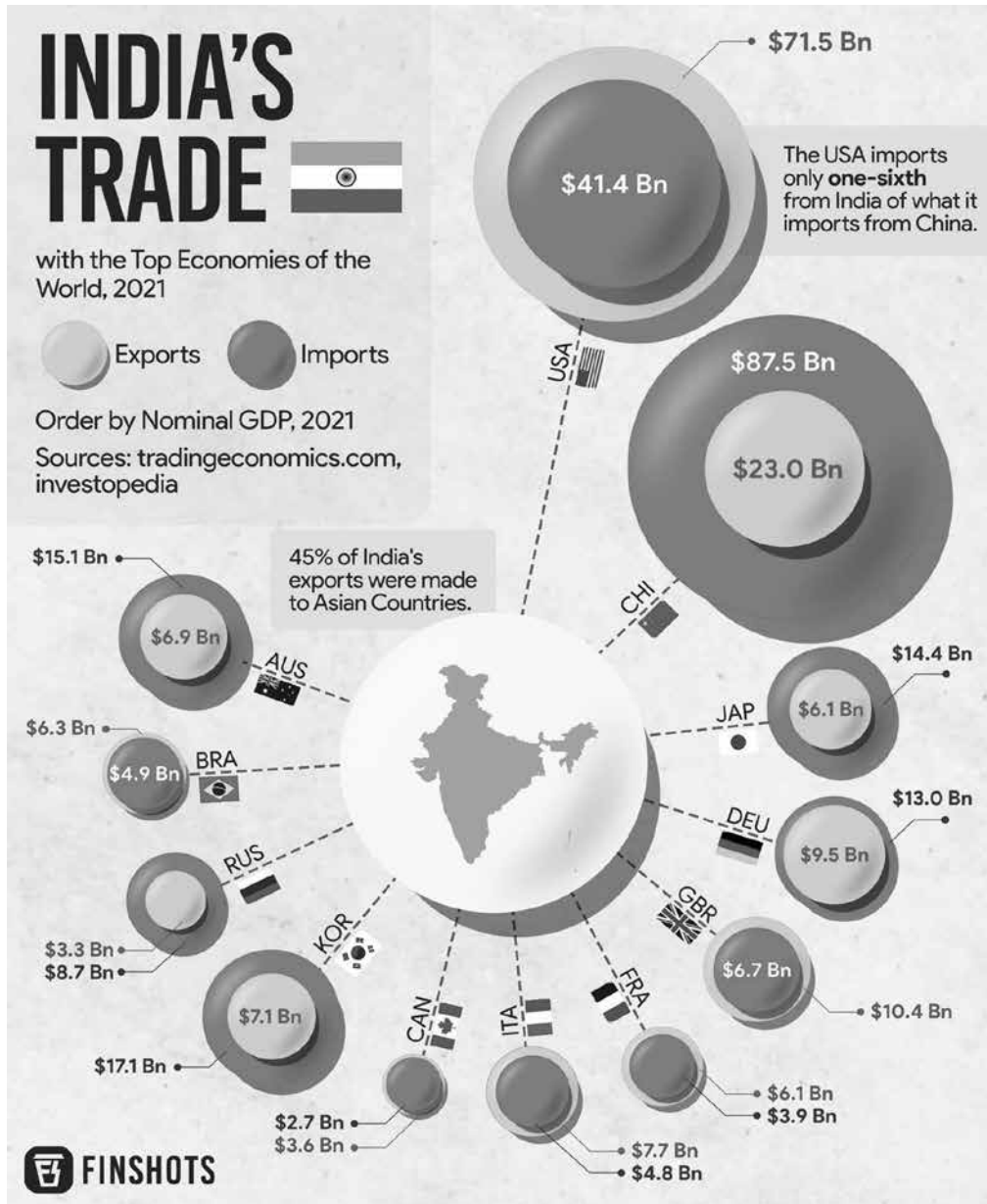

Figure 9: India's Increasing Trade Deficit with China [8]
(Source – Twitter Handle @finshots)

Intelligence Surveillance and Reconnaissance (ISR)

A functional multi-domain and multi-discipline ISR setup is the foremost step to ensure ISD. It is only a time critical common enemy picture across all levels which can facilitate timely response to deter the enemy from misadventures or prevent own strategic blunders. While timely identification of Chinese movements opposite Yangtse ensured pro-active stern response disrupting Chinese tactical ambition, ineffective ISR in 1999 led to a long drawn and extremely difficult but doggedly determined series of battles by Indian Army to dislodge Pakistan Army soldiers from Kargil heights.

Domains

☐ Space, Near-Space, Air

☐ Electromagnetic (EM)

☐ Information, Internet

☐ Cyber, Metaverse

☐ Cognitive

Discipline

☐ GEOINT / IMINT

☐ SIGINT - COMINT & ELINT

☐ OSINT - OSMINT

☐ CYBINT

☐ HUMINT
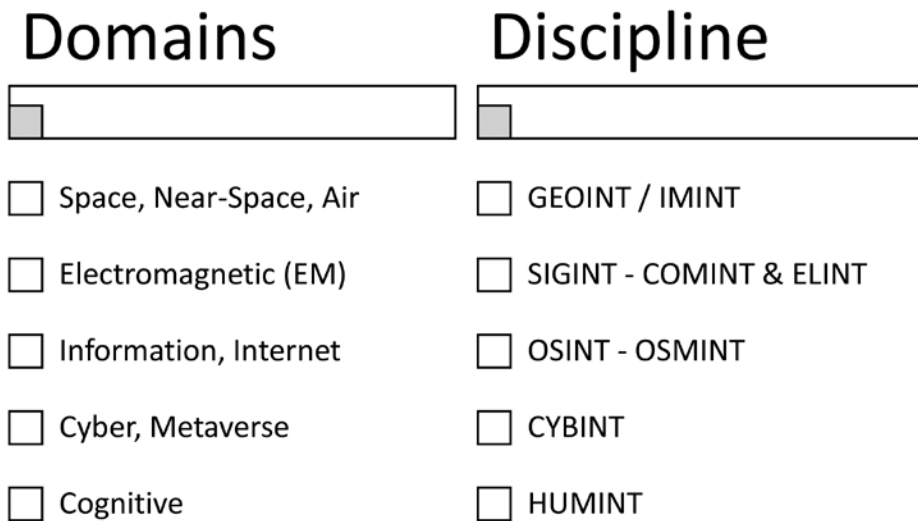
Figure 10: Multi-Domain Intelligence and Multi-Discipline Joint ISR Setup

As pointed out earlier, a coherent CMF enabled ISR setup can meet the complex requirements in the modern battlespace. While our neighbours are looking for territorial grab and destabilizing us regularly, our nation has also to look internally at many anti-national forces which are strengthened by external support. A long length of disputed borders, vast coastline with increasing adversarial activities, burgeoning social media, infosphere, cyber and cognitive domains of second most populated nation, increasingly shrinking and congested outer space and strongly

contested electromagnetic domain requires persistent multi-tiered ISR setup to safe guard our sovereign interests from any surprises. Hence, the key intelligence disciplines best exploited through CMF are discussed below.

OSINT/ OSMINT. The Armenian and Ukrainian wars and the longest ongoing Sino-Indian standoff highlighted the importance of Open-Source Intelligence (OSINT) or Open-Source Social Media Intelligence (OSMINT), particularly the role of Civilian Geospatial analysts, defence scholars and a large quantity of veteran imagery analysts. It became difficult for governments to hide anything since the OSINT community unearthed most military movements and infrastructure developments. As per varying estimates, 463 exabytes of data is likely to be generated daily by 2025. There are already approximately 6.6 billion mobile users, more than 5 billion internet users, and more than 5,500 active satellites in orbit in the world today.[9] There is thus a need for National and Theatre oriented OSINT cells, as proposed below.

National OSINT Cell - Under DIA, HQ IDS	Theatre Specfic OSINT Cells - Under Proposed Theatre Commands
• Financial Representatives - RBI, Leading Banks, Finance & Commerce Ministries, FICCI • Representatives of Leading Geospatial & Cyber firms • Defence correspondents of Selected media outlets • Reprsentatives of selected Think-Tanks • Retired Inelligence Agencies' officers & Defence veteran OSINT / IMINT experts on re-emplyment • Para-miltary & tri-service representatives	• State Police representatives • Regional media representatives with linguistic proficiency • Representatives from State Intelligence agencies • Local cyber firms / representatives of defence start-ups

Figure 11: Composition of Proposed OSINT Cells

When you combine the OSINT data available today with the data from military surveillance and reconnaissance platforms, the ISR analysts will be swimming in data. Hence, there is a need for a CMF enabled national

OSINT organization which should facilitate cueing of other intelligence discipline as well as play a key role in collaboration, collation, and easy archive.
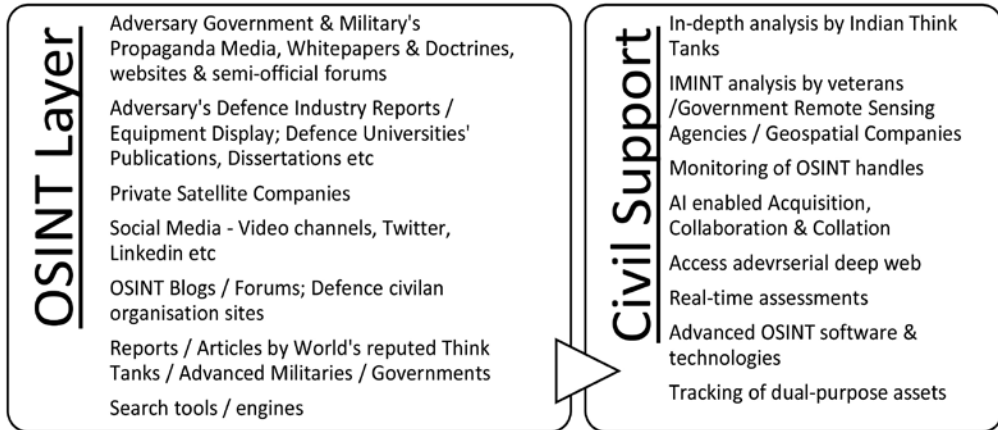

Figure 12: OSINT Layers – Civil Support for Military

IMINT/ GEOINT. Geospatial Intelligence, with Imagery Intelligence as its subset, is an intelligence field which requires domain expertise with a balanced combination of area expertise, continuous update of available Geospatial technologies, amenability to AI enablement and an in-depth knowledge of enemy ORBAT, bases, weapons, and equipment. When you add the quantum of drones (with minimum density of two per company), ISR aircrafts, electro-optical cameras, the translation of images into actionable data during hot wars is a mammoth task even with most advanced levels of Intelligentisation and automation. Hence, every IMINT expert matters whether in a natural disaster management or war fighting or grey zone management.

Today, every State has a Remote Sensing department, Drones' establishment involved with mapping, agricultural planners and many such IMINT experts. Indian defence forces have a large quantum of IMINT qualified people who have either retired or are on deputation. The expertise of every IMINT specialist needs to be harnessed through aggregation of IMINT efforts, cooperation, and coordination amongst all agencies during wars and disasters as well as in peace time. Additionally, a lot of foreign talent as well as software are available for exploitation.
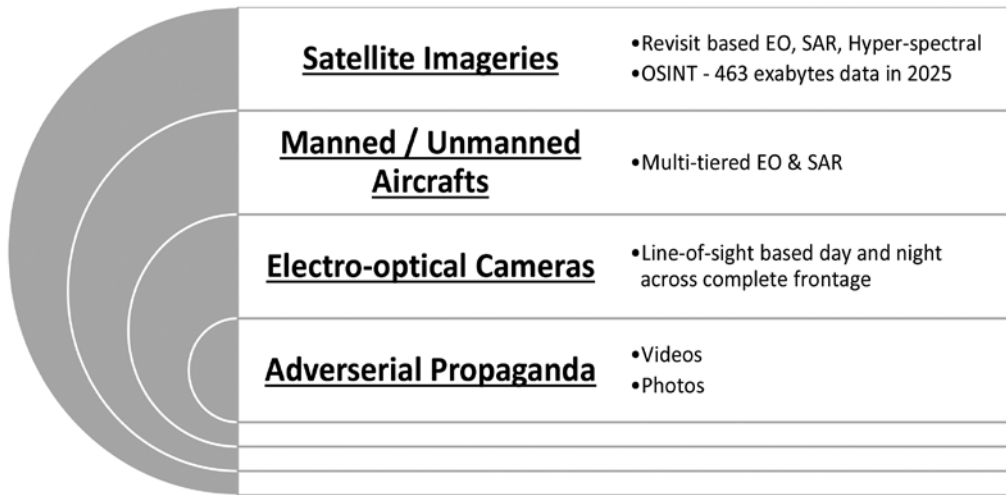
Satellite Imageries	• Revisit based EO, SAR, Hyper-spectral • OSINT - 463 exabytes data in 2025
Manned / Unmanned Aircrafts	• Multi-tiered EO & SAR
Electro-optical Cameras	• Line-of-sight based day and night across complete frontage
Adverserial Propaganda	• Videos • Photos

Figure 13: IMINT QUANTUM

CYBINT. Cyber Intelligence is in no way the responsibility of Indian military and government alone. Every Indian is a daily target of millions of Chinese cyber warriors, as elucidated in Figure below, guided by its SSF which itself is the most apt example of Chinese CMF. An Indian 'whole of Nation' cyber structure must comprise the CEOs and technological heads of leading cyber firms, Director Generals of Government and Military Cyber Agencies, heads of National Critical Information Infrastructure Agencies and Civilian Aerospace and defence firms and prominent ethical hackers to chalk out the contours of "Bharat Cyber Kavach 2024" facilitating Indian Cyber Sovereignty with persistent Cyber reconnaissance capabilities over adversaries' networks and cyber offensive architecture. The Indian CYBINT architecture will require to spread across and map multiple tiers of adversarial cyber organizations-government, military, quasi government, provincial, Militia, private companies, criminal networks etc. Hence, an effective Cyber ISR organization will require a coherent fusion of best brains within civil, government and military cyber setups.

Figure 14: Extent of Chinese 'Whole of Nation' Approach Enabled Cyber Warriors [10]

SIGINT. Signal Intelligence comprises Communication (COMINT) and Electronic Intelligence (ELINT). Although primarily military oriented, it still has a lot of Civilian participation in both acquiring as well as denying SIGINT to our enemy. While the mobile companies particularly in border areas can facilitate dual-purpose communication surveillance to provide COMINT, a large quantum of civilian satellite and aircrafts must facilitate critical ELINT collection.

HUMINT. In a longish grey zone scenario along borders and even during peacetime, border civilians play one of the most important roles in picking up early indicators of enemy movement. On our western front history, it's mostly own patriotic civilians which have given us information of Pakistan's repeated attempts to infiltrate large groups of terrorists and army personnel to disrupt peace in our valley. Although HUMINT requires expertise and military or intelligence training, the greater number of patriotic eyes and ears on ground are the only solution to persistent HUMINT cover. Since, HUMINT generally forms the basis of most corroborated intelligence, an enmeshed civil-military HUMINT grid across all levels, as elaborated below, is the necessity of truly fused ISR grid to stitch an accurate and common intelligence picture.

Agencies	Integration Parameters	Integration Tiers	
		Civil Levels	**Military Tiers**
RAW, CBI	Sources' Archive, Tasking – Areas of Interest	National	DIA / IDS – MI / IFSU, NI & AFI
State Police, CRPF, ICG	Multi-source data corroboration; Common Intelligence Picture	Regional – North East; Northern; Western; Southern; Central etc	Theatre Commands (Intelligence Battalions)
BSF, SSB, AR, RR, ITBP	Communication protocols;	State	Corps - Special Forces & Intelligence Battalions
Civil Administration		District	Divisions / Brigades
		Tehsil	Battalions

Figure 15: Joint Multi-Tiered HUMINT Grid

Veterans' Community.   India, today has a very large veterans' population which has the unique combination of combat skills and technological expertise. Many of these veterans have developed super-specialisation in their respective domains while many of the other ranks retire at a very early age and can provide the desired longevity in certain critical fields. Talent today has been recognised as a strategic resource by most advanced countries. Indian military cannot afford to waste its specialist talent because of age, supersession at younger service, or lack of career progression avenues. Hence, there is a need of 'Talent Accreditation' policies which grade the talent levels of serving personnel and veterans in their specialisation domains and then find suitable means for their absorption within the military despite retirement or supersession, deputation to government agencies or civilian industry operating in those critical domains.

Conclusion

India today stands tall and strategically autonomous in a multi-polar world. However, the national progression aspirations and security requirements are unique to every nation's neighbourhood and internal conditions. Having gone through centuries of Western looting, India unfortunately today has a great super power with second largest economy and military to its North which wants to lead the world and a seemingly failing Army to its West which still wants to bleed us through thousand cuts. When two such resource and power-hungry entities - a Party and an Army run nations and collaborate to craft a common enemy with the aim to grab our natural resources and territory while questioning the strength of our civilization, it becomes utmost essential for every Indian national and organization to fuse their efforts together for one common objective 'One-India' or 'ATMARNIBHAR-BHARAT'.

The unique Indian civil military fusion approach thus needs to coherently integrate the existing independent architectures to maximize our strengths across all domains- Diplomatic, Information, Military, Economic, Space, Cyber, Electromagnetic, Land, Sea, and Air. Our rich culture and history are replete with examples to prove that 'Nothing is impossible' and no gap unsurmountable. When every fertile Indian brain, whether civilian or military, is cognitively joined for a common national cause, no enemy can hide from us neither can any adversary deter, compel, or coerce us. A resilient multi-domain ISR structure and an Integrated Strategic Deterrence CMF architecture are thus a must for a strong and prosperous Indian nation in its march towards 'BHARAT SHAKTI 2047'.

*Brig Anshuman Narang is a keen scholar of developments in China and comprehensively researches Chinese strategic issues, military doctrinal and technological evolution. He has the unique distinction of having undertaken defence studies in reputed military institutions of all Quad countries -Japan, USA, Australia, and India. He graduated from the National Institute of Defence Studies, Japan in 2018. He is an expert on 'Intelligence, Surveillance and Reconnaissance' and OSINT and is currently pursuing PhD from CLAWS-MAHE joint doctorate

program. He has authored three books and is now working on his fourth book 'State of War with Chinese Characteristics – New Normal for India'. He is currently commanding a prestigious Artillery Brigade in Eastern theatre and has been an instructor in School of Artillery and Senior Command Wing, Army War College.

Endnotes

1   PRC's National Key Discipline Theory Works of National Defence University, 'The Science of Military Strategy (Revised in 2020)', translated in to English by USA's China Aerospace Studies Institute, January 2022, available at https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy/, accessed on 26 January 2022.

2   PRC's National Key Discipline Theory Works of National Defence University, 'The Science of Military Strategy (Revised in 2020)', translated in to English by USA's China Aerospace Studies Institute, January 2022, available at https://www.airuniversity.af.edu/CASI/Display/Article/2913216/in-their-own-words-2020-science-of-military-strategy/, accessed on 26 January 2022.

3   Vijay Gokhale, 'The Long Game-How the Chinese Negotiate with India', November 2022, ISBN: 9780143459293.

4   Richard H Solomon, Rand Corporation Study, 'Chinese Political Negotiating Behaviour, 1967-1984', available at https://www.rand.org/pubs/monograph_reports/MR663.html, accessed on 12 August 2022.

5   Saikiran Kannan and Abhishek Bhalla, India Today, 'Inside China's cyber war room: How PLA is plotting global attacks', 06 August 2020, available at https://www.indiatoday.in/amp/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06?__twitter_impression=true, accessed on 11 September 2021; Recorder Future, Insikt Group, 'China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tension', CTA-CN-2021-0228, 'Threat Activity Group RedFoxtrot Linked to China's PLA Unit 69010; Targets Bordering Asian Countries' dated 16 June 2021 and 'China-Linked Group TAG-28 Targets India's "The Times Group" and UIDAI (Aadhaar) Government Agency With Winnti Malware' dated 21 September 2021, available at http://www.recordedfuture.com/, accessed on 01 January 2022; Traffic Light Protocol White Joint Cybersecurity Advisory, 'Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department', 19 July 2021, available at https://www.cisa.gov/tlp, accessed on 21 November 2021.

6   FINSHOTS, Infographic, 'Top IT companies in the world, 2021', 28 February 2022, available at https://finshots.in/infographic/top-it-companies-in-the-world-2021/, accessed on 13 March 2022.

7   Minpao.com, 'Xinjiang and Tibet hide the two big armies that are powerful than the enemy'; Takungpao.com, 'The key to the victory of the new type of combat power/reconnaissance sergeant "Golden Falcon"; Sina.com, 'Combined Arms Reforms: large-scale replacement of the PLA's Sino-Indian border mechanized forces'; Zhuanlan.zhihu.com, 'Differences between Western Theatre Command, Lanzhou and Chengdu Military Regions'; Alexander Anatolyevich

Khramchikhin, Russian Institute for Political and Military Analysis, 'New Great Wall of China (Новая Великая китайская стена)', available at https://nvo.ng.ru/forces/2017-10-20/1_970_china.html, 20 October 2017, accessed on 07 August 2021; 'Chinese Distribution of tanks with Combined Arms Brigades'; Anshuman Narang, 'China's Strategic Deterrence'; IISS, 'The Military Balance 2021', Pp 250-258.

8   Twitter Handle @finshots, available at https://twitter.com/finshots/status/1583424810490597380, accessed on 26 December 2022.

9   Rodney Faraon and Peter Mattis, The Hill, 'We need an open source intelligence centre', 20 January 2023, available at https://thehill.com/opinion/national-security/3821075-we-need-an-open-source-intelligence-center/?s=03, accessed on 21 January 2023.

10   National Institute for Defence Studies (NIDS) China Security Report 2021: 'China's Military Strategy in the New Era', Japan MOD, November 2020, available at http://www.nids,mod,go.jp, accessed on 01 January 2022; Recorded Future, Insikt Group, 'Inside China's National Defence Mobilization Reform: Capacity Surveys, Mobilization Resources, and "New-Type" Militias', 10 March 2022, available at https://go.recordedfuture.com/hubfs/reports/ta-2022-0310.pdf, accessed on 12 March 2022.