SYNERGY

JOURNAL OF THE
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS
(Established : 2007)
Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road,
New Delhi - 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

Synergy is a bi-annual Journal that is published in Feb & Aug every year. It is supplied to the members of CENJOWS. Articles, abridged version of Research Papers and Dissertations may be sent to the Secretary CENJOWS as per the guidelines contained in the Journal. Advertisement enquiries concerning space and charges may also be sent to the Secretary CENJOWS.

The Centre for Joint Warfare Studies (CENJOWS) is an independent, professional research institute established in 2007, in pursuit of strengthening the concept of 'jointness' within the defence force, as well as with other agencies that jointly contribute towards a nation's war fighting capability. SYNERGY is the CENJOWS Journal that strives to expand and deepen the understanding of issues concerning defence, national security and civil-military interface which are so very essential for joint war fighting.

Price : Rs. 350/- INR or US 12$

TOWARDS FUTURE READY INDIAN ARMED FORCES

INDEX

TOWARDS FUTURE READY INDIAN ARMED FORCES

MESSAGE

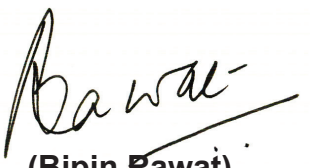
A nation maintains its Defence Services for deterrence and if compelled, to fight and win wars. Indian armed forces always remain prepared for full spectrum challenges and conflicts. Ever evolving challenges, especially those thrown up by emerging disruptive technologies, are adding new dimensions to future conflicts, as was witnessed in recent conflicts in Crimea, Syria, Afghanistan, Iraq and Ngorno-Karabakh. Our Defence Services have demonstrated their unmatched potential and capabilities on several occasions.

However, a critical relook and reappraisal of our strategies, roles, mission and tasks of the armed forces is necessary for ensuring jointness, integration and preparedness for future challenges. Gaps in capabilities need to be identified and innovative mitigation measures adopted. The instrument of military power, in all domains, need to be honed up. Atamanirbharta, ranging from research and development to manufacturing and sustenance need to be pursued in a mission mode.

The August 2021 issue of the Synergy Journal of the Centre for Joint Warfare Studies has endeavoured to bring forth important issues

needed to be addressed for ensuring that our Defence Services remain future ready to meet all security challenges. The highlighted issues need attention at all levels; headquarters to field formations. Contents of articles in the issue are sure to generate innovative ideas, to transform our military into a combat effective force.

Jai Hind !



(Bipin Rawat)
General
Chief of Defence Staff

Vice Admiral Atul Kumar Jain
PVSM, AVSM, VSM
Chief of Integrated Defence Staff to the
Chairman, Chiefs of Staff Committee
& Chairman CENJOWS

FOREWORD

The necessity to enhance Combat Capability within the boundaries of affordable budget support, calls for identification of innovative measures toward making our Armed Forces future ready in all aspects of warfighting across all domains. The Armed Forces' preparedness for meeting any eventuality demands matching supporting structures, modernisation, readiness and sustainability. While during peacetime, defence expenditure on training, maintenance and capability building contributes toward readiness and sustainment; however, a continued preparedness assessments need to be in place to indicate what our forces can do and not what they have.

Today, our country faces multiple threats across the spectrum of conflict. Security challenges for India span all war-fighting domains – land, maritime, air, space, cyberspace and information. Therefore, the significance of evolving joint doctrines, joint force structures, harnessing disruptive technologies and enhancing our joint sustenance to create a future-ready military with realistic capabilities need no elaboration. There is an urgent requirement of identifying capability gaps and putting into place an innovative roadmap for instituting mitigating measures.

Steps to provide impetus to Defence R&D, suitably complemented by private R&D needs to be outlined and promulgated. Sound preparedness calls for assured funding of these projects to bridge technology and capability gaps, ensuring early import substitution.

Towards this, CENJOWS, in their theme-based journal 'Synergy', has put together well researched articles outlining a roadmap for our armed forces to be future ready. Happy Reading!

Jai Hind!

(Atul Kumar Jain)
Vice Admiral
CISC & Chairman CENJOWS

Lt Gen Sunil Srivastava, AVSM, VSM (Retd)**
Director CENJOWS

FROM THE DIRECTOR'S DESK

This issue of 'Synergy' has chosen "Preparedness of the Indian Armed Forces for Future Conflicts" as its theme. Military Preparedness for combat rests on the pillars of force structures, modernisation, readiness and sustainability. Decision makers need to know the extent to which the preparedness of Armed Forces can underwrite National Security Objectives. Given the size, structures, training levels and technological capabilities, what can the Armed Forces achieve? Decision makers traditionally tend to conflate preparedness with readiness, and tend to evaluate readiness in terms of military resource inputs and not potential outputs. Preparedness assessments should clearly indicate what the forces can do and not what they have, be objective and verifiable, relate to likely crises and conflict scenarios, be resource informed and facilitate trade-off decisions between resources, readiness, sustainability and force structures.

Articles in this issue of 'Synergy' cover all facets of defence preparedness comprehensively. The first two articles outline the conflict scenarios and threat manifestation in multiple domains. The next two articles sketch the contours of the National & Military Security Strategies and roles & missions to leverage complementarity and jointness. The next article appraises the non-traditional challenges. Adequacy of the evolving Higher Defence Organisations and Civil-Military Fusion is appraised next.

Drawing from this context, the next few articles logically appraise the preparedness gaps in the land, maritime and Air domains, suggesting prioritized pathways. An important, but neglected challenge of outcome deficits in Joint PME is also addressed. Measures to enhance preparedness in emerging domains of Cyber, EW & IW, Space and Joint C6ISR are appraised next, together with Special Operations. The next two articles highlight the salience of disruptive technologies and collaboration in Defence R&D. Deficits in infrastructure and logistics have also been appraised holistically. The issue concludes with an appraisal of long term defence planning and outlays, and proposes strategies to underwrite the desired defence outcomes.

Preparedness gaps in National intelligence also demand a critical appraisal but were excluded from the current issue with a view to not make the volume 'heavier' than it already is! Happy Reading!

(Sunil Srivastava)
Lt Gen (Retd)
Director

EVOLVING CONFLICT DYNAMICS IN A NUCLEARISED INDIAN SUB-CONTINENT: ARE THEY DYADIC ANYMORE

Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)*

"War/confrontation is seen as an exception, an extreme and an aberration in international affairs; the paradox is that it is the invention of peace which is the artificial edifice"

"Anonymous"

Abstract

The international geo-political and security environment while integrated globally, is complex, dynamic and unstable. While the geo-political power shifts have been ongoing, the rapidity of change has accelerated ever since COVID has battered and exacerbated the unstable environment. India has been a moderate power disinclined to use force or intervene in its neighbourhood. China, in contrast, has developed a more aggressive nationalism accompanied by a penchant for coercive action against its neighbours. In the last five years, and especially post COVID under President Xi, China has moved out of its customary restraint and shown undue multi-domain belligerence and haste to challenge the US and the West, for domination of international institutions, Asia especially India, and gradually establish itself as a global power. China is unlikely to undertake a negotiated compromise with India, and will remain India's main adversary for the long term with Pakistan its 'catspaw'.

India faces the full spectrum of security threats across domains. The ongoing India-China face-off in Eastern Ladakh remains restricted within the conventional warfare domain, but it is still one between nuclear-armed states, and the threat of escalation cannot be denied. Confrontation and deterrence have got multi-dimensional to address various facets of different domains. Deterrence requires a national strategy that integrates the kinetic and non-kinetic domains. Accordingly, India must develop strategies, plans, and operations that are tailored to the perceptions, values, and interests of specific adversaries and allies. Deterrence also must be viable as a unilateral strategy. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence.

While common understanding dictates that nuclear weapons preclude a major war, however, the "stability-instability paradox," allows limited war between conventional forces. South Asia plus China is home to three NWS who have an ongoing confrontationist relationship. While India's nuclear policy has stood the test of time there is talk of an urgent review of India's nuclear policy, which may not be a bad idea for creating ambiguity. It is important for India to understand that relations are no longer simply 'dyadic'. India needs to continuously assess the trends, stay ahead of the loop to dominate the confrontation and conflicts which may emerge. For that 'New India' needs to transform to a 'Future Ready' India with matching CNP.

Prelude

Anyone observing planet Earth from outer space would certainly see a pretty vision to behold. On closer examination, they would realise that they are looking at a world in intense turbulence with man fighting with himself, nature and the universe.

The International Geo-Political and Security Environment: Complex, Integrated but Dynamic and Unstable

While the geo-political power shifts have been ongoing, the rapidity of change has accelerated ever since COVID has battered and exacerbated the unstable environment. Diminishing Comprehensive National Power (CNP) coupled with protectionism and reducing power projection capabilities of the US starting the slide to a multi-polar world; emergence of aggressive and belligerent China as a global power; resurgence of Russia under President Putin; state-controlled narratives leading to signs of ultra-nationalism; authoritarian and illiberal governments like Iran, North Korea, Iran, Syria, Turkmenistan which are not necessarily aligned with the ideology and ideals of a world order established and controlled by US and her allies; emerging powers with regional aspirations like Iran, Saudi Arabia, South Africa, Nigeria, Turkey, India; fractious Europe and the European Union (EU) confused about their role in global affairs; the rise of terrorism specially of the lone wolf kind, and religious Islamic fundamentalism with a twist of occupying territory and establishing a caliphate like the Islamic State (IS); global warming and climate change disruptors; transnational Multinational Corporations (MNCs) with their agendas, drug cartels, and international crime syndicates have changed the world scape[1].

There is renewed political, ideological, economic, and military competition due to globalisation which brought many good practices and developmental growth, but is a major driver of instability and conflict. While the threat of full-scale conventional wars has gone down, correspondingly the span of conflict, its complexity, unpredictability, lethality, accuracy, reach, and manifesting into many domains have emerged. The physical and non-physical domains including the cognitive have axiomatically expanded and contracted in space and time. There are no front, rear and flanks, and there is no place to hide. Many new types of warfare have also emerged and are emerging like hybrid, cyber, information (media and social media), psychological warfare (PSYOPS), control/domination of electromagnetic spectrum (EMS), asymmetric, digital, waged either singularly or cross domains both in peace, no war

no peace, or war! The spectre of biological warfare has raised its ugly head, which could be more devastating than even nuclear war, because they can persist, propagate and spread through a population globally, as amply demonstrated by Covid[2].

To summarise, we are in an "era of persistent, constant engagement". Nations have their national vision and aspirations and want to find their legitimate place amongst the comity of nations. India too aspires to be a regional and global balancing power. With a troubled neighbourhood, two active border disputes, constant Chinese interventions and disruptions within and in South Asia, collusivity between China and Pakistan, grappling rampant COVID, a weak economy, some internal dissensions; India has lots on its plate and needs to build up its strategic multi-domain deterrence capabilities especially nuclear.

Geo-Political and Strategic Perspective of the Sub Continent

Peaceful Non-aligned India: Time to Change. India has been a moderate power disinclined to use force or intervene in its neighbourhood. This is in line with our tolerance of neighbours, religions, and projecting civilisational influence through ideational power. China, in contrast, has developed a more aggressive nationalism accompanied by a penchant for coercive action against its neighbours. In the last five years, and especially post COVID under President Xi, China has moved out of its customary restraint and shown undue multi-domain (PDIME: political, diplomatic, informational, military, economic) belligerence and haste to challenge the US and the West, for domination of international institutions, Asia especially India, and gradually establish itself as a global power. China has also shown a tendency to use varying degrees of force against its adversaries, which are not being recounted (China seas and East Ladakh). China's proclivity for coercion reflects a deep-seated and growing insecurity within its elite and the CCP. Resolution of the boundary dispute has always been a political decision for China, and she would like to keep it fermenting and using it as a pressure point against India, and keep her contained within the strategic space of South Asia. For India, it is important not to underestimate China's

preoccupation with her vulnerability. Though China and Pakistan appear to be different, they are alike in important respects. Both are driven by a deep sense of internal fragility and ruled by elites who, lacking strong foundations, seek to build national solidarity and regime strength through adversarial relationships with other states[3]. China is thus unlikely to undertake a negotiated compromise with India except on a tactical basis. Indian foreign policy is already getting a re-set, that security stability will remain a cornerstone of the relationship, and cannot be separated from other domains especially trade. China will remain India's main adversary for the long term with Pakistan its 'catspaw'. Concurrently we need to keep a close watch of our immediate neighbourhood who are increasingly being drawn into the Chinese concentric circle. With the international pivot having indeed shifted to the Indo-Pacific, and amidst the struggle for ideological and global power dominance between China and USA (Russia pitches in to queer the pitch further), South Asia has got caught up in its vortex, and relationships can no longer be seen as dyadic specially in the security and economic sphere.

How Serious is the Threat to India? India faces the full spectrum of security threats across domains - proxy, hybrid, sub-conventional or low intensity conflict (LIC), 4/5G, conventional (localised to full), CBRN including the newer domains of space, cyber, water, resources (entire gamut), especially from collusive and collaborative partners China and Pakistan, with some other neighbouring nations joining in. The strategic collusion between China and Pakistan, has brought in a whole new equation, with much more expanded assistance in multi-domain expected from China in case of an Indo-Pak war. A worrying aspect is the increasing degree of inter-operability between China and Pakistan in soft and hard power (military and non-military) spheres which is being generated. From a policy of strategic restraint, India is beginning to propagate and practice a more aggressive strategy as is evident against both Pakistan and China. The ongoing India-China face-off in Eastern Ladakh remains restricted within the conventional warfare domain, but it is still one between nuclear-armed states, and the threat of escalation cannot be denied. In its wake,

both nations have carried out a series of missile tests: China fired ballistic missiles (air and sea launched) near the Paracel and Spratly Islands numerous times in latter half of 2020, with the additional payoff to warn the US[4], but hardly something New Delhi can ignore. Strategically few aspects are clear: threat from China is likely to persist; India needs to adopt whole of Nation security strategies, and balancing responses in a nuclear weapons environment; and Indian policymakers should be mindful of the possibilities of actual military combat, be it a limited war, or a trans-domain conflict that involves the use of advanced technologies influencing both its nuclear and conventional spheres[5]. India's military capabilities and potential especially nuclear must be visible and known to all as it's a pivotal ingredient of deterrence. All said and done, nuclear weapons remain the prima donna of deterrence.

Relevance of Deterrence

Imperative Ingredients: An analysis. The increasingly complex technological security environment, with nuclear weapons, hi-tech modern conventional weapon systems like hypersonic-weapons and low-end high impact easily available disruptive systems, which can carry out major devastation, along with the rapid mushrooming of terrorist organisations has raised questions on the current relevance, role, and impact of deterrence. Both confrontation and deterrence have themselves got multi-dimensional to address various facets of different domains.

Deterrence requires a national strategy that integrates the PDIME domains. Accordingly, India must develop strategies, plans, and operations that are tailored to the perceptions, values, and interests of specific adversaries and allies. It is enhanced through security cooperation, military integration, and interoperability with own security and intelligence agencies, allied forces, and partner nations (QUAD, BIMSTEC, BRICS). The deterrent impact of such cooperation and integration is both political and military. The political impacts are primarily derived from the effects that coalition-based responses have on adversary decision-maker's perception of India's political will: the

potentially long-lasting, harmful post-conflict political and economic effects of taking on India. Allies and partner contributions to the joint fight are significant and multi-domain, kinetic and non-kinetic. These actions contribute significantly to deterrence, force protection, and overall operational success. While military intervention of any of our strategic partners including the US is very tenuous at best, we must understand the unique potency of the US: their nuclear and armed forces contribute uniquely and fundamentally to deterrence, through their ability to threaten to impose costs and deny benefits to an adversary in an exceedingly rapid and devastating manner[6]. Deterrence also must be viable as a unilateral strategy. Our main adversaries, can and will operate with and through proxies and multiple domains, and attempt to achieve their strategic and operational goals below the threshold of armed conflict. Terrorism, proxy insurgency, information, and unconventional warfare (UC) are inherently difficult to attribute and subsequently to punish the originator, and, therefore, difficult to deter. Armed Forces do not possess the capabilities to carry out deterrence operations/deter in all domains especially non-military. Today, non-kinetic domains or instruments in particular situations can become the primary deterrent. A crucial aspect is that successful deterrence is knowledge-dependent and requires the ability to establish and secure communication access to adversaries to generate the desired decision outcomes. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence.

Human and Psychological Dimension: Increasingly Pivotal. Most defence experts and professionals acknowledge that despite the growing influence and use of niche technologies like AI, robotics and automation, machine-human interface, the human interface will remain dominant and decisive. As long as humans are responsible for waging war, warfare will remain geo-political and the province of warriors. However, recent studies and insights into the nature of human decision-making raise questions about the very logic of deterrence. Over the past 40 years, research in behavioural economics has cast great doubt on the assumption that humans will behave rationally at times of grave crisis[7].

We must always remember that even in democracies, elected leader(s) are the final decision-makers and arbiters.

Evolution of 'Integrated Strategic Deterrence'. China is gearing up to wage system of systems and 'systems warfare'[8]. They are emerging as leaders in niche and disruptive technology, space and satellite warfare, AI, cyber, big data, and Three Warfare's strategy[9]. Realising that to achieve global power status, they need to close the gap between deterrence concept and weapon and domain capabilities and capacities, a multi-dimensional set of military and non-military deterrence capabilities that combine to constitute the "integrated strategic deterrence" posture essential to achieve the "China Dream"[10] has been evolved by China. The US, Russia, and India too have realised that strategic deterrence encompasses not only the nuclear triad, but also other capabilities.

Deterrence Against China and Pakistan. Our deterrence will obviously be challenged by other affected Nations. Deterrence does not necessarily need overwhelming superiority but credible/deterrent capability. Military options/actions will always remain the final pivotal option to achieve national objectives both proactive and reactive. The Indian political and military leadership does carry out net assessment exercises regarding potential adversaries and needs to constantly review the deterrent capabilities which needs to be put in place against potential adversaries especially against a probably two and a half front threat against a collusive China-Pakistan. Security experts are talking of establishing credible deterrence and punitive deterrence against China and Pakistan respectively. For India, to list some of the main military deterrents would be a credible nuclear triad with second strike capability[11] (China has it and Pakistan claims full spectrum capability to justify their tactical nuclear weapons[12],[13]), capabilities of conventional ICBM/IRBM missile and rocket artillery, strategic lift, robust C5I2SRT (command, control, communications, computers, cyber, intelligence and information, reconnaissance and targeting), BMD (ballistic missile defence), and a robust maritime strategy to dominate IOR,

In relation to Pakistan, we face a peculiar problem of how and whom to deter! Pakistan has cleverly combined its conventional and nuclear capabilities in a way that makes it impossible for India to impose a penalty at a price that India is willing to pay. That's because Pakistan's conventional strength is sufficient to eliminate India's ability to impose significant costs with a low-intensity conventional response, and Pakistan has drawn its nuclear use red lines such that any high-intensity conventional response will lead to the risk of a nuclear war. In short, Pakistan has found a way to make the stability-instability paradox go one way. Pakistan may also use tactical nuclear weapons if presented an appropriate target contributing to the attainment of op or strategic objectives. This brings us to the strategic nuclear dilemma (faced by the major powers against each other like US, China and Russia) that India should not risk escalation for Pakistan to reach a perceived "use it or lose it" situation, especially if he perceives backing by USA. If and when India prosecutes offensive operations we must conduct a very effective Influence Operations against Pakistan and to the World too about the dangers of employing WMD, minimize vulnerabilities, and demonstrate the ability to continue operations if attacked. The option of exercising our stated nuclear policy is a constant.

Nuclear Challenges in South Asia: Dyadic Relations are no longer Pragmatic

South Asia is intertwined geo-politically with China and the USA. Every aspect of nuclearization especially between NWS therefore gets impacted accordingly (for nuclear policies and deterrence explanations see Note[14]). With Pakistan having become a client state of China, increasing collusivity between the two, overt moves to contain India within South Asia, recent manoeuvres on the LC and LAC, large physical presence of Chinese in Pakistan and PoK, coupled with China's well-publicised all round assistance in the nuclear weapons domain, India-Pakistan nuclear relations certainly cannot remain dyadic[15]. There is however, a probability of China-India nuclear relations remaining dyadic (which too is increasingly becoming multi-lateral). Numerous studies and serious

literature emanating globally including assessment of war games and global/regional simulation exercises offer very interesting conclusions and recommendations, which are highlighted below:-

- No first use (NFU), lowered nuclear thresholds, conventional and nuclear entanglement (deployment, delivery systems, ISR and communications), 'escalate to de-escalate' and 'use it to lose it' concepts, emerging technology development are all interlinked and intertwined. Precedent set by one NWS, generally USA which has started a fresh nuclear arms race which is even more dangerous as it includes the entire nuclear eco-system (launch, warheads, communications, ISR, EW) with a US $ One trillion grant.

- On China and India, there is a prevailing view among experts from both countries that they share the same stance on NFU, and that nuclear escalation between the two was not only unlikely but also unthinkable. While stabilising in the context of tensions at the China–India border, the assumption that both parties are operating from the same starting point merits greater examination—in relation not just to NFU but also to a range of nuclear postures from de-mating to targeting. Assumptions of 'postural parity' may bring stability in the short term but could contribute to misunderstanding and mis-signalling in the longer term.

- In South Asia, the confrontation between China and the West (USA and its allies), is witnessing a larger and more destabilizing role. China looks at US weapon sales to the region, the Indian–US nuclear deal, the US Indo-Pacific Strategy and the Quadrilateral Security Dialogue, from the security prism; while the US are concerned about China's conventional and nuclear weapons outreach to Pakistan, military training, and the China–Pakistan Economic Corridor (CPEC) under the Belt and Road Initiative (BRI). Experts opine that the region could break into two camps, with the

USA and India on one side and China and Pakistan on the other.

- India is concerned that the Chinese practice of deployment and command and control of conventional and nuclear platforms collectively, would impact and be adopted in Pakistan's posture and planning.

- Increasing acceptance of counter force targeting by NWS originally adopted by Russia and Pakistan, has compelled USA and China to review their posture (USA has officially announced building more low yield tactical nuclear weapons). India may be forced to review its policy too.

- NWS opt for deterrence by denial strategies by developing conventional responses besides keeping each other's cities hostage to counter-value strikes. This helps raise the nuclear threshold and provide an incentive for bargaining but has its own shortcomings due to the nature of conventional deterrence that remains contestable, especially in an asymmetric military equation, where the one with the military advantage decides to test the resolve of the other, who in turn may be forced to respond with nuclear weapons, thus, leading to a deterrence breakdown[16]. Pakistan nuclear policy follows a similar dangerous line of thought that 'if a state continues to insist that they are mainly political weapons, and not to be used, these will stop deterring the adversary. Therefore, nuclear weapons only deter by the fact that they remain useable[17].

- Emerging technologies like hypersonic weapons, AI, autonomous systems, 24X7 real time surveillance systems including satellites providing increasing transparency, shorter reaction times, will have a cascading effect which will transform South Asia's deterrence landscape and make it not only uncertain, unstable but prone to nuclear accidents with unimaginable consequences.

- Grave asymmetries in India's and Pakistan's nuclear doctrines[18], are compounded by mutual disbelief, existing and emerging military capabilities, and the prolonged absence of related dialogue mechanisms. The rest of the world is genuinely worried about a nightmarish scenario where a major terrorist attack attributed to Pakistan would raise a conventional Indian reaction. This in turn could result in Pakistan launching a low yield tactical nuclear weapon (tactical is relative as no nuclear weapon is tactical) to stall/ halt the offensive. India could respond with massive nuclear retaliation. Indian capabilities of HGVs and ASAT could create a 'use it or lose it' scenario in Pakistan whenever tensions cross a threshold. The scenario having been simulated numerous times, experts agree have a high degree of probability. Risk reduction measures urgently needs to be institutionalised.

Does India's Nuclear Policy need a Review. So far, India's nuclear policy has stood the test of time. There is talk of an urgent review of India's nuclear policy, which may not be a bad idea for creating ambiguity, and there are two different views within the strategic circle. Mr Shiv Shankar Menon ex NSA, opines that "there is nothing in the present doctrine that prevents India from responding to appreciated contingencies"[19]. The second view advocates an urgent review, due to emerging disruptive technologies, the ability of adversaries to attrite the nuclear command, control and communication (C3) systems, and even the delivery and missile systems, full transparency, and split-second reaction times which have created vulnerabilities to a nations' second-strike capabilities.

Conventional War in a Nuclear Overhang: Complex and Ambiguous

While common understanding dictates that nuclear weapons preclude a major war, however, the "stability-instability paradox," allows limited war between conventional forces[20]. The Soviet Union (USSR)-China conflict (1969), Kargil war (1999), South China Sea confrontation and East Ladakh (2020) standoff demonstrate that significant global

conventional military engagement between Nuclear Weapon States (NWS), and especially between India-Pakistan and India-China is very much possible. The imperatives of military engagement between nuclear powers are to stop short of nuclear conflict, which means, first, not crossing the conventional-nuclear divide, which is relatively clear, and second, staying on the safer side of the threshold between marginal conflict and a major war, a line which is vague at best.

Conclusion

International geo-political and security environment is undergoing rapid transformation leading to uncertainty and instability. South Asia plus China is home to three NWS who have an ongoing confrontationist relationship. When China and Pakistan gang up, interfere in India's strategic backyard, as also overtly tie down India's growth and strategic space in an already uneasy cauldron of Indo-Pacific confrontations involving global powers, we are looking at a messy, potent explosive region. It is important for India to understand that relations are no longer simply 'dyadic'. India need to continuously assess the trends, stay ahead of the loop to dominate the confrontation and conflicts which may emerge. For that 'New India' needs to transform to a 'Future Ready' India with matching CNP.

***Lt Gen PR Kumar,** PVSM, AVSM, VSM (Retd) is a former Director General of Military Operations (DGMO) of the Indian Army

(Endnotes)

1. Professional knowledge and also paraphrased from my numerous articles on International and Regional Security; Monograph on "Multi Domain Warfare in the Indian Context"; 36th USI National Security Paper 2018, (New Delhi: Vij Books India Pvt Ltd, 2018); https://usiofindia.org/publication/cs3/36th-usi-national-security-paper-2018-multi-domain-warfare-in-the-indian-context/?sf_paged=3, accessed on 16 Jan; Major General Sinha Annual Memorial Lecture, "Is the Indian Deterrence Effective Against Potential Aggressors," USI Journal, Vol CXLIX/617, July-September 2019 Issue, available at https://usiofindia.org/publication/usi-journal/is-indian-deterrence-effective-against-potential-aggressors/?sf_paged=2. Accessed on 22 Feb 21.

2. Sadanand Pandey (2019), "Are Biological Weapons More Dangerous Than Nuclear Weapons? What Is the Current State Of Biological Weapons Research?", ResearchGate, January 21, 2019. Available online at https://www.researchgate.net/post/Are_Biological_Weapons_More_Dangerous_Than_Nuclear_Weapons_What_Is_The_Current_State_Of_Biological_Weapons_Research. Accessed on June 18, 2021.

3. Rajesh Basrur, The India-China Nuclear Dynamic: India's Options, Observer Research Foundation Issue Brief No 430, December 2020, available at https://www.orfonline.org/research/india-china-nuclear-dynamic-india-options/. Accessed on May 29, 2021.

4. Ananth Krishnan, "China Fires Missiles into South China Sea,", The Hindu, August 27, 2020, available at https://www.thehindu.com/news/international/china-fires-missiles-into-south-china-sea-warning-us/article32459462.ece; Shishir Gupta, "India Test-Fires 10 Missiles in 35 Days. It is Not a Coincidence," The Hindustan Times, October 29, 2020, available at https://www.hindustantimes.com/india-news/india-races-to-upgrade-its-armoury-fires-a-missile-every-4-days/story-UB5RQaMY4zVlTlYbNFR8EL.html, November 05, 2020. Accessed May 18, 2021

5. Rajesh Basrur, The India-China Nuclear Dynamic: India's Options, Observer Research Foundation Issue Brief No 430, December 2020, available at https://www.orfonline.org/research/india-china-nuclear-dynamic-india-options/, accessed on May 29, 2021.

6. US Field Manual: Deterrence Operations Joint Operating Concept, Version 2.0, Dec 2006

7. Dr Andrew F. Krepinevich, Jr., "US-China Relations in 2019: A Year in Review," testimony before the US-China Economic and Security Review Commission, September 4, 2019, available at https://www.uscc.gov/sites/default/files/Panel%20II%20Krepinevich_Written%20Testimony.pdf. Accessed on May 17, 2021.

8. Jeffrey Engstorm, 'Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare', 2018, RAND published research, available at https://www.rand.org/pubs/research_reports/RR1708.html. Accessed on 18 Jun 21.

9. "Three Warfares" is a political and information pre-kinetic warfare strategy of the People's Liberation Army (PLA) employing media or public opinion warfare, psychological warfare, and legal warfare. Numerous publications and see China's Three Warfare's on wikepedia.org

10. Paraphrased and ideas from summary online (read -only) of RAND Paper, Michael S. Chase and Arthur Chan, "China's Approach to 'Integrated Strategic Deterrence',"

Copyright RAND Corporation 2016, available at https://www.jstor.org/stable/10.7249/j.ctt1bz3vx1. Accessed on January 14, 2021.

11. 'Modi hails 'India's successful establishment of Nuclear Triad', The Dawn, 05 Nov 2018

12. Kinza Asif, 'Pakistan completes nuclear triad', Foreign Policy News, 16 Jan 2017.

13. Hans M. Kristensen, Robert S. Norris & Julia Diamond, 'Pakistani Nuclear Forces', 2018, pgs 348-358| published online: 31 Aug 2018, 'Bulletin of the Atomic Scientists', Volume 74, 2018. Accessed on 10 May 21.

14. India's Nuc Posture. India summarized its nuclear posture in 2003 as follows:
    'I. Building and maintaining a credible minimum deterrent;
    II. A posture of "No First Use": nuclear weapons will only be used in retaliation against a nuclear attack on Indian territory or on Indian forces anywhere;
    III. Nuclear retaliation to a first strike will be massive and designed to inflict unacceptable damage;
    IV. Nuclear retaliatory attacks can only be authorised by the civilian political leadership through the Nuclear Command Authority;
    V. Non-use of nuclear weapons against non-nuclear weapon states;
    VI. However, in the event of a major attack against India, or Indian forces anywhere, by biological or chemical weapons, India will retain the option of retaliating with nuclear weapons'.

Pakistan's Nuc Posture. Pakistan has not formally declared an official nuclear use doctrine. Pakistani officials maintain that ambiguity serves Pakistan's interests better, since ambiguity does not provide information about Pakistan's nuclear thresholds that an enemy would need to exploit gaps in the plans. constantly evolving on still others. The possibility of nuclear first use and a unilateral moratorium against nuclear testing remain constant. Minimum credible deterrence and basing the nuclear posture on nondeployment and de-mated weapons are ambiguous. Pakistan's National Command Authority announced full spectrum deterrence as a part of the national nuclear policy in 2013. Full spectrum deterrence may be defined as maintaining the credibility of deterrence at strategic, operational and tactical levels, thereby covering the entire threat spectrum. Its diversification of delivery means also indicates a shift from massive retaliation to graduated response, coupled with changes in future targeting strategies. It is also expected that Pakistan might, in the near future, perceive a need to move away from the non-deployment of its weapons. Its evolving sea-based capabilities, as well as its short-range ballistic missiles (SRBMs), may also necessitate a shift from centralized to delegated command and control.

China's Nuc Posture. China summarized its nuclear posture in 2019 as follows: 'China is always committed to a nuclear policy of no first use of nuclear weapons at any time and under any circumstances, and not using or threatening to use nuclear weapons against non- nuclear-weapon states or nuclear-weapon-free zones unconditionally. China advocates the ultimate complete prohibition and thorough destruction of nuclear weapons. China does not engage in any nuclear arms race with any other country and keeps its nuclear capabilities at the minimum level required for national security. China pursues a nuclear strategy of self-defense, the goal of which is to maintain national strategic security by deterring other countries from using or threatening to use nuclear weapons against China'.

Russian Nuc Posture. Russia has described its nuclear posture as defensive as recently as 2018. This posture combines the elements of 'launch under attack' and 'launch on warning', and some experts have described it as a 'reciprocal counterstrike'. In 2020 a new document— Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence—was approved. While clarifying some aspects, the document maintains ambiguity in Russia's nuclear posture, such as with the use of nuclear weapons in response to a conventional attack.

USA Nuc Posture. The most recent document on US nuclear posture is the 2018 US Nuclear Posture Review. This calls for low-yield or tactical nuclear weapons as a flexible nuclear option. While maintaining a degree of ambiguity, it states that the USA could employ nuclear weapons to respond to 'significant non-nuclear strategic attacks', including those against 'US, allied, or partner civilian population or infrastructure', as well as 'US or allied nuclear forces, their command and control, or warning and attack assessment capabilities'.

Min Deterrence. Minimum, or minimal, deterrence is an application of deterrence theory in which a state possesses no more nuclear weapons than are necessary to deter an adversary from attacking. Pakistani experts have traditionally applied this term to describe Pakistan's application of deterrence.h

Extended Deterrence. Extended deterrence is premised on the provision of US military forces, particularly nuclear forces, to deter intimidation, coercion or attack on US allies. It is also sometimes called a 'nuclear umbrella'.

15 As opposed to this author; Dr Adil Sultan Muhammad*, India-Pakistan Crises and the Evolving Dyadic Deterrence Model, IPRI Journal, Winter 2020, available at https://ipripak.org/wp-content/uploads/2020/06/Article-2-IPRI-Journal-XX-I-Ind-Pak-Det-ED-SSA-FINAL.pdf. Accessed on 07 May 21

16 Glenn H. Snyder, Deterrence by Denial and Punishment, Research Monograph No. 1 (Princeton, New Jersey: Woodrow Wilson School of Public and International Affairs, Center of International Studies, Princeton University, 1959).

17 Michael Quinlan, Thinking about Nuclear Weapons: Principles, Problems, Prospects (New York: Oxford University Press, 2009). Accessed from College of Defence Mgt library.

18 Webinar on "Nuclear deterrence and stability in South Asia: perceptions and realities", May 20, 2021, IISS, available on https://www.iiss.org/events/2021/05/report-launch-nuclear-deterrence-south-asia

19 Stated in Shivshankar Menon, "Indian Nuclear Policy," Choices: Inside the Making of Indian Foreign Policy, (India: Penguin Books India, 2016). Accessed on 05 May 21.

20 The concept was originally developed to argue that conventional war is possible in a nuclear environment because neither side will risk escalating to the nuclear level. See Glenn H. Snyder, "The Balance of Power and the Balance of Terror," in Paul Seabury, (ed.) The Balance of Power, (San Francisco: Chandler, 1965), pp. 185-201. In practice, as argued here, the level at which armed conflict is a viable proposition is restricted to marginal war.

MULTI DOMAIN WARFARE - FUTURE CHALLENGES IN THE INDIAN CONTEXT

Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)*

"If people use information-centric bio-weapons to attack a bio-computer, should this be counted as bio-warfare or information warfare?

- Liang and Xiangsui Unrestricted Warfare,1999

Abstract

The nature of war has been and will remain an act of imposing one's' will on the adversary. However, the character of war i.e how future wars will be waged and fought has transformed due to numerous geopolitical & socio-economic factors, technological advancements and military innovations. Warfare today is a complex phenomenon likely to be waged in the multi-dimensional and multi-domain space. This complexity will increase in the future. The reasons include high technology, the nature of modern war, new threats and challenges and the reality of nuclear weapons in the arsenal of our potential adversaries.

In the last five centuries there have been 16 transitions of world power, of these only four have been non violent. 12 of the 16 transitions resulted in major wars. As the power shifts from the West to the East and China readies to challenge the US hegemony in the coming decade, despite the interdependencies, there is a considerable likelihood of a violent struggle. China is getting ready to seek a Bipolar world and the US will resist any challenge to its supremacy. As China grows in political, economic, military and technological power, it challenges the United

States for the sole superpower status. The first indicators were evident during President Xi's first visit to the United States after appointing himself as the supreme leader, wherein he asked the United States to treat China as a strategic equal. President Xi in his speech on 22 September 2015 contradicted experts who have talked about the ''Thucydides Trap" where an emerging power like China threatens an established power like the US. To quote president Xi "There is no such thing as the 'Thucydides Trap" in this world, but should major countries time and again make the mistake of strategic miscalculation, then they might create such a trap for themselves" he warned. As and when the transition of power takes place, it will directly impact India's security, as India shares a 3488 km long unsettled border with China. A responsible risen India, a regional power and a global leader, is perceived by China as a threat to the 'China Dream' and 'Dominance'. The ongoing standoff and stalemate along the Line of Actual Control (LAC) in Eastern Ladakh is indicative of China's strategic intent of containing India as she perceives that India is and can be a threat to China's ambitions and interests in challenging the US. China's 'Military Coercion' along the LAC is a manifestation of China's strategic anxiety and concern, India being the only nation which has not only not endorsed the China Dream project of BRI but in fact has openly opposed the project, as it violates India's territorial integrity and sovereignty. The emerging post Covid world order will dictate not only India's global role but also the multiple security challenges.

The nature of war has been and will remain an act of imposing one's' will on the adversary. However, the character of war i.e. how future wars will be waged and fought has transformed due to numerous geopolitical & socio-economic factors, technological advancements and military innovations. Warfare today is a complex phenomenon likely to be waged in the multi-dimensional and multi-domain space. This complexity will increase in the future. The reasons include high technology, the nature of modern war, new threats and challenges and the reality of nuclear weapons in the arsenal of our potential adversaries.

The security challenges for India can no longer be defined and definite, as these are likely to be hybrid, conducted in many battle spaces by multiple means driven by a collective ideology, plausibly

without any direct attribution and without any overt physical military application of combat power ab-initio. A collusive or collaborative threat from both China and Pakistan is a probability which India should consider seriously, especially so with China's aggressive behaviour along the LAC since May of 2020. China will exploit Pakistan as a proxy to contain India In the event of a China threat, Pakistan will only be too willing to support its all-weather friend China and a collaborative threat from Pakistan would be imminent, as it takes on a mightier India preoccupied with China along the Northern Borders. Hence, it would be prudent to conclude that during a future Indian military conflict with China, Pakistan will come to China's military aid but reverse is a high probability but not a given.

The armed forces are mandated to ensure the territorial integrity of our nation, which also implies securing our borders. India has the longest disputed land borders in the world - 3488 km of the Line of Actual Control (LAC) along the India-China border, 772.1 km of the Line of control (LC) in J&K and 126.2 km of the Actual Ground Position Line (AGPL) in Siachen Glacier in addition to a 7516 km long coastline. India's unsettled and porous borders manned by the army lie at altitudes of 4,500 meters and above with woefully inadequate infrastructure and extreme climatic conditions demanding ab initio deployment of a large number of troops. China's aggressiveness and assertiveness is increasing, both in intensity and frequency. The clash at Galwan on 15/16 June 2020 violated the hithertofore four and a half decade old 'Peace and Tranquility' along the LAC. China today is the clear and present danger. As China propagates 'Unrestricted' and 'Non-Contact Warfare', the security challenges for India have multiplied exponentially. The continuing proxy war being waged by Pakistan, the ever increasing and omnipresent threat from terrorists employing technology as enablers are the new age threats to the wellbeing of 1.39 billion Indians. Future threats emanating from Pakistan are likely to involve states or a state-sponsored actor as key tools of the 'Low Cost High Effect' proxy war. States will however continue to predominantly determine the spectrum, location and impact of threats. A conflict with nuclear overhang either with Pakistan or a limited conflict with China is a high probability in

the near to midterm. The internal political and economic instability in Pakistan, sectarianism and the rise of fundamentalist and terrorist organisations make it a major source of instability in the region given the withdrawal of US forces from Afghanistan. There also continue to remain a number of other fault lines between India & Pakistan, disputes over J&K, Siachen Glacier, Sir Creek, river water sharing and a long standing distrust of each other's intentions. Thus, making peace between India and Pakistan a rather improbable option. India's relations with China over the medium to long term will continue to be marred by disputes over the perceptions of LAC and conflicts over spheres of influence in the Indo-Pacific, which is a strategic vulnerability for China. China will also continue to oppose all Indian efforts to assert its rightful place in the comity of nations by blocking her membership of NSG, UN Security Council etc. The ongoing stalemate along the LAC is only a short term measure to contain escalation by both sides. Both India and China feel that this is not the right time and opportunity to escalate the situation on account of near combat parity along the High Himalayas. As China's strategic intent is to contain India, she will resort to 'Unrestricted and Non-Contact Warfare to tie down India and keep it away from being a dominant player in the 'Balance of Power' given the shift in the emerging global order. A limited conventional conflict of short duration can also not be ruled out, in the event both China and Pakistan see a chink in India's defence preparedness. Hence it is imperative that India and the Indian Armed Forces continue to be optimally prepared to meet and mitigate all security challenges emanating in multiple domains.

Multi Domain Warfare Challenges

2020 has been a defining year. COVID19 and an aggressive China have been the biggest disrupter of the century, impacting the behaviour of individuals, society, people and nations. As India was trying its best to battle the made in China coronavirus, providing much needed medical assistance to many a nation including the US, following Sun Tzu's dictum "In the midst of chaos, there is also an opportunity", China violated the spirit of the Five agreements which had ensured 'Peace and Tranquility" along the 3488 km India - China border for nearly four

and a half decades, resorting to its tried and tested strategy of 'Military Coercion'. Post Galwan violence in June 2020, a fragile peace has been established with the world's two largest armies locked in a standoff across the high Himalayas. The China threat is the real and present danger making the two front war a reality in the near to mid-term. China is not likely to have achieved her strategic objectives in the face of a resilient and effective Indian response based on the doctrine of 'No Blinking No Brinkmanship', with India ensuring an effective and timely equitable and proportional deployment. China's military coercion can now manifest in multiple domains based on their operational philosophy of 'Unrestricted Warfare' or multi domain warfare.

What is multi domain Warfare? Simply defined Multi-domain warfare hence implies creating an effect in one domain that produces an effect in other. Multi domain-specific capabilities can be leveraged to defeat a capable foe in another domain, or the 'force-on-force' operations would supplement the creative ways[1]. The concept of wars is growing ever more complicated, including all-pervasive information warfare, to applying multi-functional and multi-domain military capabilities below the threshold of armed conflict or the coupling of economic power with militia and irregular forces. Indeed, …the very rules of war have changed. The role of non-military means of achieving political and strategic goals has grown, and in many cases they have exceeded the power of force of weapons and their effectiveness[2]. This implies that wars in future could well remain unannounced in non-kinetic format and may even be successful in achieving political goals with or without transcending to force-on-force wars. The Key Question is how and what does multidomain warfare imply in the Indian context, given that the major threats emanate from China and Pakistan.

1 https://www.google.com/search?q=multi+domain+warfare+definition&oq=multi+domain+warfare+definition&aqs=chrome..69i57j33i22i29i30.12794j1j15&sourceid=chrome&ie=UTF-8

2 Rakesh Sharma,Multi Domain warfare - Cross Domain Deterence CLAWS , accessed athttps://www.claws.in/multi-domain-warfare-cross-domain-deterrence/#:~:text=Multi%2Ddomain%20warfare%20hence%20implies,would%20supplement%20the%20creative%2ways.

In February 1999, two Chinese Peoples Liberation Army PLA senior Air Force colonels, Qiao Liang and Wang Xiangsui, published Unrestricted Warfare. The authors argue that 'The Battlefield is Everywhere' that the combination of weapons systems can create a new kind of technical space, a new battlefield that never existed before. Electronic and information technologies have created a net space, which can become a battlefield. The battlefield extends simultaneously at the micro, medium-range and macro level as well as in various hybrid technical spaces in ways it never did before. The proliferation of weapons and technologies has blurred the distinction between the soldiers and civilians and between the battlefield and the non-battlefield. The battlefield is everywhere. From a computer room or on from the trading floor of a stock exchange a lethal attack on a foreign country can be launched. In such a world is there anywhere that is not a battlefield? Where is the battlefield? It is everywhere[3]. In the Indian context China does have the capability and capacities to wage a non-attributable war in multiple domains and dimensions, raising the costs for India and styming her growth.

The blending of technologies for war in the global era have ended the dominance of weapons in war. From this new baseline the relations of weapons to war have changed and made the concept of war itself vague. Is a hacker attack an act of war? Is using financial tools to destroy a country's economy an act of war? When we consider that any one of these non-war activities could be elements of the new kind war of the future we have to give this new kind of war that transcends boundaries and limits: "Unrestricted Warfare"[4].

"Unrestricted Warfare" means that any methods can be prepared for use, information is everywhere, the battlefield is everywhere, and that any technology might be combined with any other technology, and that the boundaries between war and non-war and between military and non-military affairs has systematically broken down[5]. Computer

3 Unrestricted Warfare Qiao Liang and Wang Xiangsui (Beijing: PLA Literature and Arts Publishing House, February 1999) pp 38 to 42.

4 Ibid

5 Ibid pp6-7

networks have greater and greater influences on world affairs. Hackers and many non-hackers wandering on the computer networks of the world act according to their own ethics they are not bound by the playing rules of society at large. They can use the web to challenge evil. One example is the eyewitness to attacks on ethnic Chinese in Indonesia by the Chinese military who broke the Suharto government's information embargo by putting a report on the web that woke up the world to these atrocities. The Indonesian military stood accused before the world. A hacker called MilwOrm as a protest against Indian atomic bomb tests broke into the India Atomic Research Center web site, changed the web page and downloaded 5 megabytes of data. A hacker might in some cases have the same impact as an atomic bomb[6].

China's Unrestricted Warfare is all encompassing as it follows Sun Tzu stratgem of 'Winning without Fighting'. China will like to avoid a direct military confrontation with India, but subjugate India by other means like targeting financial institutions, economic and commercial interests, interfering with critical infrastructure, cyber-attacks, political warfare, Water and Biological wars etc. Undoubtedly, these tactics have been accepted by the Chinese government, especially, against the US ally India. Several events in the last two years have highlighted China's attempts to ravage the world's largest democracy, these include stealth appropriation of territory, skirmishes along the Sino-Indian border, several crippling cyber-attacks, the use of unorthodox weapons, including one that caused an extensive power outage in India's financial hub Mumbai, the diversion of shared water resources, and a treacherous geostrategic alliance with India's archenemy Pakistan. China is deploying both Sun Tzu's The Art of War and the PLA officers' Unrestricted Warfare as playbooks.[7] China in a surprise move along the LAC, resorted to violence inflicting casualties on the Indian Army troops at Galwan. Indian soldiers led by Col Santosh Babu surprised the Chinese by an immediate effective and a ferocious retaliation. The retaliation ensured has ensured a fragile peace along the LAC, as thereb has been no

6 https://fas.org/nuke/guide/china/doctrine/unresw1.htm

7 https://www.newindianexpress.com/world/2021/jul/07/china-indulging-in-unrestricted-warfare-against-india-says-report-2326748.html

escalation since then as yet. In this skirmish, 20 Indian soldiers made the supreme sacrifice and 75 injured. It is also assessed that the PLA suffered over 40 fatal casualties. Several experts suggest that China used 'microwave weapons' against Indian troops that were effective up to a kilometer, cleverly dodging the "no live shot" rules of engagement. These mentioned this 'microwave technology' as something that heats up fluid under the skin, causing intense pain and vomiting and that resulted in Indian troops retreating after becoming violently ill.[8]

In American Thinker, Janet Levy also mentioned that China's attacks on all fronts are well coordinated. At the height of the border standoff, there was a 200% increase in cyber-attacks on Indian IT and banking systems over five days, with more than 40,000 attempts by Chinese hackers to install the malware in Indian networks. Chinese-sponsored groups also mounted espionage operations against India's power and transportation sector, including two ports. The grand power-cut in Mumbai in 2020 that shuttered the complete infrastructure including stopped trains, closure of the stock market, hours of power cut in hospitals amid deadly pandemic was allegedly the result of an attack by the Chinese military group RedEcho.[9]

In the Geostrategic space China's 'String of Pearls' aims to undermine India's interests and role in the region. Pakistan, China's all weather friend and partner will be more than willing to intensify the 'Proxy War' raising the costs for India and furthering its 'Kashmir Agenda'. China has cultivated politicians in the India's neighbourhood, employing her strategy of 'Debt Trap" and "Wolf Warrior Diplomacy' she aims to contain India and keep her tied down in the region.

The manifestations of these threats is likely in multiple spaces, impacting not only external and internal security, the plus two front war scenario, but all critical as also seemingly innocuous sectors to disrupt governance, administration, life and work of society and people. Exploiting new age technologies such as AI, unmanned systems / robotics, cyber, space, IoT, Block Chain etc both China and Pakistan

8 ibid
9 Ibid

employing proxies or the so called non state actors can wreak havoc in our systems. After the Jan 2016 attack on India's Pathankot airbase by Pakistan based terror group Jaish-e-Mohammad, India planned to spend approximately INR 20,000 crores on strengthening the security of air bases and other administrative bases near the IB, as also earmarked another INR 30,000 crores for constructing a smart fence along the IB to enhance counter infiltration. The recent drone attack on Jammu Airforce base is a demonstration on how vulnerable our high value assets are to low cost technologies.

In addition to a collaborative threat from the Nuclear armed neighbours China and Pakistan, India will continue to face threats from state actors involving proxies, violent non-state actors who may be sub-national or transnational in origin. These state backed terrorists would employ violent acts in conjunction with civil society, NGOs or intelligentsia supported by information warfare against the people. The widespread use of social media by a large section of the population will increasingly make it a tool to target one of the pillars of national strength i.e. the will of the people. This must be seen not only as a threat which needs better policing effort but a major internal security threat. Another major security challenge is in the cyber domain and Data security, especially so as on account of 'Supply Chain Infection' as most of the IT sector is highly dependent on China manufactured and supplied hardware. Shri G. Kishan Reddy the Minister of State in the Ministry of Home affairs while replying to a question on Cyber-attack stated that "As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 3,94,499 and 11,58,208 cyber security incidents have been observed during the years 2019 and 2020 respectively'[10], a 300 percent increase in cyber-attacks, amounting to 132 attacks every day.

Threats to national security also emanate from terrorism in the hinterland e.g., targeting of economic and population centres, Fake Indian Currency Notes (FICN) to disrupt the economy and fund illegal activities, drug trafficking etc. Besides, Piracy, the threat to Economic Zone assets and ventures, Virtual Societal Warfare that are aimed at

10 http://loksabhaph.nic.in/questions/QResult15.aspx?qref=23441&lsno=17

changing the values and behaviour pattern of society, Weaponisation of Social Media, intervention in the Education sector to degrade Indian civilization linkages, culture and beliefs[11].

Chinese strategic concerns lie in the Indian Ocean region. India a peninsular nation dominates the SLOC with the strategic located Andaman and Nicobar Islands. The IOR contains thirty-six countries in sixteen time zones, more than half the world's population, and twenty-four of the thirty-six megacities on Earth, and it covers more than half the world's surface area. It is imperative that domination of the IOR be leveraged to deter China.

The Way Ahead

India's national aim is to transform India into a 'Modern, Prosperous and Secure' Nation. Peace and security are a prerequisite for long term economic development and the wellbeing of 1.36 billion Indians. Also, economic development is a must for peace and stability. Whole of Government approach is required in a structured and cost effective organised way to meet and mitigate the multi domain threats.

India's security concerns must cater to the dichotomy in Chinese policy pronouncements, based on own core-interests. Chinese declared military strategy propagates 'Local Wars under Information Conditions' and such local wars are likely in China's neighbourhood. India should note that like the LAC, China is resorting to a show of force to assert its territorial claims in South China Sea and East China Sea. India should anticipate China's indulging in similar show of force to assert its border claims in Eastern Sector especially in Kameng and Doklam in Western Bhutan, at an opportune time as her main areas of interest are in this sector.

Having seen the major changes that will impact the way, wars will be fought in future, a quick look at the future operating environment and its implications for our Armed Forces is a must. In the coming decades,

11 Lt Gen Vinod Bhatia accessed at https://www.awazthevoice.in/newsdetail/How-prepared-India-is-to-face-non-traditional-security-challenges-2896.html

Indian Armed Forces would have to be prepared for multi-domain battles with varying intensity and duration. These would include sub-conventional conflicts involving radicalized proxies and limited use of latest technologies to conventional conflicts of varying scale involving long duration non-contact phase, Grey Zone and hybrid warfare, under an overall nuclear overhang. Information warfare including cyber, psychological and electronic warfare resources will be increasingly employed both during peace and war. Conventional conflicts will gradually see the use of networked artificial intelligence supported stealth unmanned systems in land, sea and air domain, precision guided hypersonic weapons, long range high energy weapon systems, space based sensors and weapons, to name a few. These advanced technologies would be fielded by not only major but regional powers as well. In order to ensure that the Armed Forces are capable of operating effectively in future, we need to develop suitable joint doctrines that would enable common understanding of the operating environment and its challenges. Joint Doctrines would also guide formation of integrated force structures, training and war fighting. Without jointness at all levels from the tactical to the strategic, we cannot hope to win future wars. Issues like integrated theatres, Joint Commands and methodologies for developing joint force structures with suitable combat potential to meet both immediate threats and having futuristic capabilities, would need to be resolved at the earliest at the national & military strategic level. Another major implication of the future operating environment is the necessity to accord higher priority to information warfare and develop suitable concepts that fully utilize all its capabilities. This will enable, quickly establishing dominance over the adversary in any future conflict. Large investments would also need to be made to develop new technologies, in conjunction with the civil private industry, as most of these technologies are dual use. This will entail framing suitable policies for increasing interface with the civil industry. The Armed Forces would also have to assess the impact of new technologies especially as they would increase transparency of battlefield, precision, range & lethality of engagement. Thus, over the long term, existing manpower levels may need significant reduction so that adequate funds are available for capital acquisitions. However, we must be cognizant of the fact

that ensuring territorial integrity along the LAC and LC as also sub-conventional conflicts will continue to be manpower intensive in the coming decades. This is primarily because suitable technologies that will enable better force effectiveness with minimal collateral damage, will take considerable financial investments to be made. Battle field transparency and speed of decision making by utilizing AI will reach phenomenal levels, thus posing cognitive challenges for armed forces relying on human manned legacy systems. Unmanned systems that are autonomous with precise and intelligent targeting capability would require that own forces must be comparatively smaller in size, task oriented, highly mobile & with decentralized decision making. This will enable them to disperse and concentrate as per operational requirement. Military leadership challenges will be posed by speed of maneuvers, multiple domains in which operations will have to be conducted and 24x7 nature of operations. In the absence of contact leadership, morale of troops due to the numerous battle field challenges will also be problematic. Though the future operating environment will be highly challenging, however, the Indian Armed Forces and the nation have several times overcome serious impediments, to achieve resounding success. The Armed Forces are already seized with the issues of jointness, internal restructuring, revised manpower planning and military leadership transformation. Refining of procurement processes and building up an indigenous defence industrial base are also issues which have received careful attention. There is a need for greater participation and involvement of the political hierarchy in ensuring transformation of the Indian Armed Forces, as issues involving formulation of long term strategic military objectives, reorganization of higher defence control organization, defence budget, weapon systems procurement etc need long term strategic thinking and commitment. Issues 'military' must only be seen from an unbiased perspective, keeping national security foremost in mind.

The complexities of the future security environment demand that India be prepared to face a wide range of threats of varying levels of intensity. Success in countering these threats will require skillful integration of the core competencies of the three Services into an integrated force

structure. However, reorganisation by itself will not succeed in achieving such integration. What is also required is a change in mindset, a change that makes every soldier, sailor and air warrior feel that he is a member of the Indian Armed Forces and not just the Indian Army, the Indian Navy or the Indian Air Force. Consequently, a joint force, which acts in an integrated manner, is not just desirable but an imperative.

***Lt Gen Vinod Bhatia,** PVSM, AVSM, SM (Retd) is a former Director General Military Operations and former Director CENJOWS, New Delhi.

CONTOURS OF NATIONAL SECURITY STRATEGY AND MILITARY STRATEGY FOR INDIA

Lt Gen PS Rajeshwar, PVSM, AVSM, VSM (Retd)*

"Changing geo-politics and geo-strategic equations directly impact our National Security……. We in India must therefore develop a sound strategy through a robust policy framework in order to manage and resolve future challenges faced by us."[1]

Shri Rajnath Singh, Hon'ble Raksha Mantri

Abstract

India aspires to be a strong, prosperous and modern power. We are witnessing an intense power play between the US and China, with the former shifting focus to the Indo Pacific. India has border disputes with China and Pakistan, both of whom are also colluding to pose more threats. Pakistan's proxy war in J&K and China's increasing influence in our neighborhood have only added to our concerns. The Galwan clashes were an inflection point in India-China relations and for security in the region.

National security, today, encompasses many critical facets, which need to be integrated. It is time that we formalize the national security strategy and military strategy, and place it in the open domain

1 Shri Rajnath Singh, Hon'ble Raksha Mantri, Convocation Address at NDC, New Delhi, 07 March 2020, (https://www.rajnathsingh.in accessed on 23 June 2021)

for discussion and refinement. This will give an impetus to various levers of the nation to help secure India in the best possible manner.

Introduction

India aspires to be a strong, prosperous and modern power. Our national security should comprise how we safeguard our nation's existence and protect its vital interests. Since this involves multifarious and often complex aspects it would demand a set of guiding principles that lead to sound decision making at all levels. In other words, a national security strategy for India would help in planning of the ways and means to achieve key national objectives.

Similarly, a military/ defence strategy would provide a clear roadmap as to how we lay down military objectives, specify the required resources and work out a way in which to accomplish those objectives. It would also obviate any gaps in our preparation or a stretch caused by ambitious plans.

Presently such strategies are not in the public domain. Once these are disseminated, it will provide a common understanding about the challenges faced by us, how we intend to tackle them and provide a unity of purpose to numerous levers of our nation which prosecute them. It will help not only in judicious resource allocation and optimum risk management within the country but also to indicate our intent worldwide.

Geostrategic Scan

Today we are witnessing an intense power play between the US and China in global leadership and influence. While China is asserting itself in economic and military aspects, the US has refocused its energies to the Indo-Pacific region. The EU and UK are constantly being challenged by Russia, who is attempting to regain the position it once had in global affairs. The Middle East is in turmoil with battles involving Israel, Iran, Turkey, Syria and Yemen with some resulting in large scale

migrations. Afghanistan is the scene of an US exit after two decades and destabilization due to Taliban's bid to grab power. Chinese influence in Africa and Latin America has meanwhile grown immensely. Australia's stance after the pandemic has led to economic coercion by China. Al Qaeda, ISIS and other terrorist networks are active in many parts of the world. The Covid-19 pandemic is affecting everyone concurrently.

Looking at our region, China has adopted a belligerent attitude towards us, particularly after the Doklam incident in 2017. There had been standoffs in Ladakh before, but after the Galwan clash, Chinese deployment and infrastructure developments in 2020 revealed their blatant attempt to alter the LAC, violating existing CBMs and agreements in vogue since 1995. These clashes have become an inflection point in our future relations with China and for security in the region.

Pakistan's hostility towards India has often manifested through its abetment to cross border terrorism in J&K, which led to our retaliatory air strike, after the Pulwama incident. Further, Pakistan has been spending hugely on defence procurements and sustenance. It has been helping the Taliban in Afghanistan and hopes to reap dividends soon. The emerging Afghanistan situation and a fragile economy, seem to have pushed it towards implementing ceasefire with us. "With the ceasefire holding on the Line of Control in the last few weeks, there is growing optimism about the prospects for a dialogue between India and Pakistan".[2] China has been bolstering Pak in diplomatic, economic and military spheres. CPEC, as part of the BRI helps China gain access to the Arabian Ocean through Gwadar.

Simultaneously, China has enhanced its long-term presence in our neighbouring countries in South Asia, through huge economic loans, construction projects, labour, military equipment, digital infrastructure, maintenance and training initiatives. This is impacting our relations with these neighbours adversely.

2 C Raja Mohan, For Pakistani army chief it's the economy, stupid, Tripping on Geoeconomics, Indian Express, 31 March 2021.

National Security Strategy

Every nation intends to secure itself comprehensively. Primarily national power is anchored on the diplomatic, economic and military pillars, bound together by the information one. In an interconnected world, other dimensions such as internal security, human security, science and technology, education, health and bio-security, climate, energy, and cyber, by themselves and in combination, also determine how secure a nation is or will be. Any setback in these dimensions could well undermine national security, as being witnessed in the pandemic now. National power being relative, national interest could make nations partner with friendly countries to achieve desired national security.

National security objectives could then be enumerated as given below:-

(a) Protect our sovereignty.

(b) Ensure our territorial integrity.

(c) Secure our people's well-being and interests.

(d) Preserve our way of life.

Progressing Externally

UN has been instrumental for global peace over the last seven decades. India must continue striving hard to become a permanent member of the UN Security Council. As a leading developing country, we can then champion climate-change, counter-terrorism, cybersecurity and other such important causes.

In the multipolar world today, we must strive hard to pursue 'strategic autonomy. Relations with the US have prospered in the last two decades, where we are a Major Defence Partner and member of a revitalized Quad now. These must be taken to the next level. Also, relations with Russia, which has steadily supported us, should be progressed deftly. Greater economic and security partnerships with EU and UK continue to be important. New opportunities emerging in our relations with Saudi Arabia and the UAE will help our huge diaspora, improve our connect with Islamic nations and influence Pakistan to alter its behaviour with us.

After the 2020 clashes China has probed India's vulnerabilities in the economic, cyber and information domains, which need to be guarded against. Due to globalization trade with China will remain appreciable, till we build alternative supply chains. Some environmental issues could see a convergence, but Chinese plans for more dams on the Tibetan Plateau could create greater water scarcity for us and hence must be challenged.

FATF has generated a lot of pressure on Pakistan which should be kept up, till the latter desists from supporting terror groups. This aids our national security. The situation in Afghanistan is complex and if Taliban mainstreams itself politically, we could be open for talks with them.

We have to continue strengthening our relations with immediate neighbours, especially Bangladesh, Sri Lanka and Myanmar and progress connectivity, trade, tourism, medical assistance and IT initiatives. Pursuing BIMSTEC cooperation vigorously and helping others in the IOR will deliver rich dividends.

Strengthening Internal Security

The internal security situation in India is facing challenges due to the ongoing terrorism in J&K, insurgencies in the North East and Left-Wing Extremism. The threat of Al Qaeda and ISIS in the future can also not be discounted. We remain prone to agitations on grounds of religion, caste, creed, language, ethnicity, labour, farming and such other issues, which can be exploited by any adversary.

The unrest in J&K has been prevalent for over three decades. Over the years Pakistan has been aiding separatist ideology, facilitating infiltration and financing terror in J&K. The situation is improving gradually. "Due to the persistent efforts of security forces, terrorist incidents in 2020 when compared with 2019 decreased by about 63%".[3] With the new ceasefire in vogue with Pakistan on the Line of Control since March 2021, the border areas should be more peaceful. A lot can be done to

3 Ministry of Home Affairs, Year End Review 2020, PIB, GoI, 07 Jan 2021, pp1.

assuage the concerns of the people, some of whom are alienated. A whole of Govt approach would necessitate winning their hearts and minds by empowering them in terms of political participation, education, health, local industry, enterprise and tourism initiatives. As the emerging Afghan situation could impact J&K adversely, efforts must be accelerated.

The North East has been the scene of some of the oldest insurgencies in India. Demographic turmoil, identity issues, ethnic discord, illegal migration, lack of development, porous borders, and a desire for autonomy have contributed to this situation and led to legacy issues. The Govt has been able to carve out Ceasefire/ 'Suspension of operations' agreements with some insurgent groups to usher in temporary peace. While violence levels have reduced in recent years, unlawful activities have not abated. The current situation in Myanmar has also impacted the North East. We need to enable greater political empowerment, communicate effectively with local communities, continue talks with the insurgent groups, improve development of the region and govern better. The North East is a launch pad for our Act East Policy. A stable situation here, benefits the nation immensely.

Left Wing Extremism has plagued us for over a decade. "The last six years have seen significant decline in LWE violence as well as the geographical spread of LWE".[4] The extremists operate largely from dense and remote forests aided by discontented tribals, who have been disempowered from their land, water and other resources, impacted due to deforestation and deprived of good governance. While strengthening of the intelligence mechanism and inter-state coordination have been done, the police forces could do with better training and equipment. The LWE ideological narrative will have to be countered effectively in the affected areas, apart from enabling the tribal communities and ensuring better livelihood.

Improving Core Strengths

The most fundamental of inner strengths of a nation is its economy,

4 Ministry of Home Affairs, Annual Report 2019-2020, Govt of India, Para 2.25, pp16.

which determines the overall prosperity. “India’s GDP shrank by 7.3% to Rs 135.13 trillion in 2020-21 (in real terms adjusted for inflation)”.[5] The Govt needs to improve the present state equitably, through its fiscal policy interventions and enable greater employment, price stability and growth rate. Simultaneously, the RBI will have to craft a pragmatic monetary policy to keep inflation in check. A look at certain key economic sectors becomes pertinent.

“Agriculture is the primary source of livelihood for about 58% of India’s population”.[6] As agriculture enables our food security and provides work for bulk of our people, there is a need to maximise our production, conserve our natural resources and look for sustainable technologies through scientific research. Improvement of farmer education, digital connectivity to markets, agri-information base and access to latest techniques becomes essential.

“Industry forms about 25.92% of our GDP”,[7] drives growth and provides jobs. It is also vital to our self-reliance and for our Atmanirbhar-Bharat mission. For this, basic infrastructure facilities in the country need a huge upgrade. Physical and digital connectivity, warehousing, supply chain management, computer and mobile penetration would have to be enhanced manifold. There is enough scope for the industry to grow and provide livelihood to many.

With greater urbanisation, the services sector will grow significantly from the 53.89% (GVA) share of the GDP. Indian IT/ITeS and Fin tech companies, healthcare, tourism, logistics and transportation, media, sports and entertainment contribute to this sector. We need to continuously upskill our enterprising youth and make this sector cater for regional and global needs.

5 Vivek Kaul, India’s GDP contracted by 7.3% in 2020-21, with revival postponed to 2022-23, Mint, 31 May 2021, (https://www.livemint.com accessed on 12 June 2021).

6 Snapshot on Indian Agriculture and Allied Industries Report, March 2021, (https://www.ibef.org accessed on 07 June 2021)

7 Statisticstimes, Sector-wise GDP of India, 17 Jan 2021, (https://www.statisticstimes.com accessed on 23 June 2021)

As India aspires to become a leading global economic power, its energy demands will increase for its industries, manufacturing, infrastructure development and better quality of living. “Coal fulfils 44% of our energy demand[8] while oil provides 25%”.[9] Import of oil implies greater dependency and Current Account Deficit. Distribution of power needs be fixed to improve energy efficiency. In the short term we can increase domestic coal production and endeavour more efficient solar energy and bio gas utilisation. In the long term a number of potential non-conventional energy alternatives will have to be explored. Building up of strategic petroleum reserves for contingencies also needs to be further augmented.

Science and technology provide us the platform to speedily make India modern. While we have progressed reasonably in the past, a lot needs to be done in terms of patents, publications and the quality of research for a country of our size. “Keeping in mind the impediments to worthwhile scientific research, a National Research Foundation has been set up to expand the ecosystem, coordinate and integrate across various establishments”.[10] The fruits of this initiative and the dedication of an enhanced pool of scientists and technocrats will make us more technologically secure for the future.

Cybersecurity has gained immense importance. With a number of critical services riding on the ICT bandwidth globally and hardware devices resourced from various parts of the world, cybersecurity poses a challenge. “The challenges arise from nation states, non-state actors and individuals (who) are at a peer level, all capable of waging attacks.[11] India needs to protect its critical digital infrastructure, gateways and data sets. “The reason why cyber- attacks are launched with a degree of impunity is that attribution of these attacks to a nation state is extremely difficult”[12] Facing such ambiguity, protection would become difficult and

8 IEA India 2020 Energy Policy Review, pp 229, (https://niti.gov.in accessed on 17 June 2021)
9 ibid, pp 249.
10 National Research Foundation 2020, (https://www.psa.gov.in accessed on 08 June 2021)
11 Dr VK Saraswat, Member Niti Aayog, Cybersecurity, (https://www.niti.gov.in accessed on 08 June 2021)
12 Lt Gen DS Hooda,The trajectory for future wars, India Today, 03 January 2020, (https;//www.indiatoday.in accessed on 26 Jun 2021)

retaliation more so. We will need a pragmatic policy as part of our cyber strategy. Simultaneously we must make our systems resilient through indigenization of various hardware, software and operating systems.

Every Indian aspires towards living a decent 'way of life', for which education and health are key factors. "The Human Capital Index 2020 (World Bank data) for India stands at 0.49, a measure of productivity of the next generation of workers relative to the benchmark of complete education and full health".[13] To capitalize on our demographic dividend, we need to educate and skill our youth for a strong work force. "We are increasing healthcare spending to 2.2 trillion Indian rupees ($ 30.20 billion) to help improve public health systems as well as the huge vaccination drive to immunize 1.3 billion people"[14]. But more is necessary for health outlay. Bio-security also needs greater attention at the apex level, given our present experience with the pandemic.

Climate change too threatens India's national security. Our coastline of about 7500 km is periodically affected by rise in water levels, cyclones and other ecological disasters. "By the end of the twenty-first century, average temperature of India is projected to rise by approximately 4.4 deg C, relative to the recent past under the RCP 8.5 scenario".[15] Himalayan glaciers are retreating, causing avalanches, flash floods and landslides more frequently. Coal power stations, industry, transportation and stubble burning are giving rise to huge air pollution, and leading to long term health risks. Water depletion is resulting in parched lands. We will have to develop fast, while overcoming these challenges. The risk mitigation measures will imply having coal use caps, promoting renewable energies, water conservation, audit of energy consumption and enhancing public awareness.

13 The World Bank, "The Human Capital Index 2020 Update: Human Capital in the time of Covid-19." (https://openknowledge.worldbank.org accessed on 07 June 2021)

14 NDTV, India doubles healthcare spending, more FDI allowed in insurance, 01 February 2021. (https://www.ndtv.com accessed on 27 June 2021)

15 Assessment of Climate Change over the Indian Region, A Report of the Ministry of Earth Sciences, 2020, pp xiv.

Military Strategy

Much as we desire peace, we would need to be cognizant of the adversarial attitude of our neighbours, China and Pakistan, both of whom have border disputes with us. China has greatly benefited from Pakistan's hostile actions against India. It has consolidated itself in Tibet, and built up its military infrastructure there. China's restructuring of the PLA, military modernization and formulation of its Active Defence Strategy indicate its belligerence. "Permanent terminal objectives even in the event of a full-scale war are most likely to be Chinese perception of his traditional borders which in Ladakh are close to the current LAC and in the Eastern Front includes the state of Arunachal Pradesh"[16]. It is likely to pursue military coercion, fixing our forces on the Northern borders and constraining our maritime power in the Indian Ocean. This portends more friction points in the coming decade.

"Pakistan, on the other hand, has been following a policy of a 'thousand cuts', against India".[17] It relies on Proxy War and propagates the threat of using tactical nuclear missiles to offset its conventional asymmetry with India. Concurrently it has armed itself with Chinese equipment such as JF 17 aircraft, Al Khalid tanks, submarines, missile technology, rocket launchers and UAVs.

"There is increased cooperation between Pakistan and China, both in military and non-military fields. A two front situation is something we must be ready to deal with."[18] On the other hand, though the Pakistan Army Chief has recently stated "we feel that it is time to bury the past and move forward"[19] it would be prudent to keep up our guard, especially as collusion between China and Pakistan is a possibility, with increasing

16 Lt Gen PR Kumar (Retd), India – China standoff: Need to be prepared for two-and-half front war (Part III of three-part series), 26 June 2020, (https://www.southasiamonitor.org accessed on 26 June2021)

17 Lt Gen Harwant Singh (Retd), Pakistan's policy of a thousand cuts, The Tribune, 08 April 2016.

18 Dinakar Peri, Will hold our ground along LAC: Gen Naravane, The Hindu, 12 January 2021, (https://www.thehindu.com accessed on 21 Jun 21)

19 Gen Qamar Javed Bajwa, Address at National Security Dialogue, 18 March 2021, (https:// www.dawn.com accessed on 17 June 2021)

exercises, training and build-up of war-waging potential. In fact, at worst, India could face a two and half (insurgency) front war.

Military Objectives

In the prevailing environment we could attempt the following military objectives:-

(a) Deter adversaries from carrying out any aggression.

(b) Defend the integrity of our operating domains. If war is forced upon us, end it on a favourable note.

(c) Assist to ensure internal security, when necessary.

(d) Provide aid to civil authorities, Humanitarian assistance and Disaster relief, and Peacekeeping Operations when required.

(e) Become self-sufficient in defence equipment, ammunition and sustenance.

Strategy

The military strategy in a conflict against either or both the adversaries would be specific and depend upon the circumstances and type of conflict we are involved in, calibrated by the desired level of escalation. The military strategy broadly could be on the following lines-

(a) As part of the Whole of Govt approach, integrate with other agencies and respond appropriately to any external threat with credible military force.

(b) Maintain our operational readiness to fight in situations ranging from ‘short of war’ to a full spectrum conflict against our adversaries.

(c) Develop requisite capabilities to ensure deterrence, enabled by necessary planning, equipping, infrastructure and training of our individual and joint forces.

(d) Usher in greater jointmanship by assigning combat responsibilities to theatre commands, revising doctrines and training methods for efficient resource utilization and achieving synergy in operations.

(e) When employed for internal security, assist Govt efforts by bringing the security situation under control.

(f) Assist the defence-industrial complex on military specific requirements, trials and validation.

(g) Be ready to sustain full scale operations for 30 days with adequate equipment and ammunition reserves.

The nature of war remains the same and involves the imposition of one's will on the other. However, it's the character of war, primarily tools and methods, that is undoubtedly changing rapidly. We will need to keep a close watch for developments by our adversaries to pick up any changes and tailor our strategy accordingly.

Building Capabilities

At present the three services possess certain capabilities which will optimally increase once jointmanship is enhanced. However, in future we would need to augment the capabilities of each service and further strengthen our cyber and space forces to meet emerging threats.

The land capabilities could be built up in the following manner:-

(a) Improve our border infrastructure (rail, road, airstrips and helipads) to enable swift mobilization and movement of forces.

(b) Enhance intelligence, surveillance and reconnaissance means, qualitatively and quantitatively, while integrating with decision making and firepower entities.

(c) Develop customized rapid response forces (Mountain and Plains - integrated battle groups) for application.

(d) Fill up voids and upgrade vintage equipment.

The air capabilities could be planned as follows:-

(a) Replace the depleting fighter squadrons with a suitable mix of 'State of the art' and indigenous platforms.

(b) Augment force multiplier effect with Air-to-Air refuellers, AWACS and AEW&C aircrafts.

(c) Modernise the transport and helicopter fleets for speedy inter-theatre and intra-theatre movement.

(d) Increase mix of UAVs and loitering PGMs in air vectors.

(e) Improve airborne and ground sensors, counter-UAV measures and other weapon systems.

The maritime capabilities are the key to our consolidation as a regional power and its projection. It needs to be enhanced further through:-

(a) Conventional and nuclear attack submarine fleets.

(b) Minesweepers and anti-submarine ships.

(c) Unmanned aerial and underwater platforms.

(d) Naval Utility and Multi-role helicopters.

In addition, the three services must improve combat infrastructure and train as part of joint forces to fight in envisaged scenarios, including under CBRN conditions. They should plan and integrate cyber, space, electronic warfare and information warfare capabilities for joint operations in a multi domain environment. In future we may have to counter the adversary's capabilities on AI, quantum computing and robotics on the battlefield, which will pose newer challenges. With the employment of new technologies in warfare, the 'system of systems' will change for which our strategies and tactics will have to be altered. We need to make greater investments in future technologies, especially pertaining to space and cyber domains.

As we go forward, the services and joint forces will need to rework force structures for future combat. Models would have to be laid out, test bedded and improved as we proceed ahead. The operational transition

from single service to theatre commands, in this milieu, would need careful consideration and deft steering.

Conclusion

The world is currently in the midst of a great power competition between US and China. China's economic and military power are posing new challenges to many nations. India has been particularly affected by the clashes with China on the LAC and the pandemic. The growing asymmetry between us could encourage China to coerce us from time to time. On the other hand, Pakistan is continuing with its hostility towards us and its proxy war in J&K. The probability of conflict-situations that are 'short of war' remains high. At worst, we could even be fighting a two and half front war. Under the circumstances a comprehensive national security strategy and a focused military strategy are urgently needed.

Economic power is key to our development. A potent military can only be developed based on a strong economy. Keeping in mind the threats, the services will need a greater budget, once the economy normalizes. Only then would they be able to secure the nation robustly.

The national security strategy and military strategy should be made known to the public for an informed debate over the subject. A critical appraisal will definitely drive its further refinement. It would also strategically communicate our national interests and how we intend safeguarding them. Finally, national resilience would always be vital for the success of any national security strategy.

***Lt Gen PS Rajeshwar,** PVSM, AVSM, VSM (Retd) is a former CISC, HQ IDS

REAPPRAISAL OF MISSIONS, ROLES AND TASKS OF INDIAN ARMED FORCES – GAPS AND PATHWAYS FOR COMPLEMENTARITY, INTEGRATION AND JOINTNESS: A DOCTRINAL APPROACH

Air Cmde T Chand (Retd)*

Abstract

Roles, missions and tasks of the armed forces when viewed through a doctrinal prism reveal ruggedness or the lack of it for war fighting preparedness. Intangibles like jointness and integration among the armed forces also evolve from the doctrinal framework. Like most world militaries, Indian armed forces also have a plethora of doctrines evolved over a period of time. Land Forces doctrine was published in 2018 after the publication of the Joint Doctrine of the Indian Armed Forces-2017but was required to be read in conjunction with it rather than a self-contained document. The Indian Maritime Doctrine, 2015 version and IAF doctrine of 2012 were more detailed and defined roles, missions and tasks of the respective services more clearly. The jointness and integration aspects were also spelt out to a great extent even though they preceded the Joint Doctrine of the Indian Armed Forces-2017. The non-availability of the National Security Strategy in the open domain seems to have straitjacketed the service specific doctrinal thinking of the respective services. Joint doctrine have addressed a number of issues but gaps still remain. A national defence doctrine is reportedly under preparation which is likely to suggest pathways for complementarity, integration and jointness through a doctrinal approach. Inspired by this doctrine, Service

specific doctrines would reinvent themselves and inspire the leaders for higher level of military preparedness in a shortest timeframe without much additional cost.

Missions, Roles and Tasks of the Indian Armed Forces have evolved over a period of time and have been articulated by the respective Services through various documents including doctrines. These documents are largely well researched and Service specific. The doctrines issued by the respective Services reflect the realities of times and address some aspects of the integration and jointness in a limited way. An analysis of the annual reports of the Ministry of Defence[1] also clearly reveals the Service specific nature of the functioning of the armed forces. Doctrinal aspects of the Intelligence, remained untouched by the Service specific doctrines. A joint doctrine was issued by the HQ IDS in 2017 which highlighted the changed realities of preparedness for war fighting which was far from Service specific missions, roles and tasks. Integrated Intelligence Structure were briefly described by this doctrine. This doctrine served its purpose well but gaps continued to remain requiring developments of pathways for complementarity, integration and jointness.

Reportedly, work is under progress for preparation of a national defence doctrine for addressing future requirements realistically. Earlier it was widely reported that NSA was ready with the new doctrine for the armed forces[2]. In this article, missions, roles and tasks of the Indian Armed Forces have been reappraised, gaps identified and pathways for complementarity, integration and jointness suggested through a doctrinal approach.

1 Ministry of Defence, Annual Reports, https://www.mod.gov.in/documents/annual-report. 21 July 2021.

2 Ashwin, "National Security Adviser Ajit Doval ready with India's new military doctrine", Strategic Front, 19 September 2019https://www.strategicfront.org/forums/threads/national-security-adviser-ajit-doval-ready-with-indias-new-military-doctrine.3497/. 09 July 2021.

Land Warfare Doctrine – 2018[3]

The document is not complete in itself and is required to be read in conjunction with the Joint Doctrine of the Indian Armed Forces-2017[4]. Missions, roles and tasks of the Indian Army have not been sufficiently elucidated in the doctrine. The Doctrine provides broad guidelines for the conduct of operations by the Indian Army across the entire spectrum of conflict. The focus remains on force modernisation, resource optimisation and innovative conceptual processes leading to winning strategies for future wars. As always, geostrategic environment, external and internal threats, possible responses and a way ahead to develop capabilities for the future were stated to be the major determinants shaping the Land Warfare Doctrine. The doctrine was expected to lay the foundation for formulation of strategies for the Northern and Western Fronts and Operational Directives.

As theorised in the doctrine, the Indian Army continues to develop strategies and capabilities for contingencies throughout the expanding spectrum of conflict aiming to dissuade, deter, delay and defend by proactive and responsive engagements at the place and time of own choosing, whenever there would be an imminent threat to National Security. In doing so, the strategy was expected to be application of all the elements of the military arsenal in conjunction with other instruments of Comprehensive National Power. The focus of the Indian Army continues to develop capabilities for facilitating jointness and integration amongst the three Services. Inspired by the doctrine, the Indian Army should continue to be a potent force with deterrent.

Land Force Power doctrinal aspects were summarised differently in the Joint Doctrine of the Indian Armed Forces which stated that “The threat perception arising out of large disputed land borders, directive to defend territorial integrity and response options over the entire spectrum

3 Indian Army, Land Warfare Doctrine – 2018, https://www.ssri-j.com/MediaReport/Document/IndianArmyLandWarfareDoctrine2018.pdf. 10 July 2021.

4 HQ Integrated Defence Staff, Joint Doctrine Indian Armed Forces, https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf, 10July 2021.

of conflict, in the realm of defensive and offensive operations, guide the employment philosophy of land forces. The overall force generation matrix would be achieved through optimum force structuring, modern equipment and effective training across all types of terrain and climatic conditions. Land forces could be employed singly or in conjunction with the other two Services in conventional and sub-conventional role during Joint operations at a very short notice. Capabilities through specialized forces would be maintained to fight persisting sub conventional threats with timely re-orientation, for conventional employment/deployment".

The overall doctrinal aspects of the Indian Army were well analysed by the Arzan Tarapore who concluded in his paper titled, '*The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance';*[5] that "within the military, the Indian Army is presently demonstrating a notable capacity for reform with the recent establishment of a CDS, the restructuring of Army Headquarters, and the creation of IBGs. These reforms seem to be designed to support the old offensive doctrine that has defined the Indian Army's use of force for over half a century. Modernization is not only new equipment and organization but also involves new theories of victory, and doctrinal change that allows responses along the full spectrum of conflict. Punitive incursions into enemy territory, using mass and firepower, are not always effective in wartime, and even rarely useful as coercive options during a crisis. If the Indian Army remains focused on conventional offensive operations, it is likely to become increasingly irrelevant as a tool of national security policy". The author also pointed out that, "this doctrine is orthodox in its preference for large combined-arms army formations, usually operating with minimal coordination with other services and relatively autonomously from its political masters. It is offensive in its military aims of imposing a punitive cost on the enemy—usually in the form of capturing territory for the purposes of gaining leverage in postwar negotiations—even if it

5 Arzan Tarapore, "The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance", Carnegie India Working Paper Aug 2020, https://carnegieendowment.org/files/Tarapore_Ground_Forces_in_Indian_Military.pdf, 11 July 2020.

is usually deployed in the service of a strategically defensive policy of maintaining the territorial status quo. And it is perhaps a doctrine which represents an enduring set of principles governing the Indian Army's use of force, regardless of the scarcity of public doctrinal publications".

The Land Warfare Doctrine could have adopted the essence of the Joint Doctrine of the Armed Forces to make it a self-contained document, highlighting pathways for complementarity, jointness and integration as has been done to a great extent in the Indian Maritime Doctrine and the IAF Doctrine which were authored before the publication of the Joint Doctrine in 2017.

Indian Maritime Doctrine[6]: Indian Navy, Roles, Missions and Tasks

The doctrine states that the roles, missions and tasks of a navy encompass its core activities and describe what the navy does in times of peace and war and also define the scope of employment of the navy and application of maritime power by a country. The doctrine determines the way in which the navy would be organised, equipped and trained.

The stated roles of a navy are the broad and enduring purposes that govern the establishment of that navy. In the performance of these roles, various objectives would need to be attained for which, naval forces are deployed on specific Missions for accomplishment of which, naval forces have to perform a variety of operational and tactical level Tasks, which span the entire spectrum of maritime operations.

A reappraisal of the roles, missions and tasks of the Indian Navy seen through the doctrinal prism would reveal that several possible gaps have already been plugged to a great extent through a clarity in the writings of the doctrine and strategy[7]. As these publications are navy specific, pathways for jointness and integration, even those enunciated

6 Indian Navy, Indian Maritime Doctrine, https://indiannavy.nic.in/content/indian-maritime-doctrine-2015-version. 12 July 2021

7 Ensuring Secure Seas: Indian Maritime Security Strategy, https://indiannavy.nic.in/sites/default/files/Indian_Maritime_Security_Strategy_Document_25Jan16.pdf. 20 July 2021.

in the Joint doctrine are needed to be articulated and incorporated in the doctrinal approach of the Indian Navy as is evident from the following paragraphs summarizing roles, missions and tasks of the Indian Navy.

Role of Indian Navy[8]

The role of the Indian Navy covers entire range of operations in which naval forces would be employed ranging from high intensity war fighting at one end to humanitarian assistance and disaster relief operations at the other and each role demanding a specific approach to the conduct of operations.

The Military Role. The navy's military role is characterised by threat or use of force at the sea and includes application of maritime power in offensive operations against enemy forces, and defensive operations to protect own forces and territory. The military role is performed through accomplishment of specific military objectives, missions and tasks.

Diplomatic Role. Naval diplomacy entails the use of naval forces in support of foreign policy objectives for strengthening international cooperation. The larger purpose of navy's diplomatic role is also to shape the maritime environment to serve the national interests of India. This is facilitated by the traits of the naval forces which can be readily deployed and can perform multiple roles and tasks.

Constabulary Role. In the constabulary role, naval forces are employed to enforce law of the land and force is employed for self-defence only while executing this role. The promotion of India's maritime security is one of the prime responsibilities of the Indian Navy. The range of tasks that the India Navy has to undertake in the constabulary role range from Low Intensity Maritime Operations (LIMO) to maintaining good order at sea. This further includes aspect of coastal security, as part of India's overall maritime security. With establishment of the Indian Coast Guard (ICG), law enforcement aspects of the constabulary role within

8 Indian Navy, Role of Navy, https://www.indiannavy.nic.in/content/role-navy. 13 July 2021.

the Maritime Zones of India (MZI) have been transferred to the ICG. Constabulary tasks beyond the MZI are vested with the Indian Navy. Responsibility for overall maritime security has been mandated to the Indian Navy, in close coordination with the ICG, State Marine Police and other authorities.

Benign Role. The benign tasks including humanitarian aid, disaster relief, Search and Rescue (SAR), ordnance disposal, diving assistance, salvage operations and hydrographic surveys. The Indian Coast Guard is the designated national agency for maritime SAR in the Indian Search and Rescue Region (ISRR) and Naval units are also called upon to undertake SAR operations when required.

Missions[9]

Naval mission is a clear and concise statement of the task of the command, together with the purpose, that indicates the action to be taken towards the attainment of the objective(s). Broad missions of the Indian Navy are; Maritime Domain Awareness (MDA), Sea Control, Sea Denial, Blockade, Power Projection, Force Protection, Expeditionary Operations, Compellence, Destruction, Sea Lines of Communication (SLOC) Interdiction, SLOC Protection, Special Force Operations, Seaward Defense, Coastal and Offshore Defence, Naval Co-operation and Guidance for Shipping (NCAGS) Operations and above all Nuclear second strike.

Tasks[10]

A naval task is a specific piece of work that is to be done as a duty. It defines the precise activity and its sphere towards accomplishment of the mission. Major tasks envisaged by the Indian navy are; Surveillance, Maritime Strike, Anti-Submarine Operations, Anti-Surface Operations, Anti-Air Operations, Amphibious Operations, Maritime Patrol, Information

9 Indian Navy, Role of Navy, https://www.indiannavy.nic.in/content/role-navy. 15 July 2021
10 Indian Navy, Role of Navy, https://www.indiannavy.nic.in/content/role-navy. 16 July 2021

Operations, Information Exchange, Electronic Warfare, Mine Warfare, Visit Board Search and Seizure (VBSS), Harbour Defence, Naval Cooperation and Guidance to Shipping (NCAGS) and Naval Coastal Security (NCS) Operations and Protection of Offshore Assets.

Reappraisal of the roles, missions and tasks of the Indian Navy articulated in the Indian Maritime Doctrine reveal insufficiency of incorporation of jointness and integration, later included in the Joint Doctrine of the Indian Armed Forces. This well written doctrine would need an upgrade after the arrival of the National Defence Doctrine in the near future.

IAF Doctrine 2012

The Primary purpose of the IAF is to defend the nation and its airspace against air threats in coordination with Army and Navy. The secondary purpose is to assist civil power during natural calamities and internal disturbances[11].

Roles of the IAF listed in the IAF Basic Doctrine 2012[12] state that the exact role that an air force will play would depend upon the nature of the threat, resources available and the nature of the campaign. Main roles of the Air force are listed as; Defence of the national and the island territories, against attack from the air and space both during peace and war, Deterring an aggressor from carrying out hostile acts and if deterrence fails to mount an effective response, During operations, achieve control of the air to the required degree to provide full freedom of action to the air and surface forces, Applying direct force on the enemy's power of resistance by attacking his crucial center of gravity, Synergizing the combat potential of air power with that of the surface forces to achieve joint military aims and objectives, Deploying and

11 IAF Handbook on RTI Act 2005, Chapter 2, Particulars Of Organisation, Functions And Duties, https://indianairforce.nic.in/sites/default/files/HandbookOnRTIAct2005%20-%20latest%20%2827jun19%29.pdf15 July 2021

12 Indian Air Force, Basic Doctrine of the Indian Air Force 2012, https://www.scribd.com/doc/109721067/Basic-Doctrine-of-Indian-Air-Force-2012-PDF, 15 July 2021.

employing forces to protect and project the national interests in any out of country contingency operation, Assisting the authorities in disaster management or humanitarian relief tasks, Executing counter terrorism and counter insurgency operations, Fulfilling international commitments requiring air power assets, consistent with our national interests and Providing viable second strike capability in case of nuclear attack.

The doctrine recognises that the Revolution in Military Affairs has transformed the role of technology and doctrines in fighting wars. The aim is to isolate the enemy's command and control structures, augment psychological warfare and precision strikes on the critical vulnerabilities deep inside enemy territory. These changes favour employment of air power more than any other form of military power.

The doctrine recognises that the air power today applies parallel force at all levels of war as the strategic, operational and tactical levels have been merged and are now more related to functionality than to location or type of targets. It highlights that the networking of sensors, operators and decision makers has significantly reduced the sensor-to-shooter time period which has resulted in transforming linear warfare into non-linear warfare. The doctrine states that increased focus now is on knowledge and efect and to apply forces synergistically to achieve the desired outcome in the shortest period of time, with minimum casualties and collateral damage.

Air Power and Jointness[13]

The doctrine has laid emphasis on fact that air power delivers best when used in synergy with the other components of military power stating that the conflicts and developments of the past several decades indicate a growing role for air forces

13 Indian Air Force, Basic Doctrine of the Indian Air Force 2012, https://www.scribd.com/doc/109721067/Basic-Doctrine-of-Indian-Air-Force-2012-PDF, 15 July 2021.

The comprehensive doctrine gives details of various missions and tasks which would be undertaken for performance of the role. Written nine years ago, the doctrine reveals some insufficiencies related to jointness and integration which were later incorporated in the Joint Doctrine of the Armed Forces. Gaps revealed during reappraisal of the roles, missions, and tasks of the IAF would need to be complemented in its new avatar which should follow the publication of the National Defence Doctrine.

Joint Doctrine of the Indian Armed Forces

Missions, Roles and Tasks of Indian Armed Forces have been outlined in the Joint Doctrine of the Indian Armed Forces 2017[14] to the large extent. The Military Instrument consists of the three Armed Forces of the Union, namely Indian Army (IA), Indian Navy (IN) and Indian Air Force (IAF) alongwith support elements. The doctrine recognises that the Military Instrument is characterised by provision of insurance and assurance to the Nation and its employment towards these purposes highlighted int the Seventh Schedule of the Constitution of India. It envisages that the Military instrument must remain lethal and precise as it serve as the ultimate instrument for maintaining the unity and the integrity of the Nation in the face of external and internal threats.

The major roles of the Armed Forces, encompassing both domestic and international responsibilities listed in the doctrine are **:** Safeguard sovereignty, territorial integrity and unity of India and preserve National Interests against any threat in the entire spectrum of conflict by possessing and projecting a robust deterrence capability or by application of force, as required; Assist civil authorities to cope with internal threats/ contingencies and provide necessary aid, when requested; Participate in peacekeeping operations and protect the global commons under UN charter; Render military assistance including HADR to friendly foreign

14 HQ Integrated Defence Staff, Joint Doctrine Indian Armed Forces, https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf, 16 July 2021.

countries, when requested; Progress military diplomacy to constructively engage with defence forces of friendly foreign countries.

Major functions of the armed forces are, conventional (Offensive Operations, Defensive Operations, Sub Conventional (Low Intensity Conflict Operations /Low Intensity Maritime Operations), Non-Combat (Aid to Civil Authority, Maintenance of Law and Order, Humanitarian Assistance and Disaster Relief). Conventional War will fall under the "Military Role'' and encompass Offensive Operations; Defensive Operations; Non-Combat Operations.

The Joint Doctrine in the open source domain resulted in a lot of comments and revealed gaps in jointness and integration which are expected to be mitigated through innovations. The National Defence Doctrine is expected to surpass and complement the gaps noted in this doctrine as well.

Doctrinal Aspects and Intelligence Structures

Intelligence Structures form the bedrock of successful completion of military missions, role and tasks in practice. Intelligence gaps especially in the military domain have been revealed on several occasions, including during the Kargil Conflict. Service specific doctrines have remained silent on this aspect. The Joint Doctrine has a section on the Integrated Intelligence structure[15] which states that "Defence Intelligence Agency (DIA) synergises the efforts of the intelligence agencies of the three Services. DIA also coordinates with other National agencies involved in gathering external and internal intelligence and provides requisite intelligence support to the Armed Forces". The three Services have their respective intelligence organisations. These organisations collect and collate intelligence required for Service specific operations and disseminate it to Commanders at all levels. Coordination among the plethora of Intelligence agencies within the armed forces and at a

15 ibid

national level has found many critics pointing to sub optimal response on several occasions. This vast subject of intelligence coordination with apparent gaps also needs specified pathways for complementarity, integration and jointness after a thorough reappraisal.

Conclusion

It could thus be surmised that the reappraisal of the roles, missions and tasks of the armed forces, seen through doctrinal prism, reveals a number of areas where, jointness and integration among the armed forces is required to be enhanced. Service specific doctrines as well as joint doctrine of the armed forces exhibit a number of gaps where complementarity is essentially needed to make the armed forces ready for fighting future wars. Initiatives like preparation of the national defence doctrine and national security strategy are steps in the right direction. Upgraded versions of the Service specific doctrines would need to be issued thereafter. The timeframe for preparation of these documents is important and should be issued before the end of this year 2021. Small cost for consultations with the experts and think tanks is worth the value addition and should be indulged without hesitation.

***Air Cmde T Chand (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi

ADDRESSING THE INTERNAL AND NON TRADITIONAL SECURITY CHALLENGES – GAPS AND PRIORITISED PATHWAYS

Lt Gen Syed Ata Hasnain, PVSM, UYSM, AVSM, SM, VSM (Retd)*

This needs to commence with a full understanding of the term 'security' since it helps demarcate traditional from non-traditional. Security of a nation essentially involves the well-being of the people, their land, sovereignty, resources, heritage, sentiments and aspirations. As long as people can work towards and bear hope to achieve their aspirations they can be classified as secure. National security is also sometimes described as the requirement to ensure the survival of the state through the use of economic power, diplomacy, power projection and political power. However, there will always be some factors and trends which prevent people and the nation from achieving goals. These are mostly classified as threats and can be of diverse kinds. Out of these the well-known and long considered traditional threats are primarily military in nature and in earlier years remained centre stage in the security spectrum. They fall in the conventional and sub conventional domains and involve deliberate attempts at destruction, subjugation and imposition of will, by physical means, causing disruption in the way of life of a society and preventing its advancement or progress. Since the end of World War II the propensity to employ conventional means has diluted due to the development of deterrence by various means; this includes weapons of mass destruction and air power. The usage of the sub conventional domain, however, has increased due to the lower cost and risks involved. After the end of the Cold War sub conventional has largely been the dominant domain.

Non-traditional security challenges are almost the opposite of traditional security threats and refer to the factors other than military. The broad understanding is that these are largely threats to the survival and development of a sovereign state and its citizenry as a whole due to trends of nature, abuse of nature and manmade phenomena. They are caused by diverse factors such as climate change, pandemics, disasters, migration, resource scarcity, human trafficking and even corruption which eats into the development of society. A debate continues whether domains such as cyber, trans-national crime, economic warfare and the most common one of today, information warfare, all of which are human initiated and controlled, fit into the mode of non-traditional threats. I may not wish to legislate on this as it is a debate unto itself. For the purpose of this essay we will presume that all these do lie within the ambit of non-traditional threats and combinations of these with various threats in the sub conventional domain can be also classified as hybrid threats if we are not dogmatic about the exact definition. What probably helps classify all these as non-traditional is that governments the world over are struggling to overcome the combined effects of these threats. The Coronavirus pandemic, repeated cyber-attacks, the effects of climate change especially with many countries failing to work enough towards meeting the Paris and other protocols, rise in natural disasters, the effect of migrations due to civil war and forced economic and social conditions form some of the threats. Further, even the displacement of migrant labour and deliberate efforts at economic warfare forcing an economic downturn by targeting sectors such as energy and shipping, all form a part of the non-traditional security spectrum.

This essay focuses on a few non-traditional security challenges and specific issues of internal security related to these; a comprehensive address all of the full range being constrained by space. The larger subject of sub conventional domain does not find mention here.

Pandemics

Commencing with pandemics I recall that in 1998 while researching non-military threats of that time I was surprised to learn that if the

HIV virus hit India in a serious way the nation would lack the ability to provide sufficient hospital beds and so many would be involved in looking after the sick that it would drive the population to despair. It was also then that I learnt of the 1918-20 pandemic immediately following the Great War. Between 50 million to 70 million died worldwide and the greatest sufferer was undivided India with 12-17 million deaths. Not enough has been written on this pandemic and research on it has been lacking despite the full knowledge that India was the worst affected. Considering this a hundred years later as the Coronavirus hit the world the medical infrastructure in India was still below par. Urban centres and metropolises failed the rush resulting in near paralysis and deep psychological breakdown in segments of the population. The psycho-social domain became of the more pronounced areas of concern, nation wide. Rural India too has simply no means to cater for the levels of morbidity witnessed. Among the major lessons learnt is that pandemics affect national security with four prime areas being most affected; the economy, psyche of the people, societal cohesiveness, and the plight of the poor, especially those who are migrant labour in urban settings. With aspirations at a high due to good economic performance of the last many years the economic downturn of -7 percent upset the nation's confidence. The feasibility of Coronavirus being manmade lays open the path of experiments in bio warfare. India did extremely well to research and develop vaccines against Coronavirus in a very quick timeframe confirming its reputation of being the world's pharmacy. However, gaps remain to be overcome through enhanced research undertaken by aided institutions in conjunction with international partners, creation of efficient data management centres and an effective communication strategy to bring all on a common platform of perception of the existent dangers and the actions underway. Without going into any detailed statistics it is broadly understood by the common man that the pandemic has put India back by at least ten years. The feasibility of manmade virus as a part of biological warfare or accidental leakages will remain a major threat to both developing and developed countries. Mutations of the current virus may continue for some years forcing a complete alteration in the way of existence of the world.

Disaster Management and Climate Change

In the perception of the National Disaster Management Authority of India a disaster is a serious natural or manmade event occurring over a short or long period of time that causes widespread disruption of normalcy and human, material, economic or environmental loss which exceeds the ability of the 'affected community or society' to cope using its own resources. Till Dec 2005 India continued to take an old world and rather unprofessional approach to disaster management. The focus was only on response, employing untrained resources. There was no system of early warning, technology enhancement for mitigation, preparedness or efforts towards organizing community based disaster risk reduction. The Disaster Management Act of Dec 2005 transformed this domain completely. A National Disaster Management Authority (NDMA), National Institute of Disaster Management (NIDM) and a National Disaster Response Force (NDRF) was set up. The focus shifted to preparedness, training, early warning, technology development, mitigation and build back better. 31 guidelines for different hazards have been published along with the latest National Disaster Management Plan (NDMP) 2019. Insistence on the states developing their SDMPs and every Ministry at the Centre along with important institutions also developing their DM Plans has ensured a greater awareness and improvement of the culture of preparedness. However, this is work in progress, with lots of scope for international cooperation and incorporation of best practices. The Prime Minister has personally given a Ten Point program for Disaster Risk Mitigation which provides a suitable national vision to work upon.

While DM is a field where there has been considerable improvement even with much scope remaining for more we must remain conscious of the fact that disasters cause huge financial loss to nations thus affecting national aspirations. Jun-Oct 2019 monsoon floods caused India a loss of $10 billion to be the seventh costliest ever. They also led to the death of 1,750 people — the most among all natural disasters in 2019. Cyclone Fani, which affected Odisha in India and Bangladesh, was the tenth-most costly natural disaster in the world, according to the report. There will always remain a gap between the capability and

the rising tide of hazards, both natural and manmade. Little is realized by states and institutions that investment in the field of preparedness and capacity development in response capability will actually lead to savings in the long run. A state such as Uttarkhand which is so heavily dependent on religious tourism will always remain in dilemma regarding development since this adversely affects the ecology of the fragile mountainous terrain. Broadening of roads, cutting of trees and tunneling the mountains will cause an upset in the ecological balance. Such states need to be compensated as a part of the national plan to prevent any adverse mismatch in development of states.

Sensitization to disaster risk is yet a subject hardly addressed in India but awareness is now on the rise. Inclusion of this domain as a subset in all National Security deliberations at various seminars and discussions and educational institutions will go far in giving a culture of better awareness to the nation.

Migration

Migration has an impact on the security interests of individuals, communities, institutions, nations and regions, posing unprecedented political, social, and economic problems. In addition, migratory pressures have become a significant factor in both internal and international politics.

Internal migration has two dimensions; forced and voluntary variety. Forced migration can be a result of internal conflict (Kashmir Pandits in India), economic conditions (labour from poorer states to richer states) and many times natural and manmade disasters. The ongoing pandemic led to forced return of migrant labour to their rural homes creating joblessness. Persistence of such a state could lead to increase in crimes, class conflict and waywardness of an entire society. The rural to urban migration which is mostly a continuous phenomenon in many developing countries impacts two major areas. First, it upsets the urban-rural balance and in particular adversely affects the agricultural sector. This has an effect on food security and therefore the national economy. Keeping the agriculture belts populated through farmer incentives and

assistance to the farm labour through various subsidy schemes is a commitment that governments have to undertake. Any volatility in this can majorly impact availability of food stocks and social harmony. Secondly the increasing human footprint in cities lowers the quality of life and places pressure on urban resources. Increasing density of population leads to higher crime rates, gender issues and neutralizes much of the development executed by urban bodies. From agricultural turbulence to increased crime migration affects many domains.

International migration is usually a result of conflict. Three prime examples can be quoted. The 3 million Afghan refugees nestled on the Pakistan-Afghanistan border evicted due to the Soviet invasion of Afghanistan in the Eighties became the core centre for the rise of obscurantist ideology leading to the rise of Islamic radicalism. It has troubled the world for the last 40 years and even the Taliban of Afghanistan was created from this segment. The Rohingyas of Myanmar evicted and displaced to camps in Bangladesh have been in various states of migration far from the conflict zone, including the Indian city of Jammu. Migrants of this type are fodder for terror groups. The four million refugees from the Syrian civil war made their way into Europe through all kinds of routes. The effects of the war travelled deep into Europe carrying all the problems associated with migration; societal tension, religious turbulence, political upheaval and more.

While all the above explains the extent to which migration causes problems of security, in India the issue is most acute in the rural to urban movement and the resultant pressure on the cities. A state like Uttarkhand has few opportunities to meet the aspirations of the people. Entire villages have become bereft of the younger generation and that too close in areas close to the national borders. Central aided schemes to retain youth in these areas and expand the footprint of development through education and small scale industry is considered essential.

India has structures in place to meet the challenges of climate change and has been a cooperative member of the international community in its responsibilities. A National Green Tribunal oversees

various issues concerning the environment. The challenges lie in the field of non-adherence to norms in the field of development which usually clash with the needs for the control of climate change. This has to go beyond the status of every case being decided judicially by creating a culture of awareness right from early education.

The Information Domain

Information covers a large canvas of security and is related to perception, propaganda, disinformation and manipulation. Technologically the cyber domain and social media form a part of this. Before the advent of real mass media through television and print media one of the biggest challenges was the aspect of communication to the public, both own and the adversary's. Information and disinformation are powerful tools of influence which could swing or sway opinion. The coming of social media after mass media has exponentially enhanced the capability of communication to the public in a rapid timeframe. Information in audio-visual and print form is easily disseminated and fake news is the new mantra.

China was one of the first to imbibe the lessons of Gulf War I (1990), the first televised war where CNN entered into drawing rooms, offices, coffee shops and many other public places, thus influencing opinion. It adopted the doctrine of 'war under informationised conditions' in 1993. It developed this further with the proliferating development of the world wide web. By 2003 China came out with its doctrine of 'three warfares strategy'. It is a political and information pre-kinetic warfare strategy employing media or public opinion warfare, psychological warfare, and legal warfare. With the advent of social media many nations are adopting this in a stand-alone mode on a regular basis with or without intent to undertake traditional war.

Separatist organizations within nations and anti-national elements of any kind, including networks such as finance, media, drugs and clandestine weaponry have all benefited from the revolution in social media. Creating disharmony through grey zone operations, political

turbulence and communal antipathy to weaken the fabric of nations, particularly those with diverse nature of populations, has become much easier. As 5G networks come into being this potential for mischief will rise. To protect themselves nations must adopt defensive measures and offensive capability, the latter as deterrence. Most nations have considered this threat as something which requires only guidance of the Armed Forces but not their whole time involvement. The cyber domain has now been added to National Security for good measure. India has different organizations undertaking their own cyber security but a cogent policy and structure to oversee has been added a few years ago. The National Cyber Coordination Centre (NCCC) is an operational cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. In addition there is the Defence Cyber Agency (DCA), a tri-service organisation of the Indian Armed Forces. Headquartered in New Delhi, the agency is tasked with handling cyber security threats. The DCA draws personnel from all three branches of the Armed Forces. While India has undertaken some nascent steps in the field of cyber security there is yet much to be done in terms of coordination between organisations, institutions and individual ministries which oversee this.

While the cyber domain is receiving attention the information field appears to have yet been neglected without too much conceptual thought to the structures, policy, identification of resources or a single body to handle and run the information domain where its potential use as a weapon is involved. I&B Ministry appears to have the potential to be converted to such a body or to create an authority under it to run and oversee policy. A Strategic Communication Authority composed of members from different fields such as defence, intelligence, police, academia, economics and political (to name just a few), would study the worldwide developments in the field of information as a weapon against the state and society. This body should look at both, the offensive use of information and the means to quell and counter fake information and enemy propaganda.

Trans-National Organised Crime and Economic Warfare

While transnational organized crime is a global threat, its effects are felt locally. UN Office for Drugs and Crime (UNODC) has recently launched a campaign showing how transnational organized crime destabilizes countries and entire regions, undermines development assistance and increases domestic corruption, extortion, racketeering and violence. The classic example is that of Dawood Ibrahim and his infamous D Company which commenced its operations from smuggling and went on to be exploited by Pakistan to create communal disharmony and turbulence in India's financial capital. The intent was to dent India's national economy by creating an environment of disharmony and insecurity to disallow large scale foreign investments which were lining up as the economy opened in the Nineties; Mumbai was considered the centre of gravity being the financial capital of India. Legitimate government and business operations are the target of such syndicates.

The Encyclopedia Britannica defines economic warfare as – "the use of, or the threat to use, economic means against a country in order to weaken its economy and thereby reduce its political and military power". We are experiencing this today with China. Fearful of the rise of India, China has mixed economic warfare with military coercion at the border region to intimidate India. Attempts are being made to prevent Indian companies getting ships and even containers for transporting their goods as part of international trade. Cyber, information and covert operations can also be used as instruments for economic warfare, targeting energy networks, supply chains, power grids, tourist facilities, railways and water works. The effect is twofold; first enhanced expenditure to secure all these entities and two, expenditure on the affected ones if targeted. The stock markets and connected financial systems too remained vulnerable.

Realization about economic warfare has not fully penetrated India's security sensitivity although the understanding of economics is highly developed. There is a need for greater academic investigation of this subject especially by various high profile business schools in the

country in conjunction with various strategic think tanks, the National Defence College and the National Security Council.

Education

A nation can achieve national security through the instrument of education. This is believed by all nations to be an instrument for national development and transformation. Education is seen as a veritable means of bringing about socio-cultural, political and economic growth and these foster national security. All over the world, education is viewed as the greatest instrument of change. The achievement of a scientific temper, creation of research and development, development of strategic culture, maintenance of social harmony, an egalitarian outlook and a general environment of national happiness can largely be created by providing the best education to the people. Devoid of such education a nation's international standing, reputation of its people and even its attractiveness as a centre for tourism are all adversely affected. While an adversary may be unable to use this domain as an instrument to weaken a nation it is the nation itself which becomes its own enemy if it does not prioritize education in a comprehensive manner. Education policy needs to be reviewed from time to time due to new developments in science, economics and management. The necessity to create the means to absorb the highly educated has to be kept in mind as otherwise brain drain is the automatic result. Building world class institutions and inviting foreign investment in this field will always help a nation to evolve and enhance its education and human security.

India has some high class educational institutions which must retain the freedom to pursue their work in conjunction with various international institutions. Globalization has flattened the world and best practices are available for incorporation into our model too. National pride, authentic history which promotes social harmony in a diverse nation and the necessity for tolerance and plurality of belief are essential aspects to be included in the curriculum at all levels. The academic community must robustly interact with all other domains especially now that think tank culture has entered India in a fairly big way.

The recent issue regarding education through virtual means during the pandemic related lockdown has generated much debate on thus far unrealized aspects. Discrimination due to non-availability of electronic devices among poorer segments has led to expression of concern. This same concern must be carried forward for more equitable opportunities post the pandemic so that the best talent emerges and discrimination reduces drastically.

Miscellaneous

There are numerous domains which contribute towards non-traditional threats as explained at the outset of this essay. Only a selected few have been analyzed in detail. We may include technology deficit and technology denial, narcotics and contraband, energy security as a subset of economic security, and space among many others. The security of space is going to be one of the more important domains of the future as the world is going to be increasingly dependent on satellite communication and remote sensing for defence, and climate related early warning for disaster management and agriculture needs.

National security in India continues to receive short shrift when it comes to non-traditional domains. Traditional threats involving conventional and sub conventional domains draw all attention because of the issues concerning the border, and internal security related areas such as J&K, the Red Corridor and the North East. It will need a push from the various strategic think tanks, faculties of military training institutions and university departments linked with international relations and defence studies to give non-traditional threats their place in the threat matrix. India can ill afford to live with a truncated understanding of National Security.

***Lt Gen Syed Ata Hasnain,** PVSM, UYSM, AVSM, SM, VSM (Retd) is a former 15 Corps commander

PREPAREDNESS FOR JOINT WARFIGHTING – HIGHER DEFENCE ORGANISATIONS, DOCTRINES AND CIVIL MILITARY FUSION

Shri R Chandrashekhar*

"The Armed Forces must be fully joint: doctrinally, institutionally organisationally, intellectually and technically because cyber war will be to the 21st century what the blitzkrieg was to the 20th century" –

General VP Malik, PVSM, AVSM (Retd)

Abstract

The creation of the appointment of CDS and of the Department of Military Affairs within the Ministry of Defence are significant steps. Foremost, is the CDS being appointed as ex-officio Secretary of the DMA, which for the very first time since 1952 places the edifice of management of the Armed Forces in the charge of a Military Officer in uniform. Second, it is a facilitating arrangement towards the eventual intent to set up Joint and Integrated Commands, which would need several calibrated changes being made towards orienting the existing organisational structure to meet the needs of these future structures.

These changes that would need a close, deliberate and a real-time understanding of threats the nation faces, our own operational capabilities and how these be recast and enhanced to best match the requirement of India's security. The pitfalls in leaving such a critical aspect to be settled through traditional bureaucratic procedures are obvious.

The eventual aim being setting up of the Integrated / Joint Commands, there are significant issues that come to fore. On the one side, there are issues 'internal' to the military – such as the extent to which the CDS has been empowered to meet the objective, adequacy or otherwise of stipulated timelines, the command and control of these future commands.

There are also, on the other hand, larger issues such as the structure of the national security decision-making apparatus, the association and participation of the military therein, not just at the stage of decision-making but through the course of developing options.

Future warfighting has hitherto unknown 'hybrid' dimensions that can target the very heartland of the nation – its economy and infrastructure and would need to be fought between nations, with all their assets and capabilities, not just by the military alone but also involve other Departments of the Government and even the private sector.

The need for all stakeholders in such an extended battlefield to be aware of impending threats and their respective roles in combating these cannot be overstated. In this context, there are pertinent lessons to learn from the Chinese model of such a broader 'Military Civil Fusion' which we can consider to bring into our own systems to raise national security to be a truly national endeavour.

There is no gainsaying the creation of the appointment of the Chief of Defence Staff (CDS) and the Department of Military Affairs (DMA), created as a new vertical within the Ministry of Defence, have redefined Civil Military Relations.

Besides his functions as Military Advisor to the Raksha Mantri and as Permanent Chairman of the Chiefs of Staff Committee, the CDS has is ex-officio Secretary of the DMA, thereby bringing an Armed Forces Officer into the apex structure of government for the very first time since 1952, when the "Organisation, Functions, Powers and Procedure of Defence Headquarters, 1952" under which Services HQ made 'Attached Offices' to the Department of Defence.

Equally momentous is that in follow-up, the Government have approved appointment of Military officials to positions in the Ministry of Defence, opening the prospect of their being included in the Central Staffing scheme and to hold even more positions, not only in other Departments of the Ministry of Defence and other Ministries of the Government of India.

Political Direction and Guidance

The rationale for these defining decisions and the strong political intention underlying them is best gauged from the following excerpts from the Hon'ble Prime Minister's address to the nation on Independence Day 2019:-

> *"…. The world is changing today, the scope of war is changing, the nature of war is changing. It is becoming technology driven; in the circumstances India too should not have a fragmented approach…"*
>
> *"Our entire military power will have to work in unison and move forward… things cannot move smoothly if anyone from the Navy, Army and Air Force is a step ahead from the other two forces, while the other two are lagging behind. All the three should move simultaneously at the same pace."*
>
> *….. today we have decided that we will now have a Chief of Defence Staff- CDS and after formation of this post all the three forces will get effective leadership at the top level".*

Three aspects that clearly stand out from these excerpts are:-

(a) Acknowledgement that the (then) approach was 'fragmented'.

(b) Need for the three Services to 'march in step' with good coordination, which should be in line with the changing war and security environment in the world.

(c) An expectation that 'the three forces will get an effective leadership at the top level'.

Significantly, the creation of the DMA finds no mention in that address of the Hon'ble Prime Minister and it could be that step has been taken due to a realisation that emerged in the course of drawing up the role and responsibilities of the CDS that for him to execute the mandate placed on him, it would also be required for him to be adequately empowered.

Pith and Substance of the Approvals

The Notifications spelled out the CDS' functions as Permanent Chairman COSC to be to administer tri-services organisations, including tri services agencies/ organisations/ commands related to Cyber and Space; Member of Defence Acquisition Council chaired by Raksha Mantri and Defence Planning Committee chaired by NSA, Military Adviser to the Nuclear Command Authority with his role being to bring about jointness in operation, logistics, transport, training, support services, communications, repairs and maintenance, etc of the three Services.

The CDS is also to ensure optimal utilisation of infrastructure and rationalise it through jointness among the services, implement Five-Year Defence Capital Acquisition Plan (DCAP), and Two-Year roll-on Annual Acquisition Plans (AAP), as a follow up of Integrated Capability Development Plan (ICDP) and assign inter-Services prioritisation to capital acquisition proposals based on the anticipated budget. He is to bring about reforms in the functioning of three Services aimed at augmenting combat capabilities of the Armed Forces by reducing wasteful expenditure.

Correspondingly, the mandate of the Department of Military Affairs, in addition to subjects transferred from the Department of Defence to the DMA, include the following areas:-

- Promoting jointness in procurement, training and staffing for the Services through joint planning and integration of their requirements.
- Facilitation of restructuring of Military Commands for optimal utilisation of resources by bringing about jointness in

operations, including through establishment of joint/theatre commands.

- Promoting use of indigenous equipment by the Services.

The Limiting Stipulations

The approvals however carried the following caveats/conditions:-

- The CDS will not exercise any military command, including over the three Service Chiefs.
- The three Services Chiefs is that they will continue to advise RM on matters exclusively concerning their respective Services.
- The critically significant stipulation is that these structures and systems were to be established within three years of the first CDS assuming office.

While there will always be divergent, even contrary views on how to implement a particular political decision, it is beyond the scope of anyone at the functionary level in service to intrinsically question the authority or efficacy of the decision itself. What is required of them at this stage is to put minds together to forge viable joint structures.

Range and Scope of the CDS' Authority

In the erstwhile dispensation prior to the appointment of the CDS, all issues relating to the administrative and operational control of the Armed Forces were dealt by the Ministry of Defence. The following major areas of work were transferred to the Department of Military Affairs which itself was placed under the ex-officio Secretaryship of the CDS":-

- Military Operations including CI Ops. Deployment of Forces, Border intelligence, Air Defence.
- Organisation and Manpower Planning, Pay and Allowances, Defence Services Regulations.

- Personnel Management - Postings, Promotions, Cadre Management, Complaints, Discipline etc.
- Service Conditions, Grant of PC, SSC etc., Recruitment Policy, entrance exams etc.
- Training Matters. CAT 'A' Estts, Field Firing Ranges,
- Budget Aspects, ATGs, War and Peace system of accounting,
- Procurements through Revenue route.
- Development of communication / roads.
- Provisioning / procurement of clothing (incl. spl clothing) and spl. Eqpt.
- Maintenance of Platforms – Aircraft, Ships
- War Wastage Reserves.

From the perspective of bringing about 'Integration' of the forces, important amongst these subjects are the Personnel Management - Postings, Promotions, Cadre Management, Complaints, Discipline etc. Service Conditions, Grant of PC, SSC etc., Recruitment Policy, entrance exams besides Training Matters. Substantive integration would come about only upon all these subjects coming on to a common template.

Present State of Flux

Determining the form and shape of Integrated Structures is work in progress. What is on the anvil is a tectonic transformation of structures and systems which require not just a new working ethos but also a large scale shake out from diecast mindsets that make it unrealistic to think that such transition would be pain-free.

Beyond the din of the high voltage slogan-driven narrative, at the leadership level, this is time for high professionalism and sagacity to understand contrary proposals and accept them. There would be an expected impact, even some tumult at the tactical, supported, supporting with a spill over on to the operational aspects but leadership, at all levels has to ensure that there is no compromise on strategic interests at any time.

Two guiding principles that need mention here are first, that 'geography is not joint; warfighting is' and second that 'Integration is not equivalent of sameness'. **While a deft functional understanding of the intended integration and jointness is not yet visible, it is clear that a lot of churning s indeed taking place, and happening so before rather than after the proposed structures are approved.**

The CDS in the National Security Decision-Making Architecture

While the CDS is well empowered to meet the requirements of fulfilling his mandate, and is taking the requisite strides towards accomplishing that mandate, certain areas and aspects of concern come to fore that are determinant on the how the decision-making apparatus is cast.

Higher Decision Making Apparatus

The issue that comes to fore is how the Armed Forces obtain the requisite political authority and guidance to execute their functions, whether the extent of empowerment is adequate to achieve the stated objectives. There is need to understand the structure of Higher National Security Decision making apparatus, the dynamics of its functioning and the extent to which the military, at its highest echelons is associated with and participates in the decision-making processes.

The Cabinet Committee on Security (CCS), chaired by the Prime Minister of India with the Home, Defence, External Affairs and Finance Ministers of the Union Cabinet as its members is the highest decision-making body on all matters of India's national security including defence policy and expenditure. While the National Security Advisor (NSA) is a permanent invitee to the CCS and the Secretary of the concerned Department would invariably be in waiting, the Services Chiefs are invited to be in attendance only on a 'as required' basis. **As Secretary DMA, the CDS would be in attendance in the course of deliberations on subjects pertaining to his department but is not a 'permanent invitee', nor are the Services Chiefs. This is a long-standing proposal on the part of the Defence Services for the Service Chiefs (in present**

day context the CDS as Chairman COSC to be 'permanent invitees' at CCS Meetings merits immediate acceptance.

The National Security Council (NSC), also chaired by the Prime Minister and includes all members of the CCS, the National Security Adviser and the Deputy National Security Advisor. The NSC's agenda includes issues of external and internal security, military affairs, conventional and non-conventional defence, space and high technology, counter insurgency, counter terrorism, economy and environment. The military has no representation in this tier. **If the Military is indeed to be given its due presence in the national security architecture, it is incumbent for the CDS to be a permanent invitee to the NSC**.

The Strategic Policy Group, is the first level of the NSC support structure. It is headed by the NSA and Members include the Vice Chairman NITI Aayog, Cabinet Secretary (the erstwhile Chairman), the CDS, the Services Chiefs, Governor RBI, Foreign Secretary, Secretaries for Home, Finance, Defence, Defence Production, SA to the RM, Secretary (R), Secretaries for Revenue, Atomic Energy, Space, Director IB, and the Secretary NSCS. Reps of other Mins/ Departments invited as required. The Cabinet Secretary coordinates implementation of SPG decisions by Union Mins/ Departments and State Govts. ***The CDS is member both as PC COSC and as Secretary DMA. Once Integrated Commands are set up and if the role of the CDS becomes an operational one, it needs to be ensured that the 'military' representation within the SPG at the tri-services level continues by inclusion of the VCDS as member of the SPG.***

The National Security Advisory Board (NSAB), constitutes members who are "persons of eminence" outside the Government with expertise in external security, strategic analysis, foreign affairs, defence, the armed forces, internal security, science and technology and economics. The NSAB is the Council's think-tank. **The NSAB does not have formally 'earmarked' slots for the Defence Services which would be essential for the military perspectives to be factored into deliberations. Ironically, the NSC Secretariat does not even have a**

Military vertical. Clearly time to recast the NSAB and the NSCS to enhance formal Military participation at both forums.

The Defence Planning Committee

Notified in Apr 2018 as a 'Permanent Body' under the Chairmanship of NSA To *'analyse and evaluate all relevant inputs relating to defence planning"* including National defence and security priorities, Foreign policy imperatives, Operational directives and associated requirements, Relevant strategic and security-related doctrines, Defence acquisition and infrastructure development plans including the 15-year LTIPP, Defence technology and development of the Indian defence industry and global technological advancement. Its other members are Chairman Chiefs of Staff Committee, Service Chiefs, Foreign Secretary, Defence and Expenditure Secretaries and the CISC (Member Secretary**). Importantly, the HQ IDS is the Secretariat for the DPC**. The DPC functions on a 'think tank' mode and submits is recommendations to the Raksha Mantri whereafter the proposals follow the normal Government channels of progressing for consideration and approval. **The DPC is a crucial 'all of government' body with representatives from the MEA and the Finance Ministries and can be leveraged to fortify the planning process. As the DPC caters to the requirements of the Ministry of Defence and in particular to the Armed Forces, the CDS, chairing the DPC in his capacity as Permanent Chairman Chiefs of staff Committee may in fact be a pragmatic move, especially as the Committee is already being administratively serviced by the HQ IDS.**

Centrality of the NSA

On all matters relating to National Security (with Defence Strategy as a subset) - the NSA has come to be a the 'central pivot' at doctrinal and planning levels. The NSA chairs the Strategic Policy Group, the Defence Planning Committee and is advised by and oversees the National Security Advisory Board (NSAB). He is importantly, a Member of the NSC.

In contrast, the long-standing requirement projected by the Armed Forces for a 'one on one' interaction with the PM, a 'permanent invitee' status in the CCS for Chairman COSC / Services Chiefs has not been acceded even after the appointment of the CDS. In effect, the realm of the CDS is within the zone of the 'military' as a subset of the larger 'security' canvas with the NSA at its centre. **The functional relation between the CDS, the Services Chiefs and the NSA needs to be clearly stated and understood.**

Doctrines – Facilitators or an Enigma

Military doctrines reflect *"the will and philosophy of an organisation and specifies premises and convictions to sustain its endeavours"* and provide a set of principles that guide the Armed Forces to function in support of our National Security Objectives.

It is from these generally accepted but not formally propounded National Security Objectives that India's National Military Objectives would flow. While these too have not been formally promulgated, they would broadly include prevention of war through strategic and conventional deterrence across the full spectrum of the conflict continuum; prosecute military operations to defend territorial integrity; ensure Internal Security and Stability, provide for contingencies at home and abroad to provide Humanitarian Assistance & Disaster Relief (HADR), Aid to Civil Authority and International Peacekeeping, and defence cooperation when called upon to do so.

In the context of the rapidly changing nature of warfare, kinetic and non-kinetic character of conflict and the continually changing challenges faced by the nation, there is need for the Armed Forces to remain operationally current, agile, efficient and utilise scarce resources in an optimised manner.

It is hence imperative that Doctrines, collectively and individually, provide an 'enabling' environment for functioning rather than an 'impeding' one. 'Joint' military doctrines must provide foundations for 'greater

integration and interdependence, to achieve higher inter-operability and compatibility within the Armed Forces' and must therefore be facilitators for seamless and effective bi-service or tri-service operations.

There are also Single service doctrines that are 'special to force' and seek to enhance operational efficiency within respective Forces. Doctrines, importantly, preclude or obviate finding ad hoc solutions and guidelines for carrying out operations which carry the potential to be disastrous.

All the three services have but one common aim – to either deter war or to fight and win it. A Joint Doctrine, duly accepted for adherence and compliance by the Armed Forces is inevitable, especially when there is no overarching National Security Doctrine to draw guidance from. The Kargil War is itself a suffice example for why there is need for a cogent, all-encompassing Joint Warfare doctrine.

National Security and Defence Doctrines

Democracy, ipso facto is premised on the 'will of the people' with the 'people' also being the eventual bearers of the consequences of the 'outcomes' of political decisions. Their stake in the decision-making processes and the portent of these decisions is therefore abiding. It goes without saying that people of the nation need to be kept abreast of the state of the nation's security, the nature of threats the nation faces and the 'strategic vision' of the political authority in understanding them and drawing up responses. It is therefore imperative that a 'National Security Doctrine' that that covers in realistic detail issues relating to border disputes, conventional and non-conventional threats, duly approved by the NSC, be formalised.

On the 'functional' side, the CCS must rise to play an assertive role as the final arbiter on how the Armed Forces of the nation and the various security agencies function in seamless unison. The 'traditional' irking points of inter-cadre primacy and supremacy are present day context, vestiges of an era that precedes the CDS and DMA days

when there was a deliberate intent to keep the Armed Forces at a safe distance which was done in an ambience of anonymity. It is time now to revisit this aspect, understand the on-ground dynamics and protocols on which the Armed Forces and other Agencies mutually coordinate their functions. An 'Integrated' Military Doctrine as also other single-service Doctrines should derive from this Defence Doctrine.

Likewise, decision-making on matters of security also involves a plethora of functionaries across other Departments and Ministries of the Government of India as also of State Governments. In the context of modern-day warfighting, these decisions may also require to be made at great speed, even perhaps on a 'real-time' basis. It is time to frontally address the lingering 'us vs them' approach by defining the role and responsibility of various Departments / Ministries, place the onus of responsibility of specific functionaries.

Military Civil Fusion

The Chinese construct of Military Civil Fusion (MCF) warrants a very close understanding. Unlike in India where innovations and technological progress is regular and routine in every sector other than defence to an extent that the generally 'holy cow' has come to be tec impoverished. Several schemes and steps have undoubtedly been taken by both by the Services HQ and the DRDO but these are not at 'platform' level where in fact the real techno voids exist and can only be made up be imports. INS Vikrant, recently launched for sea trials has been flaunted as a shining example of Atmanirbharta' with over 74% indigenous content. What is not stated is that the Engines installed in the carrier are GE Marine four GE LM2500 engines. Creditable, but not yet there. **China on the other hand has a robust and all-encompassing framework in which seven categories of factors shape the MCF system: catalytic, input, institutional, organizational, networks, contextual, and output factors.**

There are important lessons to draw from China's strategy to reorganise its entire edifice of Science and Technology Enterprises of that new innovations are available simultaneously to the Civil and military

sectors. Its MCF model is premised on AI being the driver for the next technology revolution and future military dominance will accrue to the country that first applies AI to next generation warfare and transition to 'Intelligent warfare'. Key technologies being targeted under MCF include quantum computing, big data, semiconductors, 5G, advanced nuclear technology, aerospace technology, and AI. The acquisition of these new technologies is being done through investments. These include investment in private industries, talent recruitment programs, directing academic and research collaboration to military gain, forced technology transfer, intelligence gathering, and outright theft. The MCF strategy allows a growing number of civilian enterprises and entities to undertake classified military R&D and weapons production, exploiting blatantly the transparent nature of the global research enterprise. Bodies like the China Scholarship Council require academic scholarship recipients to report on their overseas research to PRC diplomats.

Technologies developed and procured on the civil side are seamlessly available for development in the military. The support and sustenance for this framework derives from a 'hands on' leadership involvement, direct involvement of key state and military agencies, financial mechanisms such as hybrid state-private sector investment funds. Without doubt there would be limits to setting up such a 'framework' in a democratic country where systems work in transparency based on strict adherence and compliance to the laws of the land which includes honouring IPRs. However, within there is much space even within these limitations to bring in enabling provisions that allow sharing of technologies for application towards national security.

Present Role of the CDS – Evolving or Temporal

To revert to the role of the CDS, has the appointment been accorded the requisite positions in these decision-making apparatus of the Government to an extent that ensures 'effective and real' integration?

The answer is substantially Yes. However, harnessing the full potential of the appointment towards the larger aspect of national

security, there is far more that needs to be done. Hopefully, this too is work in progress and several consequential changes, even perhaps redefining the present role of CDS could come up once Integrated Commands are set up, **even a possible reversion of the Secretary DMA to another Military Officer or even a bureaucrat, dependent on how the Government assesses the Military's success or otherwise in managing itself.**

Conclusion

Both the bureaucracy and the military sharing the characteristic of adhering to the status quo with little propensity to throw up substantive concepts and ideas of reform on their own volition, it is really the political dispensation that needs to understand the requirements and enforce requisite changes through 'diktat'.

To visualise the creation of the DMA having come through such 'diktat' is not hard. Neither is it to expect the setting up of Integrated Commands, their control and organisational structures and aspects of territorial ambits of each to also 'happen' in a similar way.

To reiterate, time line within which to set up Integrated structures has already been stipulated by the political authority. This timeline would without doubt have been set after extensive consultation from across the Armed Forces. Also, no political authority worth its salt has stomach to rescind a project initiated with such gusto.

In many ways, the Armed Forces are on test as to whether they can indeed 'manage themselves'. The collective endeavour must be to accomplish. Yet, if it is the unanimous opinion across the military spectrum that more deliberations are required before Integrated structures are cast or that the time to make the 'grand shift' is not opportune, reverting to the political leadership for fresh directions is only logical. The justification to do so must however be embedded in justifications that go beyond those for which the Armed Forces have been advocating creation of these commands in the first place.

In doing so, the Armed Forces need to keep in mind the old adage that 'good enough is the enemy of perfection' and each shot on or off the war zone invariably has to be the very best.

To recall Gen VP Malik's terse message quoted at the beginning of this essay, that shot may well hit the heartland of India and its economy and infrastructure through cyber-attacks. The need of the hour is hence to brace up for eventualities that go beyond the battlefields as encrusted in classical thought.

Intended fruition from the bold and determined initiatives would accrue only when integration encompasses body and soul of the entire National Security apparatus. It is still a long way to get there.

***Shri R Chandrashekhar** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi

PREPAREDNESS RISKS MITIGATION - PRIORITIES FOR THE LAND FORCES

Lt Gen Dushyant Singh, PVSM, AVSM (Retd)*

"It would be fallacious to assume that a single service will dominate future warfare. Joint integrated operations across multiple domains is the way ahead."

General M. M. Naravane PVSM, AVSM, SM, VSM, ADC

Abstract

The nature of warfare is rapidly changing primarily due to rapid advances in communication, Internet of Things (IOT), automation, robotics, Artificial Intelligence and Quantum Computing technologies. The preparedness of the Land Forces will also be dictated by the nature of threat facing the country. The key drivers of this threat are and will be China, Pak, terrorist threats emanating from across the borders on either front. Due to this the nation is likely to be in a constant state of war in the grey zone. Therefore, the wars will no longer be the preserve of the military let alone a single service and the Land Vector will be one amongst the many entities that will be involved in conflict resolution or response.

Land forces must adapt to function in an integrated manner in a multi domain environment. Non - contact warfare with primacy of fire power and disruptive technologies will dictate the way land forces will have to structure, prepare and fight. Human Resources will need to be oriented to fight in tech heavy environment but at the same time taking

care to exploit the advantages offered by the Himalayan terrain and Weather conditions against China and use of disruptive technologies such as swarm drones, long-range vectors and high mobility forces in HAA/SHAA terrain in consort with Air Forces. The focus of land forces must be prioritised towards threat number 1 that is the northern borders. A 2-2 or 3-1 orientation of Strike Elements is highly recommended.

China is expanding its influence in the IOR to strangle India, accordingly the Naval Forces in synergy with Air Force and Land Forces need to restructure their response. Land Forces can contribute immensely in this endeavour by raising a small marine force. This force could be the last nautical mile entity to secure a maritime operations to defend our unheld Island territories and expeditionary operations in times of humanitarian assistance, evacuation of our diaspora and securing national interest.

There is a need to work towards creation of tri service entities such as cyber command, Special Forces command, Information Operations Agency We may consider upgrading the ADG PI to a tri — service organisation. The land forces need to assist the raising of tri-service theatre commands and tri - service functional commands in the best possible manner without destabilising itself in the transitory phase.

Internal Security does lead to diversion of effort from the primary task of the military especially the land forces. It is highly recommended that the Land Forces commitment from such tasks should be minimised and restricted to disturbances along the Borders such as LC, LAC and Myanmar. It would be even more advisable to place the Central Armed Police Forces such as the ITBP and SSB under command the Army along these borders for better response and avoid Pangang Tso from reoccurring. Other Desired Capabilities for the Land Forces in the current and foreseeable future pertain to greater synergy in intelligence gathering, upgradation of the Special Forces to deal with grey zone threats, electronic warfare, air defence, logistics, command and control, manoeuvre, defence diplomacy and strategic mobility. Land Forces need to master niche technology and exploit unmanned systems to deliver

maximum TNT on the enemy target coupled with deft moves in the grey zone to emerge victorious in future wars across the entire spectrum.

Introduction

Given the ever evolving nature of warfare brought about by the magnitude of technological developments in the military affairs, mounting cost of waging conventional war in terms of lives and physical destruction, wars have become option of last resort . Also due to existential consequences of a nuclear conflict, nuclear wars are unlikely to take place. Quite simply put, the Clausewitz's theory of war comprising the famous trinity "People - Army - Government" is gradually losing its shine to the subsequent thinking of Clausewitz in his famous work "On War" where he started laying "more and more emphasis on people's war and co-operation between the regular army and militia or partisan forces, or citizen soldiers, as one possible——sometimes the only——method of defence."[1] The countries are gradually shifting to this form of warfare which is now commonly referred to as the Hybrid, Proxy or Grey Zone Warfare. However, this does not imply that the importance of conventional military is diminishing. It continues to remain relevant even today and will remain so in foreseeable future. Military power acts as an underwriter for deterring a conventional war against an adversary should the non-military means to secure strategic advantage in a geopolitical contest spiral out of control. The implications are that wars will become more and more complex and challenging with coexistence of non-military and military content in the ratio of 4:1 as prophesied by General Gerasimov, the Chief of General Staff of the Russian Armed Forces.[2] It implies that the wars will no longer be the preserve of the military let alone a single service. The Land Vector will be one amongst the many entities that will

1 Handel, Michael I. (1986). Clausewitz and Modern Strategy. Psychology Press. p. 71.

2 Russian version by General Valery Gerasimov, "The Value of Science Is in the Foresight" Voyenno-Promysh-lennyy Kurier online, 26 February 2013, http://vpk-news.ru/articles/14632 For English version see For English version see, Sivitski Arseni, "The Belarus-Russia conflict through the lens of the Gerasimov Doctrine," Belarus Digest, 06 March 2017, https://belarusdigest.com/story/the-belarus-russia-conflict-through-the-lens-of-the-gerasimov-doctrine/ (accessed on 18 April 2021)

be involved in conflict resolution or response. If this be so how should the land forces prepare themselves? Answer to this question and related aspects will be the focus of this paper.

Aim

To suggest measures for enhancing the defence preparedness of the land forces to operate in an integrated manner with other vectors of war fighting across the entire spectrum, emerge victorious and mitigate the risks of waging such conflicts.

Current and Future Conventional Security Threats to India

Collusion between China and Pakistan stems from the Pakistani desire to settle scores with India and the Chinese interest to settle boundary dispute on its own terms coupled with mutual interest in the China Pakistan Economic Corridor (CPEC). While China being the stronger power will not like to be seen as overtly seeking collusion, Pakistan jumping into the milieu opportunistically in the event of a Sino - Indian conflict is a distinct possibility. Sino - Pak nexus may include enhanced military deployment along the borders, economic coercion, increased maritime activity in the Indian Ocean Region (IOR) and in the worst case threaten military action to stretch the security effort of India.

China is the primary security threat to India. The ongoing confrontation between India and China has dashed the hope of revival of cooperation that got kindled following the informal Wuhan[3] and the Mamallapuram summit meetings[4] between Modi and Xi Jinping. The long term intention of China remains subjugation of India by targeting its national will. In the process it is likely to address our strategic vulnerabilities including

3 Shruti Godbole. "Wuhan Summit: An important signal of intent by India and China," May 23, 2018, Brookings, https://www.brookings.edu/blog/up-front/2018/05/23/wuhan-summit-an-important-signal-of-intent-by-india-and-china/. May 11, 2021.

4 V. Nivedita. "Modi-Xi informal summit: Key takeaways." October 15, 2019, the HindustanBusinessline.Com, https://www.thehindubusinessline.com/news/modi-xi-informal-summit-key-takeaways/article29680297.ece . May 11, 2021.

our nuclear assets and missiles, undertake offensive along our northern frontiers for which it has earmarked between 40 to 45 Combined Arms Brigades (CAB) including three to four PLA, Airborne CABs.[5] It has cut down its land forces, increased the mechanised content, and made them firepower heavy. It is modernising the Navy at a frantic pace. At the structural level it has transformed its military into Theatre Commands with five theatre commands covering the entire country.[6] India faces the Western Theatre Command. China already has two carrier task forces and is soon going to add the third one in its arsenal.[7] However, the Chinese are unlikely to start a major conflict in the short to medium term till they are not assured of a sure win. Reasons are: a) slowing down of the economy because of COVID; b) tardy progress of CPEC and BRI upon which hinges the mega dream of Xi Jinping to become the economic powerhouse of the world; and c) the loss of face due to the resolute and determined response of India during the Dokalam and Galwan crises. China will continue to play around in the grey zone with transgressions along the Northern Borders, undertake cyber-attacks and conduct information wars in the short term.

Pakistan's economic health, threat of being black listed by the FATF and the worsening internal situation discourages it from waging a conventional war with India but it will continue to wage proxy war in J&K. However, if pushed to the wall or if it gets an opportunity in the event of a collusive opportunity, conventional operations cannot be ruled out. Pakistan will maintain a dissuasive conventional capability along the land frontiers with ability to exploit an opportunity in the event of a collusive war and deploy submarines in the IOR.

5 Authors assessment based on experience and the total force level available with PLA in the open source domain.

6 Kenneth W. Allen, Dennis J. Blasko, John F. Corbett, Jr. "Updated - The PLA's New Organisational Structure: What is Known, Unknown and Speculation, Parts 1 & 2." Jamestown.org. https://jamestown.org/wp-content/uploads/2016/02/Updated_The_PLA_s_New_Organizational_Structure_-_What_is_Known__Unknown_and_Speculation_Parts_1_and_2.pdf . May 12, 2021. P.5-7.

7 "Comparison of China and India Military Strength 2021." Global Firepower. Com, https://www.globalfirepower.com/countries-comparison-detail.php?country1=china&country2=india. May 11, 2021.

Grey Zone Threats / Unconventional Threats

Internal threat in the country is manifesting in the form of religious extremism cum ethnonationalism in J&K. The military threat in the state manifests in the form of infiltration across the Line of Control (LC), attacks against the Security Forces, attacks against innocent civilians and host of grey zone threats. Similarly in the NE, although the militancy is going down, but peace eludes us. The now famous draft Naga Accord remains in a limbo. LWE is even bigger threat to the country. Attack on the CRPF in Bijapur and Dantewada are few examples. In fact the LWE Militant Group is fifth most virulent terror group in the world way ahead of the LeT, JeM, AQ, etc. See Table 1.[8] Further, "Since 1999, to 15 November 2014, 12,353 persons have been killed in Left Wing Extremist violence in India."[9]

Cyber Attacks by China have become a common occurrence. Report of the US based Insikt Group clearly establishes this assessment . "It observed a large increase in suspected targeted intrusion activity against Indian organisations from Chinese state-sponsored groups. From mid-2020 onwards, ten distinct Indian power sector organisations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets… Other targets identified included two Indian seaports."

Table 1: Top Five Perpetrators of Terrorism

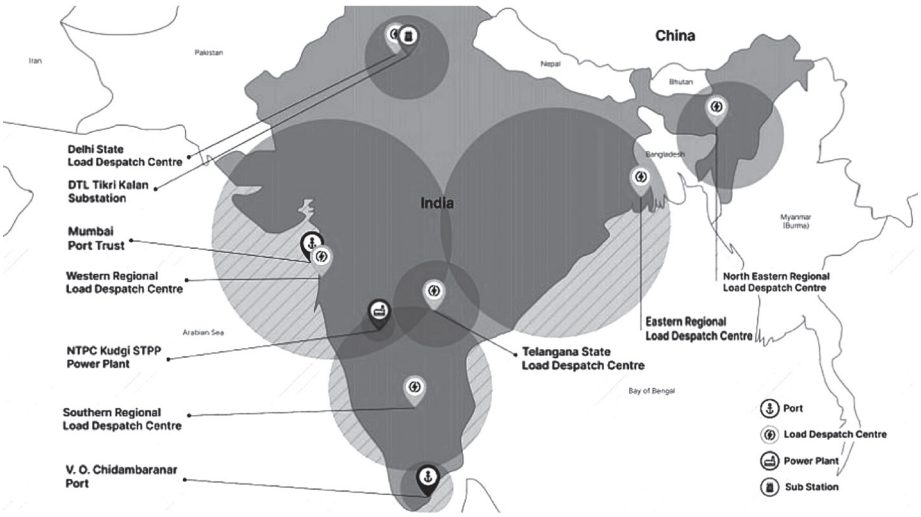
Perpetrator Group	Total Attacks		Total Deaths*		Total Injured*		Kidnapped / Hostages	
	2019	2018	2019	2018	2019	2018	2019	2018
Taliban	1034	987	5094	6214	4984	4064	550	1285

8 Global Terrorism Data Base, July 2020, https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf (accessed on 25 April 2020)

9 Ajai Sahini. Bullet Holes in Village Walls. October, 2015. Routledge Handbooks Online. https://www.routledgehandbooks.com/doi/10.4324/9781315674742.ch18#sec18_2 . Abstract. May 12, 2019.

Houthi extremists (Ansar Allah)	446	277	436	258	609	260	394	410
Islamic State of Iraq and the Levant (ISIL)**	343	560	954	1601	1319	1423	41	970
Boko Haram	245	171	1069	732	378	589	304	376
Maoists/ Communist Party of India - Maoist (CPI - Maoist)	226	247	136	175	87	154	94	135

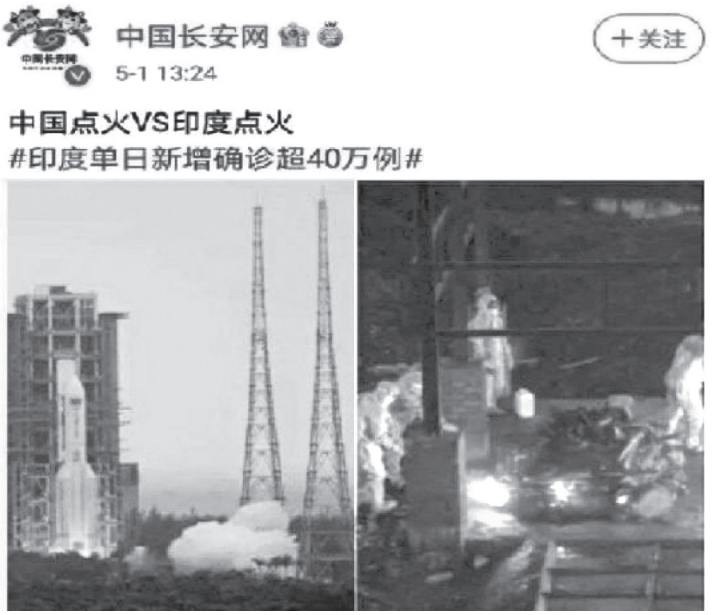
Figure 1



Given such a capability, PLA would be able to paralyse our defence systems, airports and other important military bases.

Information Warfare is also becoming a preferred tool of statecraft. India is constantly targeted by our adversaries. Global Times, a Chinese Communist Party paper has been working overtime to spread rumours and fake news following the Dokalam and the Galwan incidents. The recent tweet in Chinese media by CCP showing the picture of launch of a Chinese Rocket alongside burning funeral pyres

Figure 2



of COVID cases is a blatant example of information war. See figure 2. Pakistan too has left no stone unturned to internationalise the Kashmir issue be it in the UN or other International Bodies. Likewise, the International Terror groups such as the Willayat - e - Hind (ISIS India Branch) and AQIS have been indulging in information operations against the country taking advantage of the recent unrests following the NRC and CAA agitations. Such actions also have an adverse impact on the morale and motivation of our troops.

RECOMMENDATIONS FOR BETTER DEFENCE PREPAREDNESS AND RISK MITIGATION

Land Forces Capability to Enable Smooth Transition to Integrated Theatre Commands

Recently the Army Chief gave a statement that it will be fallacious to think that any single service would be able to deal with the future military challenges. He hinted at integrated war fighting as one of the important

factors in winning the current and future wars.[10] Have we integrated our armed forces, afraid not? While some entities and structures have been raised such as the office of the CDS but is that enough? Where are the Geographical commands? Where are the much needed resource for A&N Command 21 years after its foundation? Future demands military transition into Theatre Commands and Joint Functional commands. To achieve this the Land Forces need to reorient and reorganise themselves to enable smooth transition to integrated structures and war fighting. Salient issues are discussed below.

High-tech Capability of Land Forces (LF) needs a Quantum Jump. China has heavily invested in Artificial Intelligence(AI) and robotics. On the other hand Indian research on AI and other niche technologies such as unmanned systems is in a nascent stage. The private equity investments in Indian AI companies in 2019 were between 900 million to $1.2 billion. This investment is way less than the US and China ($25 billion and $5 billion respectively in 2019), but the good news is that India nearly tripled its AI investment in 2019.[11] Capability in the areas of AI, robotics, cyber security and employment of armed drones, UAVs, navigation and guidance systems, sensor shooter links are recommended to be taken up on top priority and personally driven by the Chief.

Space Based Defence Capability of the Armed Forces especially the Army needs to be enhanced. While, the IAF has outlined its space vision in detail, the Land Warfare doctrine just has a brief mention about it. There are 14 satellites that are being used for military purposes. Navy and AF have a dedicated satellite GSAT 7 and GSAT 7A. Although the Indian Army is also likely to get a dedicated satellite it needs to improve the exploitation of space based resources.[12] Accordingly

10 Barnwal J. Ed. "COAS Interview with SP". SP's Land Forces December 2020-January 2021. Volume 17 No. 6. https://spslandforces.com/ebook/75062020.pdf . Accessed on May 19, 2021.

11 Raibagi K. "AI Ecosystem: Where Does India Stand Compared To The US & China." April 19, 2021. https://analyticsindiamag.com/ai-ecosystem-where-does-india-stand-compared-to-the-us-china/ . May 14, 2021.

12 Sanjay B. Maharaj. "India's Military Satellite Options." www. geoplitics.in. January 2020. https://reader.magzter.com/reader/ig8h88vi6veydpppwm6zr39842816575909/398428#page/18 May 15, 2021.

following is recommended: (a) Operationalisation of Indian Regional Navigation Satellite System (IRNSS) to overcome our vulnerability of being dependent on a foreign navigation system NAVSTAR/GPS. (b) Fast track the completion of our Defence Communication Network to ensure net centric warfare. (c) Early Warning Capability to detect missile attacks. For this there may be a need to have dedicated military satellites. (d) Dedicated military satellites are also needed for SIGINT and COMINT. (e) we need to reduce revisit time, secure data transmission, quick processing of the military images upto the field formation level.[13]

Cyber capability too needs an urgent attention. Our ability to defend against cyber attacks is questionable. There is a need to raise a Cyber Command with strong components from each service which should control and conduct military defensive as well as offensive cyber operations. Till the tri service Defence Cyber Agency matures and transforms into a Command Land Forces must develop an effective defensive as well as offensive cyber capability.

Information Dominance cannot be over emphasised. Such operations have to be properly integrated with the national strategic level guidelines. ADGPI is currently doing a fine job but it is no match to the IW agencies of our adversaries. ADGPI must rapidly enhance its capabilities and take the shape of a tri service entity with expanded role. Land Forces could take the lead in this capability development.

Expeditionary Capability continues to remain restricted to HADR. However there is a need to be prepared to undertake low level military operations of the Maldives type to safe guard our national interests especially in our neighbourhood. An important component of this capability is the need for marine component. This must be conceptualised with a brigade strength force under the Indian Navy for future envisaged role in the Indian Ocean Region (IOR), as regional net security contributor. The force should be capable of multi-mode insertion and adaptability to wide

13 Ramesh Krishnan. Mission ASAT: Why India needs a satellite killer. Business Today, March 28, 2019. https://www.businesstoday.in/opinion/perspective/mission-asat-why-india-needs-a-satellite-killer/story/331884.html . May 15. 2021.

spectrums of conflict. It must have organic point AD capability. Finally, it must be have to capability to operate with other two services including international defence forces.

Joint Training is an area that is extremely important from the perspective of fighting in an integrated battlefield environment which entails functioning under joint structures. Therefore, ARTRAC must inject greater joint content in various courses and training programmes. HC and DSSC need a relook for greater jointness. The NDC (National Defence College) must start laying more stress on strategic games. It may also be a good idea to have a mega joint APPA - NDC Strategic War-game conducted by either the USI or VIF or the ORF to empower future leaders from various domains to respond to security situations with a whole of a nation approach.

Land Forces Specific Capabilities

Infantry is the edifice of land forces. The new normal of warfare created due to tsunami in technological development demands that all the components of land forces especially infantry is capable of surviving modern wars yet remain mobile and lethal. This necessitates transformational doctrinal changes and reorganisation. Suggested doctrinal framework should comprise firstly, an offensive outlook/capability to successfully prosecute conventional and unconventional operations across all spectrums of conflict and frontiers. Secondly, improve survivability, lethality and mobility for undertaking operations at the tactical and operational levels. Thirdly, force preservation and force projection are vital battle winning factors in informationalised environment for enhanced lethality, precision and range. Accordingly, the desired capability for the infantry should be first, a future ready soldier. The soldier with his weapon and equipment will remain the core element and at the centre of land warfare be it conventional, unconventional or Military Operations Other Than War (MOOTW). Second, the IBG concept suitably customised to operate in Mountains and Plains will need to be gone into. This will facilitate the current and future demands of multi domain warfare. Third, force Preservation/ Protection and Enhanced Standoff Lethality will be of prime importance for effect based operations

under informationalised conditions. Threat and terrain based tailor-made anti-tank and Air Defence capabilities at stand-off ranges would be required. Force preservation by way of protection, both during static and mobile operations, require inclusion in the structural construct. Fourth, and possibly the most crucial is the C^4I^2SR and Battlefield Transparency under intense EW environment and systems to facilitate 'Mission Oriented' command structure. And finally, mobility, deployability and sustainability will be the driving factors for reorganisation. The infantry modernisation must focus on Task and theatre specific organisation in combined arms and multi-domain environment. Also every soldier must transform into a Sensor (S3) and shooter as well. Keeping all these in mind the structural concept of Infantry warrants threat and terrain based reorganisation into Mechanisation, Motorisation and Standard Infantry, Airborne, to transform Infantry. Further, there is also a need for Tailor-made Specialised Forces such as Scouts, special light infantry battalions.

Mechanised Forces will be driven by technology in future wars. Hence, commanders at all levels should be able to imbibe technological tools into their war fighting strategy and operational and tactical plans. Despite technological advantages, ground still remains the most important factor both on the Northern as well as the Western front. Mechanised forces also have to survive in technologically advanced future war environment otherwise the degradation of the mechanised forces will make the task of the adversary easier for launching his offensive plans — both along the northern and the Western front. Hence, it is imperative that counter RPA systems are inducted which gave area protection as well as protection to individual tanks oblique ICV. Induction of light tanks in northern borders and high-altitude is also imperative since the lesser weight offers multiple benefits like the power to weight ratio which allows scaling high passes and mountain heights, less weight also facilitates air transportability and inter sector move. With technological advancements Light Tank would be comparable in firepower with medium tank and as also with active protection systems and soft skill measures will enhance its efficacy. The counter RPA systems can be integrated into the light tank and made more ISR enabled with ability to control UAVs.

Air Defence have become All Weather (AW) and multi-platform centric with focus shifting towards Remotely Piloted Systems (RPS). Future AD threat can be visualised as accurate delivery of a large number of guided munitions either through manned or unmanned platforms to inundate a space segment in short time frame to achieve Favourable Air Situation (FAS). Hence it will need a variety of weapons to engage the threat. No single system can counter the RPF threat completely. However guns combined with multiple detector including acoustic electro-optic / IR, micro Doppler radar, RF and visual sensors can affordably be used to detect track and engage RPS. High energy lasers are another viable options. Capability development should address firstly, establishment of an integrated early warning in conjunction with assets of all services and civilian resources. Second, the focus to remain on countering 5th generation aircrafts and SSL with modern technologies. Third, there is a need to create capability inherent to weapon systems to pick up and engage small size target such as RPS, UCAVs so as to reduce shooter to sensor time. Fourth, minimum three layer of AD cover to be planned for critical assets with a mix of weapon system. Fifth, closed in stage weapons or terminal AD system to be capable of protecting the assets from Rockets, arty, and motors also for example the Iron Dome System. Sixth, auto target designation to the most suitable weapon system should be built in to the C&R system. Further, placing Air Defence under the command of land formations and units has always been debated given the challenge to manage the airspace where AF is the major player. However, AD cover in the TBA is also of utmost importance. Accordingly it is felt that AD components in terms of Smart Guns and Smart Missiles must continue to remain with proposed IBGs and Pivot as well as Strike Corps be it for the HAA, Mountainous, plains or desert sectors. The systems should be portable and present a small signature especially for the Super HAA and HAA. It should be capable of operating through EW environment. As regards coordination, the concept should be decentralised and distributed responsibility and centralised system of sharing information of air picture through a foolproof interoperable communication network and C&R Structure.

Aviation Support is the future of warfare, no doubt that Air Force is the primary service to manage air support but it has been experienced that given the commitments of the AF more often than not the TBA gets ignored. To fill the gap and to avoid the delay in shooter — sensor link an effective aviation arm is a must for reconnaissance, surveillance, close fire support and logistics requirements. The procurement of Apaches will help speed up the mechanised formations especially in the plains and the desert sector. Its utility in SHAA, HAA and mountainous regions is limited due to ceiling limits and bulk. For the mountains the LCH (Light Combat Helicopters) units are ideal and should be increased in numbers along our Northern Borders. As far as UAVs, UCAVs, drones and RPAs are concerned ideal would be that unmanned UAVs be placed under the Arty. However, given the way these birds were being handled and crashes taking place these assets would be best utilised if placed under the Aviation. As regards making the Shooter and Sensor loop faster the General Staff has to configure effective communication and command and control network to make them effective. In any case the control always rests with the General Staff. There may be a need to create a Manned, Unmanned Teams to effectively utilise the RPA/UAVs/UCAVs/. Effective communication and C& R is key to its success. As regards future capability development is concerned the need will be to focus on lethality and accuracy of firepower systems, night capability including operating in bad weather conditions and finally the survivability both physical and digital.

Long Range Fires capability also lacks adequate punch. As has been proved in the Kargil war and in the recent Armenian - Azerbaijan conflict that unless long range fires are delivered along with air power on the enemy defences including targets in the Tactical Battle Area, victory will be hard to come by. As part of the modernisation drive in the FY 2020-21, Six Pinaka Regiments are under procurement. However, is that enough to succeed on the future battle field? Many defence experts feel and rightly so that given India’s long frontier with China, Pakistan and the need to defend Island territories we require a far greater number of Pinaka Regiments. As per earlier estimates of few years back when

the Chinese threat was much less than today, 22 Pinaka Regiments were considered essential for defence of the country. Now when the threat has increased and become more serious we have reduced the requirement to only 10.[14] This defies logic. We need to exploit this weapon for defence along our northern borders especially in the light of the fact that the Chinese have deployed 280 Km AR 3, the PHL - 03 MRL with 12 launch tubes for 300 mm rockets (range 130 - 160 km) or the standard A-100 rocket launchers similar to the Russian Smerch.[15] Hence, it is recommended that the Pinaka regiments must be enhanced to a minimum of 26 from the currently planned 10 Regiments. In addition, other long range heavy weapon systems should also be inducted in a prioritised manner.

Signal Support needs to be rephrased as Digital Electromagnetic Spectrum Support. As part of risk mitigation measures some of the suggested measures are firstly, there is a need to have proper Technological component in the newly created IBGs in the form of Electromagnetic Support Organisation. Secondly, there is a need to spread technological awareness amongst the combat arms especially the infantry. It is a known fact that technology in today's world is all pervasive yet while appreciating an operational and tactical situation. As we discuss ground, relative strength and time and space it is now mandatory to include Technology as the fourth Sub Head of appreciation before finalising an operational plan. Thirdly, formats of appreciation, operational instructions and directives must have a comprehensive examination of technological factors. Fourthly while we do have components dealing with providing communication, communication denial measures are still very weak or non — existent. Fifthly, net centricity needs improvement on a war footing. Our sharing of information, intelligence and operational inputs is very tardy and slow especially lateral between two IBGs and Divisions. Sixthly, while we still have a well-developed communication infrastructure to share external intelligence amongst various entities of

14 Lt. Gen. P. Ravi Shankar. "Match Chinese MRLs with Pink." India Today Insight. April 22, 2021. https://www.indiatoday.com/emag . May 14, 2021

15 ibid.

the Armed Forces it is still archaic as far as sharing of internal intelligence between SMACs and MACs are concerned. Technologically we need to focus on five year upgrades of our electronic systems as obsolescence rate in electronic domain is very high. In the long term we need to build communication, communication denial systems using the 5G, Big Data, and Artificial Intelligence technology. As far as possible these should be developed indigenously given the sensitive nature of such system.

Engineering Support in the given operating environment needs to focus on enhancing mobility of own forces, countering the mobility of enemy and enhancing the survivability of our combat elements. As part of mobility enhancement we need to look for mechanically launched bridges, mechanic launched aerial cable ways of 1 to 3 km, high capacity dozers and JCBs and innovative use of existing equipment such as PMP/PMS bridges to make shunts around land extension into lakes and rivers. For example we can make shunts around the finger areas (Finger 3 to 4) in Pangang Tso Lake. Similarly as part of countering enemy mobility, we could look at vehicle based mine scattering system in mountainous terrain on an urgent basis. Similarly, we need to go in for man packed mine scattering systems and innovative use of combined teams comprising of mechanised elements, infantry anti-tank weapons/ missile detachments, and engineer assault teams (for constructing operational tracks) to fight the battle of delay lines and channelising the enemy into to killing zones. For survivability, we need to go in for tunnelled storage, CDLs for storage of water and supplies and IR lights for Helipad markings etc. From a futuristic perspective, we need to go in for, rapid erectable shelters, heavy duty excavators-track and wheeled, AI based mine detection and destruction systems, water purification equipment and high head water pumps.

M**ilitary Infrastructure** along the Northern Borders still remains short of the requirement. As per open source report besides the ongoing projects which include the construction of 3,323 km roads along the boundary with China, the Ministry of Defence is working on additional 104 roads (around 6,700 km) along the Line of Actual Control (LAC) in Ladakh,

Himachal Pradesh, Sikkim, Uttarakhand and Arunachal Pradesh.[16] This momentum must continue if India wants to secure itself against a Chinese misadventure.

Airborne Forces of the Indian Armed Forces have fundamental airborne infrastructure and airlift capability in the form of Independent Para Brigade and strategic air-lift squadrons of the Indian Air Force, which at the moment are sufficient and can be augmented in future, if required. However, we need to work towards providing them with all terrain mobility and protection.

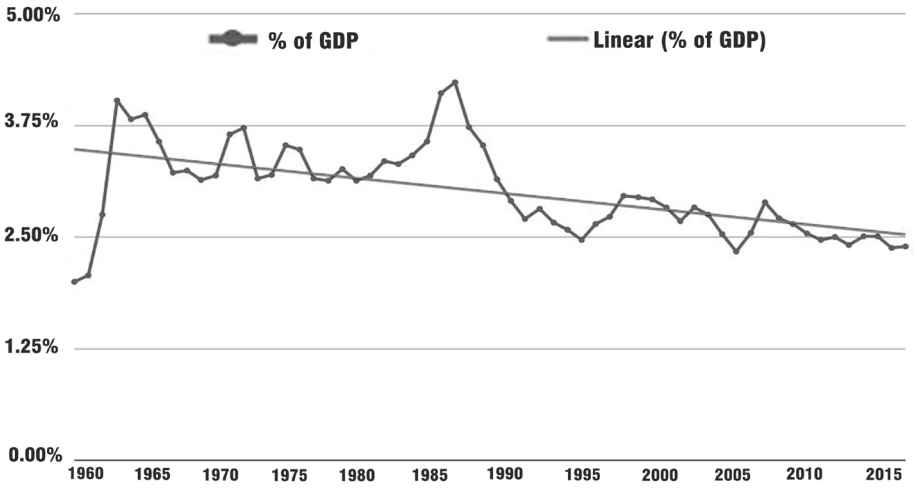
Unconventional Operational Preparedness to respond to terrorist threats in the valley and elsewhere in the country including the LWE has to continue. Ideally internal security tasks are best left to the CPAF but due to the presence of external dimension and proxy war the J&K sector, it should continue to remain under the Indian Army till these disputes are resolved. As and when the proposed Western Theatre command is raised the Corps could be placed under the proposed Western Theatre Command for conventional operations. There is also a recurring demand to deploy the army in LWE. But unless an internal security situation manifests along an international border **t**hat too with a cross border content of a serious nature, employment of the armed forces in IS situation should be avoided.

Table 2 : Table Showing Details of Capital Expenditure of Revenue and capital expenditure of Army, Navy and Air Force in 2020-21

	Army	Navy	Air Force
Revenue Expenditure (in Rs cr)	146941	22935	29963
Capital Expenditure (in Rs cr)	32474	26688	43282
Total (in Rs cr)	179415	49623	73245

16 Eurasian Times Desk. “India-China Border Row: India Continues To Upgrade Border Infrastructure As Chinese PLA Looks To Pre-Empt India.” May 4, 2021. https://eurasiantimes.com/india-continues-upgrading-border-infrastructure-amid-chinese-challenges-in-himalayas/ . May 16, 2021.

Figure 3 : Defence Expenditure as Percentage of GDP



Revenue Expenditure as % of Total	82%	46%	41%
Capital Expenditure as % of Total	18%	54%	59%

Integrated Border Management capability. CPAF (ITBP and SSB along the Chinese border and BSF in the IB Sector of J&K) units are deployed to manage these contentious borders. The Army also gets involved due to the possibility of a military conflict. Since the CPAF is under the MHA and the Army under the MoD proper coordination and control suffers at the functional level, leading to suboptimal response to any trans LAC/LC/IB incident.[17] Accordingly, it is recommended that CPAF be placed under the operational control of the Army along the unsettled borders.

Availability of Capital Funds for the Land Forces has always been low when compared to the other two services. Our defence budget has been episodic in planning. It shoots up during wars and conflicts like Dokalam and Galwan. See graph at Figure 2.[18] For example, the Army Budget

17 Bajwa M.S. "Chinese order of battle in Aksai Chin: What are we up against?" July 11, 2020. https://indianexpress.com/article/india/chinese-order-of-battle-in-aksai-chin-what-are-we-up-against-6500207/ . May 16, 2021. Barring mechanised elements Chinese Border Regiments are at par with PLA Infantry Units in terms of communication, leadership and equipment.

18 World Bank. https://www.macrotrends.net/countries/IND/india/military-spending-defense-budget . Accessed May 20, 2021.

for FY 2020-21 had only 18% allocation for capital expenditure.[19] See Table 2. Capital expenditure as a percentage of the defence budget has steadily fallen from a high of 36% in 2013-14 to 25% in 2018 – 19.[20] The capital budget of the Army needs to be enhanced to a minimum of 30 to 35% of the Army budget allocation.

Conclusion

Other Desired Capabilities for the Land Forces in the current and foreseeable future pertain to greater synergy in intelligence gathering, upgradation of the Special Forces to deal with grey zone threats, electronic warfare, air defence, logistics, command and control, manoeuvre, defence diplomacy and strategic mobility. These are equally important and the Indian Army is hopefully well on course to address them. While formulating our Land Warfare Capability, the Land Forces need to target modernisation in niche areas such as AI, Robotics, UAVs, Space, long range fires, air defence capabilities, creation of joint organisations for better joint war fighting, enhance Cyber, EW, Information dominance capabilities, ramp up the construction of military infra structures and usher in Joint Training so as to improve defence preparedness and mitigate risks due to conventional and grey zone threats. What clearly stands out is the side that can master niche technology and exploit unmanned systems to deliver maximum TNT on the enemy target coupled with deft moves in the grey zone will emerge victorious.

***Lt Gen Dushyant Singh,** PVSM, AVSM (Retd) is a former GOC of the prestigious Vajra Corps

19 Bhatnagar Aman. India's defence spending in 7 charts. TOI, January 30, 2021. https://timesofindia.indiatimes.com/india/indias-defence-spending-in-7-charts/articleshow/80600625.cms . Accessed May 19, 2021.

20 Lt. Gen. Dushyant Singh. "Union Budget 2021 Dashes Defence Expectations." February 18, 2021. The Daily Guardian. https://thedailyguardian.com/union-budget-2021-dashes-defence-expectations/ . May 16, 2021.

Endnotes

1 Insikt Group, Feb 28, 2021, "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions", Recorded Future, https://www.recordedfuture.com/redecho-targeting-indian-power-sector/ (accessed on 25 March 2021)

2 Karan, Pradhan . "How China-linked group RedEcho is targeting India's power grid: The Recorded Future interview10:35:46 IST", First Post, March 09, 2021. Accessed March 21, 2021. https://www.firstpost.com/india/how-china-linked-group-redecho-is-targeting-*indias-power-grid-the-recorded-future-interview-9393741.html* .

PREPAREDNESS RISKS MITIGATION – PRIORITIES FOR THE INDIAN MARITIME FORCES

Captain (IN) Kamlesh K Agnihotri (Retd)*

Abstract

India enjoys a unique geographical position in the Indian Ocean Region (IOR). As the Country seeks to leverage this spatial advantage as a regional power to secure its maritime environment for economic betterment; it faces specific challenges from two of its 'not so friendly neighbours. While the first challenge arises out of Pakistan's 'concept of maritime operations' deriving out of its ambitious maritime doctrine; the other concerns the Chinese aspirations to maintain permanent presence in the IOR. When the stated tasks of PLA Navy to "safeguard development of national economy and overseas interests" intersect with national security imperatives of the Indian Navy, the potential for conflict along with attendant risks would naturally arise. India must therefore continue with focused maritime 'Force preparedness' to mitigate risks associated with traditional conflict scenarios in its immediate maritime domain.

Introduction

India holds a predominant position in the Indian Ocean region (IOR), which itself has been progressively taking center stage on the global maritime map since the dawn of the 21st Century. This Ocean connects many States with different systems of governance, myriad cultures, vibrant democracies, fragile or isolationist regimes, underdeveloped nations of coastal Africa and oil rich Arab nations. India's inseparable

linkage to the Indian Ocean could not have been explained better, than in the words of noted Indian maritime historian, KM Panikkar:-

"The vital feature which differentiates the Indian Ocean from Atlantic or Pacific is the sub-continent of India, which juts far out into the sea for a thousand miles. It is the geographical position of India that changes the character of the Indian Ocean."[1]

Even though India paid a heavy price for its proverbial 'sea-blindness'[2] in the past despite this locational uniqueness, it has now recognised its rightful place in the geo-political affairs of the region. It thus, acknowledges the emerging security challenges posed by contemporary geopolitical dynamics, in addition to the non-traditional threats brought about by natural calamities and man-made causes; and is ready to play its legitimate part as a credible 'net security provider' in the region.

In this context, this article seeks to explore traditional risks that India faces in the maritime domain due to its enforced geographical co-existence with two of its neighbours – one decidedly hostile and the other blowing hot and cold. The geostrategic dynamics arising out of this spatial reality could play out in two possible scenarios – each with its associated type and quantum of risks. Thereafter, certain 'Force Preparedness' initiatives, measures and pathways to mitigate such risks – by way of their acceptance, avoidance, control, reduction and monitoring– are proposed.

Probable Scenarios in the Indian Ocean Region and Associated Security Risks

Majority of the Global community believes in exploiting the seas –

1 KM Panikkar, 'India and the Indian Ocean' (George Allen & Unwin Ltd, London 1945), P. 19.

2 The term 'sea-blindness' has been used as recently as in June 2021 to indicate compulsive and systemic politico-bureaucratic neglect of the maritime spaces surrounding India, to the detriment of its national security and economic progress. See Admiral Arun Prakash, 'China has become a maritime power: It's time India caught up,' Indian Express, 21 June 2021, https://indianexpress.com/article/opinion/columns/india-china-rivalry-maritime-power-navy-7367947/ (accessed 10 July 2021)

including the IOR – for peaceful purposes in accordance with the rules-based order. However, proactively dubious agenda of two States – Pakistan and China – and related activities of their maritime entities in northern IOR in particular, are a cause of acute concern for the Indian economic and security establishment. In this backdrop, two security scenarios could probably emerge in India's proximate seascape. The first would be on account of Pakistan's 'concept of operations' in the Arabian Sea, duly supported – actively or tacitly – by Chinese high technology enabled facilitators. The second scenario could play out when the Chinese naval force and other maritime assets equipped with or incorporating such high technologies, adopt unambiguously coercive stance in the northern IOR – and in fact, in entire IOR – with a potential to adversely impact India's economic and security interests. Broad contours of these scenarios which would increase the quantum of traditional risks for Indian maritime security forces, are laid down in subsequent paragraphs.

Scenario 1 – Pakistan's 'Concept of Operations' in the Arabian Sea Facilitated by Chinese Support

Pakistan, in accordance with its first ever Maritime Doctrine titled 'Preserving Freedom of Seas' – released in December 2018 – considers the north Arabian Sea as its primary area of interest; and the broader Western Indian Ocean as extended area of interest.[3] In the words of a Pakistani analyst, this Doctrine assesses that "nuclearisation of Indian Ocean by the adversary [Read India][4] has raised stakes in the region …" and that the adversary intends to "keep the conventional theater alive under cover of nuclear umbrella."[5] The Pakistan Navy (PN), in order to

3 Cdr (Retd.) Azam Khan, 'Pakistan launches first formal Maritime doctrine,' Pakistan Defence Forum, 12 February 2019, https://defence.pk/pdf/threads/pakistan-launches-first-formal-maritime-doctrine.608697/ (accessed 12 July 2021).

4 Words in parenthesis have been added by the Author for imparting better clarity to the statement.

5 Hamzah Taoqeer, 'Maintaining Command of the Sea: Maritime Doctrines of Pakistan and India,' Modern Diplomacy, 07 August 2019, https://moderndiplomacy.eu/2020/08/07/maintaining-command-of-the-sea-maritime-doctrines-of-pakistan-and-india/ (accessed 12 July 2021).

seize 'maritime command and control,' and to ensure suitable deterrence against this supposed intent, advocates an "approach of provocative and flexible mobility using sea space…" PN approach also includes "hit first with maximum effects and minimum application of force." [6]

It is however, posited that the PN with current level of capabilities would not be able to undertake the overarching tasks envisioned in Pakistani maritime doctrine. Thus, the only way to meet its doctrinal guidance of "hitting first with maximum effects and minimum application of force," is by allying with China – as a Pakistani Scholar suggests.[7] This will enable the PN also to benefit operationally from Chinese high-technology-enabled support infrastructure. This scenario is thus, built on the premise that Pakistan will execute this 'concept of operations' in its area of maritime interest on its own, with covert – and indirect – support being provided by China.

Pakistan's maritime doctrine also advocates the use of submarines to cause "high-intensity diversion and disruption of enemy's sea lanes of communications (SLOCs)… to dominate the war theater".[8] Towards this, the Yuan class submarines fitted with air independent propulsion (AIP) system – eight being imported from China[9] – could be equipped with the artificial intelligence enabled fire control and decision making systems to assist the submarine's captain in quick and accurate appreciation of situation and select appropriate response strategy. Yaogan series of satellites associated with space-based ISR chain of Chinese ASBM architecture, would assist in detection of adversary's force well away from Pakistani coastline. With access to 'restricted' positioning signals from Beidou satellite navigation system being made available to Pakistan,[10]

6 Hamzah Taoqeer, 'Maintaining Command of the Sea: Maritime Doctrines of Pakistan and India,' ibid.

7 Hamzah Taoqeer, ibid.

8 Hamzah Taoqeer, ibid.

9 The News, 'China building eight submarines for Pakistan,' 17 July 2018, https://www.thenews.com.pk /print/342558-china-building-eight-submarines-for-pakistan (accessed 12 July 2021).

10 Global Times, 'Pakistan 1st foreign nation to fully benefit from China's BeiDou system,' 17 May 2017, http://www.globaltimes.cn/content/1047421.shtml (accessed 12 July 2021).

PN ships and submarines would be able to carry out precision targeting of enemy assets. Medium Altitude Long Endurance (MALE) UAVs like Wing Loong-2 and UCAVs like the CH-4 imported from China could be used by Pakistan to track and target the adversary's naval forces and interdict its SLOCs in Pakistan's near-coast areas.

Certain types of Chinese special purpose ships of overtly non-military classification – like Mobile landing platforms, research ships and intelligence collection ships – could assist the PN in raising domain awareness, enable data and communication relay, and facilitate targeting. Chinese civilian oil tankers 'built to military specifications' could provide logistics support to PN ships and submarines at sea, thus increasing their endurance and reach.

Scenario 2 – Coercive Presence of Chinese Maritime Assets in IOR

Chinese Navy's envisioned role of 'conducting international cooperation in distant waters' as first articulated in its Defence White Paper of 2008; progressively expanded to 'protecting its strategic SLOCs and overseas interests' by 2015.[11] China acknowledges that accomplishment of its military tasks – including that of the PLA Navy – would face technology-enabled challenges from its adversaries.[12] It has therefore, been prioritising the incorporation of high technologies-driven development of its military hardware and operational plans. Accelerated pace of contemporary warship shipbuilding[13] continues to provided numerical superiority and capability accretion to the PLA Navy. Chinese shipyards have been constructing between 17-20 ships/submarines annually since

11 Chinese Defense White Paper of 2015, 'China's Military Strategy', section IV.

12 Chinese Defense White Paper of 2019, 'China's National Defense in the New Era', July 2019, section I.

13 Over last two decades, China has commissioned 2 aircraft carriers, 13 nuclear-powered submarines, 24 destroyers, 30 large frigates and 60 missile corvettes. See Liu Xiaobo, 'Sino-U.S. naval warfare capabilities amid great power competition,' CSIS Update, 26 May 2020, https://amti.csis.org/sino-u-s-naval-warfare-capabilities-amid-great-power-competition/ (accessed 12 July 2021).

2013.[14] It has gone on to launch 28 warships – 10 destroyers, 1 LHD, 1 LPD and 16 missile corvettes – in 2019.[15] Assuming that this trend continues – and China has not given any indications to the contrary – then the PLA Navy with about 270 blue water capable ships, could become the World's largest Navy by 2035[16].

Not with standing what happens in 2035, the current PLA Navy force level of 70 submarines – 4 SSBNs, 9 SSNs, and 57 conventional boats – 63 surface combatants over 3,000 tons, 12 ocean going replenishment ships, 60 odd missile corvettes, 46 large amphibious ships (LHA/LPDs/LSTs)[17] supported by ancillary and special purpose vessels; is itself quite sizeable. This whole Force Level can obviously not be deployed in the Indian Ocean. In fact, contemporary geo-political compulsions resulting in myriad maritime security challenges in the Pacific Ocean, will per-force necessitate majority of PLA naval force being deployed closer home. Thus, if China decides to allocate even 10 percent of its blue water forces for the Indian Ocean, it would empirically translate into eight surface units – six destroyers/frigates, one replenishment ship and one LPD.[18] As for submarines, One SSN may be deployed in addition, after excluding the SSBNs for strategic role from home waters, and conventional submarines required for tactical employment in the western Pacific itself.

14 China Military Online, 'Opinion: Intensive commissioning of PLAN warships in line with China's goal to safeguard its maritime rights and interests', 09 January 2014, http://eng.chinamil. com.cn/news-channels/china-military-news/2014-01/09/ content_5727866.htm (accessed 12 July 2021).

15 For full list of warships launched in China in 2019, see https://twitter.com/Loongnaval/status/ 1211646745815343104 (accessed 12 July 2021).

16 Michael A. McDevitt, 'China's Navy Will Be the World's Largest in 2035,' USNI Proceedings, February 2020, https://www.usni.org/magazines/proceedings/2020/february/chinas-navy-will-be-worlds-largest-2035 (accessed 12 July 2021).

17 Liu Xiaobo, 'Sino-U.S. naval warfare capabilities amid great power competition,' CSIS Update, ibid.

18 This estimate has been arrived at by the Author, purely as a conservative prudent assumption, considering the critical requirement for naval forces in the Western Pacific Ocean, as also taking into account, operational availability of ships, their endurance/sustainability at extended ranges, and mission profile at distant seas.

This pattern of PLA Navy deployment has in fact, become quite evident, since China commenced its anti-piracy escort duties in the Gulf of Aden in 2008. Starting with three ships, it progressively scaled up to 7-8 warships; mostly on account of prolonged 'post anti-piracy escort duty' commitments, bilateral/multilateral exercises, global/regional search and rescue (SAR) or HADR missions, 'Showing Flag' etc. One PLA Navy submarine also started getting deployed along with a support ship for 3-6 months in the IOR – and particularly in the Arabian Sea – since 2013. A mix of conventional and nuclear boats was deployed, of which the SSNs were observed in 2014, 2016 and 2018.

The total number of Chinese warship, submarines, deep-water research ships, support ships, intelligence collection and survey vessels present in IOR has exceeded 15, at times.[19] Considering the fast-paced shipbuilding programme – including aircraft carrier construction – and establishment of operating bases in IOR like Djibouti, Gwadar – and some more under negotiation; The PLA Navy would be able to deploy many more units to the IOR in future, while being able to manage its existent challenges in its immediate maritime neighbourhood.

It can thus, be reasonably assumed that the PLA Navy force level in IOR would easily double – to 16 as compared to current 8 – in 2025-2027 timeframe. Further, these ships would surely be more capable than those currently deployed; and would most probably include an aircraft carrier strike group (CSG) too. Combined with other types of support and special purpose vessels which are also being rapidly inducted in large numbers, the 'PLA Navy+' force level could aggregate to 26-28 vessels. The threats primarily associated with such a large Force, and consequently the risks arising therefrom are mentioned below:-

- A Chinese CSG strategically positioned in the Southern Indian Ocean to consolidate MDA picture from its own and space-based assets; and also ready to surge in either the Arabian Sea or Bay of Bengal, when required.

19 The PLA Navy and associated support ships – referred to as 'PLA Navy+' – in fact, created a record of sorts, when 19 ships were present in IOR between June-August 2017. This information was compiled by the Author from various Chinese news sites.

- The CSG could also detach one or two surface action groups (SAGs) to accomplish anti-ship, ASW or escort missions, on demand.
- SSN, attached to the CSG, may be used to selectively target Indian warships or interdict Indian SLOCs proceeding towards/ from the Malacca Strait.
- Independent SAG, being logistically supported from its base in Djibouti, could be off Somalia for interdicting Indian shipping passing Suez Canal and Persian Gulf.
- An independently tasked SSN could be anywhere along the western Indian coast, to disrupt India's critical energy supply routes and target enemy warships.
- An Amphibious Ready Group (ARG) could be in the Andaman Sea for posturing, strategic signaling and quick insertion into a targeted island; with its air safety cover being ensured either by Chinese carrier based aircraft, or PLA Air Force assets overflying Myanmar – well within the realm of possibility.
- Intelligence collection ships, interspersed in the Arabian Sea and Bay of Bengal, for monitoring operational activities of Indian naval ships, and relaying them.

Indian Maritime Force Preparedness towards Risks Mitigation

Force Preparedness Assessments – as the Concept Note explains – relate to what the Forces can do to mitigate risks associated with future conflict scenarios, rather than what they have at present. Towards fulfillment of this objective, the Indian security establishment has to dwell on certain risk mitigation pathways – accepting, avoiding, controlling, reducing and monitoring risks – so as to ascertain their efficacy in a given scenario. As for maritime domain, broad conflict scenarios with associated risks have been broadly explained above. Thus, while acceptance of risks in maritime warfare is axiomatic and avoidance of

the same is rarely an option; it would be prudent to try and reduce risks through comprehensive monitoring and credible control mechanism.

Maritime Force preparedness therefore, must firstly, aim at generating maritime domain awareness (MDA) – including new-found underwater domain awareness (UDA) – as an all time continuous activity; followed by best utilisation of these vital inputs to implement robust operational strategies to control traditional security risks.

Monitoring Risk – Maritime Domain Awareness (MDA)

MDA has the potential to be a game-changer in augmenting combat capabilities of the Indian Navy, not only in IOR, but also in the extended Indo-Pacific Region. It comprises the ability to effectively detect, locate, track and identify the presence of likely hostile targets in an uncertain and unpredictable maritime area interspersed with presence of neutral ships and merchantmen. Major elements of MDA include:-[20]

- Satellite-based surveillance technologies, duly supported by maritime reconnaissance and AEW aircraft, and long range UAVs, both ship-borne as well as shore-based.
- Joint and single service identification systems with an ability to discern between friend and foe.
- Sub-surface surveillance including both, mobile and static systems, deployable from ships, submarines and aircraft at critical vantage points in IOR.
- Robust networking infrastructure to provide high-speed large-bandwidth connectivity for sharing multimedia data with requisite built-in confidentiality.
- Development of effective cyber-space monitoring capability for safeguarding, and also obtaining information in cyber domain.

20 Ensuring Secure Seas: Indian Maritime Security Strategy (Integrated Headquarters Ministry of Defence (Navy), New Delhi, 2015), p. 134.

Controlling Risk – Key Force Preparedness Imperatives[21]

Anti-Submarine Warfare (ASW) Operations. Induction of modern submarines and other potent undersea hardware – including unmanned submarines, manned submersibles and UUVs – by Pakistan and China; and their potential employment for sea denial role in the Indian area of naval operations, calls for priority enhancement of Indian Navy's ASW capabilities. Thus, long-term vision and plan for enhancing Indian Navy's ASW capabilities at strategic, operational, and tactical levels for conduct of deep Ocean as well as shallow water ASW operations, is a must.

Air Defence and Anti-Air Operations. Indian Navy has made definite progress in the conduct of anti-air operations by inducting ship-borne/ airborne weapon systems and matching surveillance systems. This has been further enhanced with the induction of modern carrier-based aircraft, UAVs and airborne surveillance systems. Need of the hour is for procurement of more force multipliers (AWACS) – including carrier-based Airborne Early Warning (AEW) aircraft – to increase surveillance and Fleet Air Defence envelope, thus ensuring distinct advantage in air defence and anti-air operations.

Joint Expeditionary Mission Capabilities. In recognition of the fact that influencing events on land is one of the primary roles of a Naval Force, the Indian Navy must develop additional capabilities to conduct large scale amphibious operations in the IOR littoral. This would entail creation of strategic sealift capabilities through acquisition of heavy-lift helicopters and air cushion vehicles. In addition, more role specific land force formations would require to be allocated and closely integrated with amphibious, marine, and Special Forces of the three services. Creation of a Joint Rapid Deployment Force (RDF) would considerably enhance the Indian military's capability to conduct multi-domain expeditionary missions.

21 See 'Freedom to use the Seas: India's Maritime Military Strategy' Document (Integrated Headquarters Ministry of Defence (Navy), New Delhi, 2007), Chapter-8, 'Strategies for Force Build-up.' pp. 117-121.

Mine Counter-Measure (MCM) Warfare. Mining is one of the most economical ways of threatening powerful fleets while they are leaving their secure bases, and disrupting ship traffic in choke points or harbours. Thus Indian Navy's ability to keep designated channels open for safe departure of warships during a conflict would have a direct bearing on the conduct of further maritime operations. Critical deficiency in MCM hardware – mine-sweeping and mine-hunting ships and equipment – in contemporary times may cost the nation dearly in either of the above discussed scenarios; and must be made good at highest priority, by double -quick acquisition.

Special Operations. The ability to deploy Special Forces through multi-dimensional platforms to ensure their effectiveness against State/ non-State threats is well understood. Therefore, development of Naval Special Forces (MARCOS) as potent force multipliers must be a priority area for this decade.

Joint Operations. Future wars – including expeditionary operations – will invariably be undertaken by joint forces. Coordination and cooperation amongst the three Services and other associated forces like the Indian Coast Guard, including promulgation of common doctrines, coordination of strategies, commonality in equipment and standard operating procedures, are essential to the success of joint missions.

Conclusion

India does recognise very well, that evolving risk bearing scenarios in IOR and contemporary concepts of force employment require a maritime Force which should be optimally equipped to perform full spectrum of missions at sea. However, it is posited that 'Force preparedness' is not a one-time discrete activity, but a constant effort to sustain and progressively build on previously achieved levels. Since navies are built over several decades in a cost intensive manner, their 'preparedness' per-force, would depend on long-term financial commitment from the Government. Further, maintenance of 'Core Competencies' over long term would entail specific focus on niche areas related to warship and

submarine building, aircraft production and development of a future-ready defence industrial base. Towards this, recent reorganisation and corporatisation initiative of the Indian Government is a step in the right direction.

Finally, investment in future technology should be progressed as a national level project. This will not only catalyse naval 'preparedness' enhancement over next 10 years, but also ensure that risks associated with asymmetric advantage that China seeks vis-à-vis India in maritime domain, are balanced out. Thus, there is a need to seriously invest in military applications in Information Technologies, nano-materials, unmanned systems, quantum computing and Communications, artificial intelligence and other evolutionary technologies. Though it is easier said than done, but no effort is too much, and no price is too great to pay for ensuring national security – particularly in the maritime domain. As Raja Menon, a noted Indian maritime thinker, ruminates:- [22]

India, post-Galwan and Pangong Tso experience, must develop some punitive capability options in the Indian Ocean, lest it be consigned to look at future India-China security matrix from a position of tactical inferiority.

***Captain (IN) Kamlesh K Agnihotri (Retd)** is a former Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi

22 K. Raja Menon, 'Our larger China picture: A new strategy, combining diplomatic and military means, is needed to counter Beijing,' The Indian Express, 17 September 2020, https://indianexpress.com/article/opinion/ columns/india-china-border-dispute-galwan-valley-ladakh-6598913/(accessed 14 July 2021)

PREPAREDNESS RISKS MITIGATION - PRIORITIES FOR THE INDIAN AIR FORCE

Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)*

The recent India-China showdown in Ladakh has once again brought to focus, and also in public debate the preparedness of Indian armed forces to take on the aggressive and sometimes belligerent China[1]. China has had a fast growing economy for last three decades. The Communist Party dominated China[2] has had aspirations to be a world power. In the last two decades they have spent large sums on modernisation of the armed forces. India is a rising economic power with soon to have the largest population in the world. It is among the most threatened nations in the world. It has two nuclear neighbours with both of whom India has serious territorial disputes and has had full-scale wars.

China realised early that one who controls aerospace controls the planet. Airpower today is the dominant means of prosecuting war. It offers prompt multiple response options to the political leadership. Air and space give a vantage point to see wide area, allow connectivity, and allow large distance high speed weapon transit, and helps targeting. Today, Space greatly supports all warfare on earth. Weaponisation of space is also a reality. Aerospace offers speed, range, accuracy,

1 Christopher W. Bishop, To Understand China's Aggressive Foreign Policy, Look at Its Domestic Politics, Council on Foreign Relations, October 8, 2020, https://www.cfr.org/blog/understand-chinas-aggressive-foreign-policy-look-its-domestic-politics 01 June.2021

2 Srijan Shukla, "The Rise of the Xi Gang: Factional politics in the Chinese Communist Party," ORF Occasional Paper No. 300, Observer Research Foundation. February 2021. https://www.orfonline.org/research/the-rise-of-the-xi-gang/ 01 June 2021

and lethality for achieving military effects. Air power and future of all warfare are intertwined. Air superiority, will still be a pre-requisite for all operations on the surface to succeed[3]. Even armies and navies are wanting to spend more and more on air assets.

Current State of IAF

The Indian Air Force (IAF) is the fourth largest air force of the world. The primary mission is to secure Indian airspace and to conduct aerial warfare during armed conflict. Defence minister's operational directive of February 2009: "We should be prepared to fight on both fronts simultaneously a war at 30 days (intense) and 60 days (normal) rates.[4]" The IAF has 32 fighter squadrons. These broadly include two of Rafale, 12 Su 30MKI, 5 MiG 21 Bison, three each of MiG 29 and Mirage 2000, 5 of Jaguar, and two of LCA. IAF's induction of Rafale fighters will enable it to maintain air superiority over China's J10, J11, and Su-27 fighter jets[5]. Armed with very long-range Meteor and MICA beyond visual range (BVR) air-to-air missiles, the Rafale fighters are expected to pose a significant threat to Chinese aerial assets. The Sukhoi Su-30MKI serves the IAF as the primary air superiority fighter with the capability to perform air-to-ground strike missions. With 11 C-17 and C-130 each, 17 IL-76, and over 100 upgraded An-32, IAF has significant cargo and troop lift capability. Similarly having inducted 15 Boeing Chinook heavy-lift and 22 Apache AH-64E attack helicopters, and with already a significant fleet of 240 Mi-17 series medium-lift helicopters and nearly 100 ALH variants and smaller Chetak/Cheetah fleets, IAF is in a good position

3 Phillip S. Meilinger, Supremacy in the Skies, Air Force Magazine, February 2016, https://www.airforcemag.com/PDF/MagazineArchive/Magazine%20Documents/2016/February%202016/0216supremacy.pdf 01 June 2021.

4 Sushant Singh, The Challenge of a Two-Front War: India's China-Pakistan Dilemma, Stimson, April 19, 2021, https://www.stimson.org/2021/the-challenge-of-a-two-front-war-indias-china-pakistan-dilemma/ 17 May 2021.

5 Ajay, India vs China: Airpower compared, Air Force Technology, July 31 2020, https://www.airforce-technology.com/features/india-vs-china-indian-air-force-iaf-vs-peoples-liberation-army-air-force-plaaf/#:~:text=PLAAF%20is%20the%20second%20biggest,IAF%20is%20the%20fourth%20largest.&text=PLAAF%20has%20a%20long%2Drange,drones%20compared%20with%20the%20IAF. 17 May 2021

for rotary wing assets. IAF has only three large AWACS aircraft and two indigenous DRDO developed AEW&C aircraft. Similarly IAF has only six IL-78 Flight Refuelling Aircraft (FRA). Both these fleets are highly inadequate for a continental size country like India which has also to cover the Indian Ocean Region.

India has a well-covered and integrated air defence radar cover. IAF continues to operate some of the legacy surface-to-air missile systems like the SAM-3 Pechora and SAM 8 OSA-AK. With the induction of a large number of indigenous Akash AD systems, and also, to arrive by November 2021, five S-400 systems[6] from Russia, the AD coverage will be significant. To cover the large Chinese border, more systems will need to be inducted. With induction of the MICA, Meteor, Astra, SCALP, BrahMos and Hammer, among others, IAF has a significant aerial weapons inventory.

Effects from the Air

Air power is inherently strategic in nature and simultaneously provides conventional deterrence. Air Campaigns can be executed simultaneously against different spread out target systems. It can provide both kinetic and non-kinetic options with pin point accuracy. It can influence outcomes and actions of the surface forces. It can simultaneously produce physical as well as psychological effects. Strategic airlift allows strategic reach and strategic effects. IAF has repeatedly demonstrated it. IAF is technology intensive service and aerial systems have early obsolescence, and require greater investment in R&D and also funding. IAF is looking at reach from the Persian Gulf to the Straits of Malacca, using long range aircraft supported by FRA and AWACS. More of these are being acquired. IAF transformation is being driven from just being platform-based to being capability-based. Effects based, network centric operations are the new normal. Advantage of air power is ability to

6 Dinakar Peri, Delivery of S-400 missile systems to begin by November, The Hindu, April 13, 2021, https://www.thehindu.com/news/national/delivery-of-s-400-missile-systems-to-begin-by-november/article34312445.ece 02 June 2021.

exploit swing-role capabilities. When you say Rafale is an Omni Role fighter, means it can do many roles in a single mission. Intelligence, Surveillance and Reconnaissance (ISR) has become even more crucial for decision-superiority in net-centric warfare. Air power is best suited for it.

All countries are engaged in network-centric warfare[7]. Cyber and electronic warfare is where action is. Securing own networks and denying the same to adversary will be important. Air and Space platforms will greatly support cyber and electronic warfare operations much deeper into the enemy territory. There are dedicated aircraft for this purpose. The future is unmanned. Artificial Intelligence supported autonomous systems will fly independently or in conjunction with each other in a swarm or with manned aircraft as a team. This is one area India needs to invest more in. Unmanned systems are required for civil logistics and delivery, policing, and a variety of civil roles, but in military they will take on all the "Dull, Dirty and Dangerous Missions[8]". Dull means boring long reconnaissance missions. Dirty means going into contaminated areas. Dangerous means entering much contested and well-defended areas.

Rapidly Growing PLAAF

China's People's Liberation Army Air Force's (PLAAF) mammoth fleet of fighter aircraft and advanced air defence systems poses an intimidating challenge to the IAF's relatively smaller fleet size. PLAAF currently has nearly 2,000 fighter/bomber aircraft, with over 600 of 4th generation plus[9].

7 Lt Gen (Dr) R S Panwar, Network Centric Warfare: Origins And Main Characteristics, Future Wars, September 08, 2017, https://futurewars.rspanwar.net/network-centric-warfare-origins-and-main-characteristics/ 03 June 2021

8 Editorial Team, Drones Doing Dirty and Dangerous Jobs, Smithsonian National Air and Space Museum, Nov 28, 2017, https://airandspace.si.edu/stories/editorial/drones-doing-dirty-and-dangerous-jobs 03 June 2021

9 Ajay, India vs China: Airpower compared, Air Force Technology, July 31 2020, https://www.airforce-technology.com/features/india-vs-china-indian-air-force-iaf-vs-peoples-liberation-army-air-force-plaaf/#:~:text=PLAAF%20is%20the%20second%20biggest,IAF%20is%20the%20fourth%20largest.&text=PLAAF%20has%20a%20long%2Drange,drones%20compared%20with%20the%20IAF. 01 June 2021

PLAAF has a long-range strategic bomber fleet and holds more strategic assets such as airborne warning and control system (AWACS) aircraft and combat drones compared with the IAF. PLAAF's operational fourth-generation fighters including J-10B/C, J-11B, J-16, and Su-30. PLAAF already has around 40 fifth-generation J-20 fighters, and targets to have 200 of these by 2027[10]. Meanwhile, the FC-31/J-31 remains under development. PLAAF has clear edge in having nearly 120 H-6 strategic bombers, with some variants able to carry up to six cruise missiles with 1500 km range. China also has much larger number of indigenous AEW&C aircraft and Flight Refuellers (FRA). China also has an edge with a huge surface-to-surface missile force. China's biggest strength is its indigenous aircraft industry that produces all types of aircraft and advanced helicopters. China has a huge Unmanned Aerial Vehicle (UAV) fleet of indigenous design. China also has significant Maritime air power, with PLA Navy (PLAN) having two operational aircraft carriers and nearly 600 aircraft. Two more carriers are under construction and two further, larger ones, on drawings boards. It can be seen that China has significant air power.

Pakistan Air Force (PAF)

PAF has 19 squadrons with around 400 fighter aircraft, but many are awaiting replacements. In the long term, PAF will have around 300 JF-17s, 75 F-16s and will choose some other Chinese fighter, may be of J-10 class. PAF has a mid-sized transport aircraft and helicopter fleets. But they have acquired significant number of Chinese UAVs and will soon set up production of Wing Loong UAVs in Pakistan[11]. The PAF is primarily air defence orientated. While PAF in itself does not pose any significant threat to India, it has been exercising closely with PLAAF

10 Editorial Team, China's J-20 fighter turns 10, The economic Times, January 19, 2021, https://economictimes.indiatimes.com/news/defence/chinas-j-20-fighter-turns-ten/article-show/80328358.cms 03 June 2021

11 Editorial Team, Wing Loong Unmanned Aerial Vehicle (UAV), Air Force Technology, https://www.airforce-technology.com/projects/wing-loong-unmanned-aerial-vehicle-uav/ 03 June 2021

and has advantage of equipment interoperability. It could also allow the PLAAF to use some of its airfields. At the end of "Shaheen IX" joint PLAAF-PAF exercise in late 2020, PAF Air Chief Mujahid Anwar Khan said, "Evolving global security situation demands greater cooperation between Pakistan and China"[12]. IAF has to thus factor in a two front confrontation.

Targeted End State IAF

"IAF will have 37-38 fighter squadrons in a decade", said the Deputy Chief of IAF, Air Marshal Sandeep Singh at a webinar[13] in September 2020. This effectively meant 2030. The then IAF Chief Dhanoa had said in 2018 that "…. The force would get the authorised strength of 42 fighter squadrons by 2032"[14]. My personal assessment is that the IAF could reach 42 squadrons earliest by 2038. The end state could be 14 squadrons of Su-30 MKI, two each of Mirage 2000 and MiG 29, 12 squadrons of LCA variants, two of Rafale, six of the new fighter, and four of Advanced Medium Combat Aircraft (AMCA). This would make it 42. Effectively we would have stretched the Mirage and MiG 29 fleets. These figures are highly achievable as long as timely funds are allotted and there are no serious development delays in AMCA. IAF must also target to have 8 large and 10 smaller AWACS, at least 12 FRA aircraft. IAF must have by then a significant fleet of Unmanned Combat Aerial Vehicles (UCAV) systems, including the indigenously developed

12 Economic Times, Evolving security situation demands greater Pak-China cooperation: Pakistan Air Force chief, December 24, 2020, https://economictimes.indiatimes.com/news/defence/evolving-security-situation-demands-greater-pak-china-cooperation-pakistan-air-force-chief/articleshow/79942342.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst 2 June 2021

13 Dinakar Peri, IAF will have 37-38 fighter squadrons in a decade, says deputy chief, The Hindu, October 01, 2020, https://www.thehindu.com/news/national/iaf-will-have-37-38-fighter-squadrons-in-a-decade-says-deputy-chief/article32735076.ece 01 June 202

14 The Economic Times, Indian Air Force capable of striking nuke, other targets in Pakistan: IAF Chief, July 14, 2018, https://economictimes.indiatimes.com/news/defence/indian-air-force-capable-of-countering-china/articleshow/60954330.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst 01 June 2021

DRDO's "Ghatak"[15]. IAF should also have a large inventory of aerial missiles with longer ranges including the later variants of BrahMos and Astra missiles.

Synergy at National Level

India is in the process of evolving afresh its national doctrine based on ancient Indian thought. "Strength is power. And well-being is the goal" (Arthashastra, 6:2-31, 32)[16]. The political direction to the forces is very clear and have been given a free hand. Due to the multi-dimensional nature of conflict, increasing levels of synergy amongst the armed forces and civil agencies is operationally critical. IAF is going to be a key element in support of the surface, maritime and sub-surface wars.

Pakistan Centric to China Centric

For long, India's military assets and infrastructure were Pakistan border centric. This is fast changing, for both infrastructure build up and assets position. While border roads and connectivity are being improved, IAF has upgraded its Advanced Landing Grounds (ALG) near China border[17]. All IAF airfields are getting hardened aircraft and equipment shelters. IAF now has significant number of Su-30 MKI squadrons facing China. Also the new acquisitions like Rafale, C-130 J, Chinook and Apache helicopters have all been located in the eastern sector. The same is also applicable to air defence systems and weapons positioning.

15 EurAsian Times Desk, India's Most Secretive 'Stealth Drone' Project Uncovered; Aims To Counter Dassault, Boeing & Northrop UCAVs, EurAsian Times, October 12, 2020, https://eurasiantimes.com/indias-most-secretive-stealth-drone-project-uncovered-as-it-aims-to-counter-dassault-boeing-northrop-ucavs/ 01 June 2021

16 Editor, A National Security Doctrine for India, Takshashila Institution, June 2019, https://takshashila.org.in/a-national-security-doctrine-for-india/ 01 June 2021.

17 Editorial Team, Big boost to military infrastructure near China border! IAF opens another ALG in Arunachal, Financial Express, September 18, 2019, https://www.financialexpress.com/defence/big-boost-to-military-infrastructure-near-china-border-iaf-opens-another-alg-in-arunachal/1709840/ 03 June 2021

Hindustan Aeronautics Projects

Over the years, Hindustan Aeronautics Ltd (HAL) has produced under license a large variety of fixed and rotary wing aircraft. ADA developed LCA 'Tejas', and its in-house Advanced Light Helicopter (ALH) are the two major indigenous programs. Larger and more capable variants of these are being built. HAL also overhauls and upgrades of many aircraft and engines. HAL also has several multimillion-dollar contracts from leading international aerospace firms such as Airbus, Boeing, and Honeywell to manufacture aircraft parts and engines. From IAF point of view, priority has to be to complete design and development LCA Mk 1A, and mark up annual production initially to 16 aircraft. Tasks further down include developing the LCA Mk II and AMCA. HAL has been handed over an RFP for 70 HTT-40 basic trainer aircraft. HAL is also still working further on the long-delayed Intermediate Jet Trainer (IJT). The midsized, 80-90 seat, Indian Regional Jet (IRJ) has still to take off. Similarly, the Saras small transport (20 seats) is still struggling.

Projects DRDO

Defence Research and Development Organisation (DRDO) has had its successful projects in the LCA, SU-30 MKI avionics, MiG-27 and Jaguar upgrades, UAVs, and EW suites of many aircraft. They are also making missiles and radar, and integrating the indigenous AEW&C 'Netra' on the Embraer platform and will be responsible for the development of the AMCA. DRDO also runs the Integrated Guided Missile Development Program, which includes the successful Akash air defence system and Astra air-to-air missiles, and Nirbhay missiles. BrahMos missile is through Indo-Russian joint venture evolved by DRDO. DRDO has plans for Long and medium-range SAMs. LRDE has had successes in the development of radars like the INDRA, Rajendra fire control radar for the Akash missile system, the Central Acquisition Radar (CAR), LRTR a 3D AESA with help of Elta of Israel, and the 2D Low-Level Lightweight Radar (LLLR). It is also developing the Uttam AESA for LCA Mk II, and

S-Band AESA array for the DRDO's AEW&C. ADE made the Lakshya aerial target, some flight simulators, and a few avionics for Tejas LCA. GTRE's flagship program was the GTX Kaveri engine intended to power the HAL Tejas which ran into failure for many reasons. The program was abandoned in 2014. Meanwhile, a 52-kilonewton dry variant of the Kaveri engine is planned to be used in the DRDO UCAV. Defence Avionics Research Establishment (DARE) is in the areas of airborne electronic warfare, airborne processors, and mission avionics. DRDO is also involved in Artificial Intelligence (AI) research.

Atmanirbharta the Only Answer

The Make-in-India, Atmanirbharta, in defence is being aggressively pushed at the highest levels. Defence imports not only take away large chunks of foreign exchange but also perennially put the nation at the mercy of foreign powers. India currently also has the dubious reputation of being one of the largest importers of defence equipment. To promote indigenous design, development, and production many measures have been initiated. Defence Acquisition Procedure DAP-2020 is a greatly evolved document. Clearly, the thrust is to promote 'Made-by-India' as a first choice. 'Make-in-India' is being driven as an interim solution. Big private industrial houses like Tatas, L&T, Reliance, Mahindras, Adani, Bharat Forge and many others have come into defence manufacturing in a serious way. The government's thrust is to increase the share of all manufacturing from the current level of 15 per cent of Gross Domestic Product (GDP) to 25 per cent. The defence will be a significant area. India's target is to reduce defence imports to initially 40 percent from nearly 70 percent[18].

Adding to the existing list of 101 defence items banned for import, the Ministry of Defence has released a list of 108 more items to be added to the negative import list to give further impetus to self-reliant defence

18 Editorial Team, Arms race: India approves defence procurements worth $3.5 bn, says report, The Tribune, July 19,2014, https://tribune.com.pk/story/738177/arms-race-india-approves-defence-procurements-worth-3-5-bn-says-report 02 June 2021

manufacturing[19]. The list also comprises of many complex systems, sensors, simulator, weapons and ammunitions related to the IAF like Helicopters, Air Borne Early Warning and Control (AEW&C) systems, Medium Power Radar for Mountains, MRSAM Weapon Systems, among many others.

Government formulated the 'Defence Production and Export Promotion Policy 2020' to provide impetus to self-reliance in defence manufacturing under the 'Aatmanirbhar Bharat' scheme. The ministry aims to achieve a turnover of Rs. 1 lakh 75 thousand crore (US$ 25 billion), including an export of Rs. 35 thousand crore (US$ 5 billion) in the aerospace and defence goods and services by 2025[20].

India has finally come of age with the LCA program. We are building good helicopters. We have a great space and missile program. We need to increase production, and also hasten development of Mk1A and Mk2. The fifth Generation Advanced Medium Combat Aircraft (AMCA) must succeed for India to come into big league. India must accelerate development of its own mid-size transport aircraft and airliner. We need to convert pure research into products that can be physically inducted in the armed forces.

Private Sector in Defence

India has a great industrial base and significant defence equipment demand to allow advantage of scale. If India can succeed in its missile, space and nuclear programs, it can do the same in defence production. Privatization of DPSUs has been spoken for long. Embraer of Brazil is a successful model to emulate. Of India's defence market, roughly 70% has been through imports, 25% with the Defence PSUs and the

19 Abhishek Bhalla, Mini UAVs, mine-protected vehicles among new list of 108 defence items banned for import, India Today, May 31, 2021, https://www.indiatoday.in/india/story/mini-uavs-mine-protected-vehicles-among-new-list-of-108-defence-items-banned-for-import-full-list-1809194-2021-05-31 01 June 2021.

20 Indian Brand Equity Foundation, June 02, 2021 https://www.ibef.org/industry/defence-manufacturing.aspx 02 June 2021

remaining 5% with private partners. This will change soon. BrahMos tactical cruise missile is a successful JV with Russia and ready for export. India has great success in ship-building both through public and private sector shipyards. Among the airborne systems projects, And Tata Power is handling the modernization of airfield infrastructure for IAF. Tata Aerospace and Defence (Tata A&D) have been making the AH-64 Apache combat helicopter fuselage. They are also making aero-structures for Boeing's CH-47 Chinook helicopters. All C-130Js delivered to customers around the world have major aero-structure components from India. Sikorsky, a Lockheed Martin company, also relies on Tata Advanced Systems (TASL) in Hyderabad, India, as the manufacturing base for its global supply of cabin aero-structures for the S-92 helicopter. Lockheed Martin Aero-structures (TLMAL), is a joint venture with TASL and Lockheed Martin, producing 24 C-130 empennages annually. Tata group is working with GE to manufacture CFM International LEAP engine components in India. Lockheed Martin selected TASL to produce F-16 wings in India. EADS unit Cassidian plans to make India a hub for a large number of defence products that are locally manufactured and also offer technological value. GE has a huge India presence. There is also a large MRO market that can create an R&D base for engineering services. Adani-Elbit JV will make Hermes 900 UAVs in India.

In 2012, Centum Group, a Bangalore-based defence electronics company was selected to supply to French defence solutions provider Thales. It is now cleared to supply directly to any of the 70-plus Thales sub-groups. Tata Power Strategic Engineering Division (SED) has secured orders for the Akash Air Force Launcher for the Indian Air Force. Mahindra Group bagged a large aero-components production contract to manufacture a variety of metallic components for several Airbus aircraft. Bharat Forge is a major player in the artillery and specialized vehicles segment. Several small companies – such as Dynamatic Technologies, Avasarala Technologies, DefSys, Ravilla, and Taneja Aerospace – have of late acquired advanced technological capabilities.

Dynamatic Technologies makes assemblies of vertical fins for Sukhoi 30 MKI fighters. Samtel electronics makes SU-30 Head-Up Displays and other electronics. Indian companies have the global opportunity not only due to cheaper skilled labour but have also developed the ability to manufacture accurately to specifications, particularly in aerospace, metalworking, and electronics.

An estimated 24,000 MSMEs currently involved in defence supply chain, and the contribution of private players in the defence sector has steadily grown over the years with more than 460 licenses issued so far to private companies. Over the next 7-8 years, India's defence modernisation plan is projected at $130 billion and contracts worth over $55.17 billion are expected to be placed with domestic manufacturers, as per Engineering Exports Promotion Council (EEPC) India[21].

Technologies India Must Master

India needs to identify new game-changer technologies and start investing, lest be get left behind. These include cyber and electronic warfare, artificial intelligence, unmanned systems, hypersonic, among others. Hypersonic flight and weapons will be difficult to engage. They will act as force multipliers against high-value targets. There is a lot of action in Directed Energy Weapons. Lasers that can burn incoming missile electronics or dazzle electro-optical sensors. For India to become significant, it must also master aircraft engine, and AESA radar technologies. Many of our successes are from joint venture route. Sixth Generation fighter technologies are evolving. Stealth will remain a feature. Very long range weapons would mean air combat shifts farther apart. Ranges of around 400 kilometres for air-to-air missiles are already a reality. Air launched cruise missile ranges are going up and are a vital technology.

21 Editorial Bureau, Over 460 licences issued for private players in defence production, The Hindu Business Line, March 23, 2021, https://www.thehindubusinessline.com/companies/msme/over-460-licences-issued-for-private-players-in-defence-production/article34142204.ece 03 June 2021

Imperatives for IAF

Clearly IAF will have has been sturdily growing in capability. It must get back to the authorized force levels of 42 squadrons. Some often suggest that since Rafale and Su-30 MKI can achieve much greater effects than the older MiG 21s, why IAF should continue to seek 42 squadrons. The argument is flawed. India's adversaries are already having fifth generation fighters. They are not cutting down numbers. Type of aircraft and weapon platforms must be comparable to the adversary. India must have them too. IAF also urgently needs additional AEW&C and FRA. The future being unmanned, IAF needs to invest more into combat UAVs. India has also to defend itself against a possible sizeable Chinese surface-to-surface missile (SSM) attack. We need more air defence SAM systems of the S 400[22] and Iron Dome[23] class, and the many indigenous air defence systems India is working on, including some in JVs with Israel. It is important to have a larger ammunition and missiles stocking. SSMs and Cruise missiles are going to be important. India has a good missile program. The Prithvi, Agni, BrahMos, Akash and Astra missiles are a success, and newer variants must be hastened. Electronic and cyber warfare capability is going to be important. More needs to be done on this score.

Way Ahead

India has threat from two-fronts has been acknowledged by the government and has been repeatedly stated by the Chief of Defence Staff (CDS) General Rawat[24]. India is surely factoring in such a scenario.

22 Huma Siddiqui, India to get world's best Air Defence System S-400 from Russia, Financial Express,
April 16, 2021, https://www.financialexpress.com/defence/india-to-get-worlds-best-air-defence-system-s-400-from-russia-check-details/2234332/ 02 June 2021

23 Krishn Kaushik, Explained: How Israel's Iron Dome air defence system intercepts rockets, Indian Express,
May 25, 2021, https://indianexpress.com/article/explained/explained-how-israels-iron-dome-intercepts-rockets-7312743/ 02 June 2021

24 Krishn Kaushik, Army, IAF chiefs visit forward areas, CDS Rawat warns of two-front threat, The Indian Express, September 4, 2020 https://indianexpress.com/article/india/india-china-border-dispute-cds-bipin-rawat-naravane-6582279/ 01 June 2021

But currently there is a backlog of modernisation of all three services. In particular for the IAF, the obsolescence sets in much faster for aerial systems. The gap with China is continuing to increase. India certainly needs to increase its defence allocations, from current 2.15 percent[25] of GDP to around 2.5 percent. IAF is well trained and operationally well exposed. IAF has clear advantage in terms of more and better located and equipped airfields than China. IAF can well match the PLAAF, but once the numbers increase, IAF will be much better placed. Time to act is now.

***Air Mshl Anil Chopra,** PVSM, AVSM, VM, VSM (Retd) is the Director Centre for Air Power Studies (CAPS), New Delhi

25 Abhishek Bhalla, India's defence spending in terms of total govt expenditure for 2021-22 lowest in six years, India Today, March 17, 2021, https://www.indiatoday.in/india/story/india-s-defence-spending-in-terms-of-total-govt-expenditure-for-2021-22-lowest-in-six-years-1780407-2021-03-17

JOINT PROFESSIONAL MILITARY EDUCATION (JPME) AND SERVICE SPECIFIC PME – A FRAMEWORK TO ADDRESS THE OUTCOME DEFICITS

*Lt Gen Atulya Solankey, AVSM, SM

"Live as if you were to die tomorrow, learn as if you were to live forever."

– Mahatma Gandhi

Abstract

PME lays the foundation of intellectual component of warrior culture and propels the military leaders towards professional mastery. The military power can be maximized if employed in an integrated manner - jointness being the key. The edifice of 'Jointness' rests on three pillars viz. Joint Warfare Doctrines, Joint Operations and Joint Training. The curriculum in training institutions, both joint and service specific, is designed such that the focus at lower levels is to enhance the depth of knowledge, while at the senior levels, the emphasis shifts to broaden the horizon – enhance the breadth of knowledge. The current dynamic situation, both on the Northern and Western fronts and the challenges of internal security situation, inevitably draw attention to the adequacy of PME or deficit therein and the need to re-align, to address the concerns.

Effective Service Specific PME is a major strength, proved beyond doubt during innumerable operations and deployment on the

frontlines. However, inadequate jointness, heavy lean on the tactics, lack of leadership training beyond the initial career, lack of study of military campaigns, absence of yearning for research and reading; are some of the deficits that need immediate attention. Though, the overall effectiveness of the PME is fairly satisfactory, the hierarchy at the apex level have recognised the inevitability to re-align the PME to meet the future challenges – a work in progress. The Indian military is already planning to set up a Joint Training Command (JTC) to achieve greater synergy. At the Army level, the mandate of PME has been assigned to the ARTRAC. Several Army formations, have taken the lead to inculcate and encourage the spirit of inquiry, research on futuristic technologies, ideas and innovations. The initiatives include the Command Availability Model for Training (CAM-T), research and publication by officers on a military subject and R&D projects in collaboration with trade.

In the process of re-alignment, certain niche areas viz. PGMs, AI, Robotics, Quantum Computing, Cyber Technology, Mobile Communication Engineering and Enterprise Resource Management should receive enhanced focus. Further, the IA, IN and IAF need to articulate 'recommended reading lists' to channelise the thoughts of military commanders, at all levels. Besides, increased emphasis on joint training, joint war games and joint exercise be laid. To jointly safeguard our National Security Interests with confidence, we must 'Train Jointly to Operate Jointly'.

Professional Military Education (PME) lays the foundation of intellectual component of warrior culture and propels military leaders towards professional mastery, a state that changes as individuals continue to gain knowledge and broaden horizon. It entails separate, yet inextricably linked constituents i.e. Training and Education. The education imparts the military leaders with analytical abilities, critical thinking, evaluating differing perspectives, forming and communicating cogent views, ability to take calculated decisions in the fog of uncertainties and deftly tackle the unforeseen events. **The development of Intangible traits viz. thinking about the problem, analysis and finding solutions where none exist– creation of**

Professional Wisdom; is achieved through education. The training, on the other hand, develops tangibletraits, which encompasses individual, collective and institutional training with the focus centered on development of combat abilities and skills, required to accomplish the assigned tasks with proficiency. *The PME essentially complements the individual training, operational experience and self-development to produce professionally competent leaders.*

The Foundational Overview

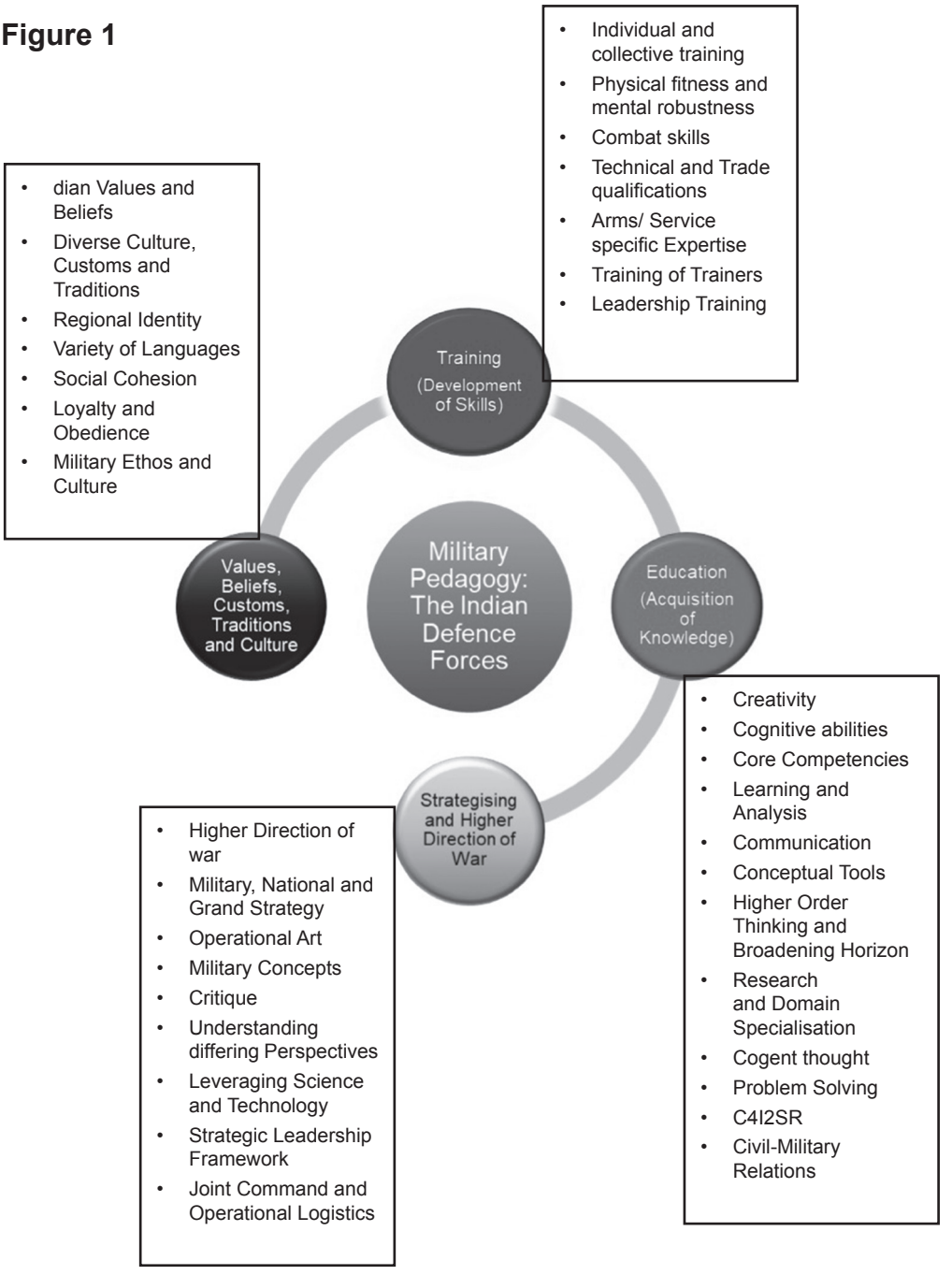
The JPME, which is a need of the hour, aims to constantly engage through knowledge at Tactical, Operational and Strategic levels to build intellect in military leaders and develop joint processes for service synergy.

Military Pedagogy. Military pedagogy is the basis of teaching and learning followed in the military training institutions. It is a military science that looks into the philosophies, conceptions, visions, doctrines, objectives, approaches and technologies of military education and training.

Pedagogy Styles in Vogue. Indian Army (IA), Indian Navy (IN) and Indian Air Force (IAF) follow different service specific pedagogy styles. The basics of pedagogy are, however, common and designed to suit the requirements of Defence Forces. The fundamental pedagogy style, which reflects the Indian values, beliefs and cultural practices which further narrow the thoughts and action, is discussed hereunder: -

Military Pedagogy: The Indian Context

Figure 1



Source: *Author*

The Enabling Institutions. The enabling institutions and levels of PME to create professional mastery, are discussed hereunder: -

Table 1

Level of Service& PME Applicable	Service PME(SPME)/ Institutions			Joint PME (JPME)/ Institutions	Remarks
	IA	IN	IAF		
Service - 25 years' and beyond (Operational & Strategic Level, Institutionalised Training)	Think Tanks			National Defence College (NDC), Advanced Professional Program for Public Administration (APPPA), Fellowship at Think Tanks, Study Leave, Orientation Courses, Core Programme	Joint training coordinated by HQ IDS through Joint Training Committee (JTC).
	Centre for Land Warfare Studies (CLAWS)	National Maritime Foundation (NMF)	Centre for Air Power Studies (CAPS)		
15 – 25 years' service (Operational Level, Institutionalised Training))	Army War College (AWC)	Naval War College (NWC)	College of Air Warfare (CAW)	Higher Defence Management Course (HDMC), Lead Service War Colleges*, Study Leave, Fellowships at Think Tanks, Sponsored Study Programmes	* Limited vacancies allotted to sister services. Focus on jointness.
	Joint Faculty exists				
8 – 15 years' service (Senior Tactical Level, Institutionalised Training))	Army War College, Service Specific Institutions	Technical Manage-ment Course	Advanced Professional Knowledge Course	Defence Services' Staff College (DSSC), Technical Staff Officers' Course (TSOC)	Jointness emphasised in Staff Colleges.
5 – 8 years' service (Tactical Level, Institutionalised Training))	Infantry School, HAWS, CIJWS, Service Specific Institutions	Long Course	Basic Professional Knowledge Course	-	Domain specialisation. Focus to enhance depth of knowledge.

Young Officers (YO) - upto 5 years' service (Basic Military Training (BMT))	Service specific institutions. (Combat training, basic tactics, weapon operation and administration of a sub-unit.) 32 category 'A' & 47 category 'B' establishments of IA; and many institutions of IN and IAF provide training at all levels.			-	Jointness lacking. Focus on individual service.
Pre-commission Training (PCT)	IMA, OTA, CTWs	Naval Academy	AF Academy	NDA	Focus on individual service, less NDA.

Source: *Author*

The Felt Need

The 'Nature of War' is enduring but its character remains dynamic. The future conflicts, characterised by the pre-dominance of information, cyber and space assets; and fought in multiple domains; require own forces to be well poised, to jointly execute operations harder, quicker and better synergised than our competitors; while, simultaneously maintaining optimal readiness to combat the challenges of counter terrorism (CT) operations. Besides, the short and swift future wars demand versatile, adaptable and rapidly deployable Strike forces. Currently, the operational dynamism, both on the Northern and Western fronts and the challenges of internal security situation, inevitably draw attention to the adequacy of PME or deficits therein and the need to re-align.

If the modern war is 'All Nation's Approach – a National Effort', then the PME should not remain limited only to the Defence forces, but look beyond to include defence partners in Para-military Forces, industry, academia, inter-agencies and ministerial participation.

The PME, though single service based, yet should provide the joint learning. The curriculum formulated by the lead service should enhance the spirit of jointness among the participating military leaders.

Development of Joint Forces, Joint Warfare Doctrine, National Security Strategy and Policy, Technology and Capability should be central to the PME. The services need to be integrated institutionally, organisationally, intellectually and technically to fight future wars, which will increasingly require the armed forces to fight jointly. Thus, joint critical, creative and strategic thinking is vital.

Development of joint backbone curricula, combined with targeted approach and measures with online options for self-study is inevitable, to bring jointness in thought, action and application.

Joint problem solving, factoring in emerging technological trends and disruptive technology effects, is inevitable to leverage modern technology and remain competitive in the foreseeable future. JPME at the tactical, operational and strategic levels would progressively result in enhanced integration in planning, execution of operations, logistics support functions, better interoperability and sharing of assets.

With lean budgets and vigorous thrust to economise the revenue expenditure, efficient resource management is implicit. While efforts to streamline equipment, materials, transport and services' management have been reasonably successful; optimal efficiency is achievable by implementation of Enterprise Resource Management (ERM).

The Searching Questions

The system of PME has progressively evolved, the changes being incremental in nature, rather than transformational. To enable an assessment of effectiveness of PME, certain questions emerge, as discussed hereunder:-

(a) Do adequate joint institutions exist for promoting jointness at various levels, among military commanders of the three services?

(b) Is the existing system able to develop the desired level of Core Competencies for joint operations?

(c) Are any specific joint programmes in vogue, which commit to self-directed learning skills at various levels of command?

(d) Does current system build rapport and cooperation within & outside service and prepare military leaders to effectively execute command tasks and achieve objectives at the tactical and operational levels?

(e) Does JPME at the NDC, CDM and the War Colleges, sufficiently facilitate the transition from tactical & operational levels to the strategic level?

(f) Are leaders encouraged to study military campaigns, to gain knowledge and learn from the history to build competencies to tune in the competitive and technologically complex environment?

(g) Do research projects focus on the joint problem solving and pragmatic subjects of military value or dwell in the realm of abstract academic issues, having limited application in the defence forces?

(h) Does the present system of education build leadership and joint warfighting skills which support and promote organisational purpose and direction?

Identifying the Deficits in the Current System of PME

The military leaders must train for certainty and educate for uncertainty. While at lower levels, the degree of certainty is high; the situation reverses with exponential increase in degree of ambiguity at higher levels. Stimulating intellectual abilities, gaining domain expertise, nourishing conceptual clarity and flexibility; widening the horizon; identifying, understanding and adroitly managing macro issues with strategic ramifications; ought to be emphasised in the PME. Towards that end, the JPME and SPME entail numerous training activities, structured courses and educational programmes. A candid assessment of the current system with specific focus on identifying the deficits, is discussed hereunder:-

(a) The joint training at the junior (tactical) and middle (senior tactical) levels is insufficient due to limited number of armed forces'

training institutions (AFTIs) - a work in progress. Without joint training at tactical levels, insufficient joint structures and lack of core competencies for joint operations; optimal joint application of force is difficult. Further, limited joint assignments & exercises and inadequate career diversity, result in exceptional depth in service specific knowledge but inadequate breadth - narrow horizon.

(b) Specific joint programmes / modules for self-directed learning at various levels of command do not exist. Reading, analytical thinking, critique, etc, deserve higher emphasis in units, to develop intellectual edge and superior decision making. The lack of habits of mind, affects the quality of research by the combat leaders, as they grow in service.

(c) The structured PME at staff colleges, CDM, war colleges and the NDC, affords ample opportunity to military commanders to build rapport with colleagues, within & outside the service and civilian attendees. PME at the CDM and War colleges is pitched at the tactical and operational levels; and prepares them to execute command tasks at these levels. However, the nuanced understanding of the Higher Direction of War is difficult to achieve. The transition from tactical and operational level to the Strategic level is, thus, only partially facilitated.

(d) At NDC, the highest level of structured course, that offers a six-stage curriculum the two subjects viz. 'Strategy & Structures for National Security' and 'Science & Technology' that are crucial for the military leaders for assimilating the concepts on higher direction of war, are weighted disproportionately low. This results in inadequate exposure of senior leadership to strategic studies, thus inhibiting the provision of qualitative advice at the strategic \level.

(e) At lower and mid-levels, the current system of PME leans disproportionately on the tactical aspects of operations in all stages of professional development; while limited exposure at

operational level is afforded to officers at the DSSC, TSOC and SC courses.

(f) Military campaigns, as part of the curriculum, exist in none of the premier military institutions, less the Naval War College. The study of major military campaigns is essential to stimulate understanding of the complex dynamics at play and the strategies engaged, besides, building of competencies to leverage competitive technology to outmaneuver the adversary.

(g) The strategic communication and perception management are introduced as part of PME at the mid-level, which is an impediment to requisite skilling at the formative stage.

(h) The research projects in the staff & war colleges and the CDM cover a very wide range of electives, to include military issues, subjects having national and international ramifications and abstract academic aspects. However, the quality of research needs substantive improvement. Besides, the electives lack focus on subjects that promote joint problem solving and pragmatic subjects of military value.

(j) Leadership skills development at the junior and mid-levels is aptly emphasised. While the IAF and IN already have the leadership programmes for junior and mid-levels, the IA has established a FACMIL (Faculty of Military Leadership) at the Army War College. However, formal leadership training at the NDC is not included in the curriculum.

(k) The current system does not adequately support the development of 'Joint Warfighting Skills' to include joint doctrine, joint strategy, joint planning, joint operations, joint logistics and sharing of assets. In simple terms, the true jointness in 'Thought, Action and Application' and congruity in Policy, Strategy and Doctrine, remains to be achieved.

(l) Reputed 'Think Tanks' viz. CLAWS, CENJOWS, CAPS, NMF, Observer Research Foundation (ORF), MP-IDSA and USI offer fellowships and provide immense exposure at National and International levels; and afford the fellows, opportunities to interact with the industry, civil administration and research organisations at the apex level. However, we need to leverage these 'Centres of Excellence' more towards joint warfare, National Security Strategy and policy formulation.

(m) Powerhouses of technology are the big multi-national companies and unfortunately the Defence Forces do not have any immersive presence, with the exception of IN, in Naval R&D. The current system of Project Management Teams (PMTs) merely assists in coordination between the lead directorate and the vendor, which is grossly inadequate.

(n) Education of military leaders on 'cyber strategy and operations', both from offensive and defensive perspectives, faces several challenges. The War & Staff Colleges and the NDC need to accord enhanced focus on the use of cyber capabilities as offensive weapon for shaping the battlefield for conventional operations and counter-measures against cyber threats to own networks and critical military assets.

The ibid deficits underpin the need to re-align our PME, to achieve the desired team goals.

Re-aligning the PME – Where do we stand

The hierarchy at the service HQ and Integrated HQ have realised the inevitability to re-align the PME, in view of the 'Felt Need'. While some progress has already been made, the work continues in the right earnest.

Indian Defence University (IDU). Conceived in 1967, the necessity of IDU was realised post Operation Vijay (1999) and the Government laid the foundation, at Gurugram in 2013. The bill is currently awaiting passage in the Parliament. The IDU, broadly envisioned as a teaching

and affiliating University to promote higher education and research in National Security Studies, Defence Technology and allied areas; would serve as a 'Think Tank' contributing to policy formulation and create competencies related to national security issues.

Promoting the JPME. The creation of Integrated Theatre Commands (ITCs) is imminent, as the roll out of Air Defence and Maritime Commands is well set, with final validation exercise in full swing. The action to achieve enhanced joint training is being pursued with a plan to set up a Joint Training Command (JTC). Besides, all training policies and methodologies, including foreign training will be handled by a single agency.

Actions at the Service HQ Level. The mandate for PME in the IA has been assigned to the ARTRAC, as the single Nodal agency. Enhanced effectiveness of training, better coordination, pursuance of research in-line with the organisational objectives, utilisation of facilities offered by civil institutions and avoidance of duplication of efforts are some of the benefits that have already begun to be realised, slowly moving towards 'Tri Services Joint Training Command'.

Focus at the Formation Level

(a) **Ideas and Innovations.** Several Army formations, have taken lead to inculcate and encourage the spirit of inquiry, research on contemporary technologies, ideas and innovations. The initiatives include the Command Availability Model for Training (CAM-T), research and publication by officers on subjects of military value, formulation of proposals for major R&D projects in contemporary technologies and R&D projects in collaboration with trade having a direct impact on the battlefield. Further, qualified M Tech officers are encouraged to conduct feasibility studies & research on futuristic technologies and platforms.

(b) **The Knowledge Repository.** The web pages of formations, have separate modules that make unclassified

research papers, articles and publications readily available to the military leaders. Besides, the facility to upload research papers, provides tremendous encouragement to write on varied subjects.

Comparative Approach by Various Countries

A wider view of some of the global leaders in their pursuance of the conduct of PME to build the military leadership is revealing, as discussed in subsequent paras.

USA

(a) **Aim.** To develop strategically minded joint warfighters, who think critically and can creatively apply military power to inform national strategy, conduct globally integrated operations, and fight under conditions of disruptive change.

(b) **Method / Frame-work:-**

(i) Adapt and innovate PME.

(ii) Infuse joint context throughout officers' careers.

(iii) Leverage joint exercises and develop practical warfighting skills.

(iv) Adapt and innovate talent management.

(v) Demand and reward academic excellence.

(vi) Identify and develop strategists.

(c) **Intended Outcome:-**

(i) Warfighting joint leaders, staff officers and strategists.

(ii) Anticipate and lead rapid adaptation and innovation.

(iii) Operational to strategic levels warfare.

(iv) Execute and adapt strategy through campaigns and operations.

Peoples Republic of China

(a) **Aim.** To Build and develop military skills required to lead the next level of combat operations.

(b) **Method / Frame-work:-**

(i) Initial focus on skill building.

(ii) Tactical and operational training.

(iii) Single-service and combined arms tactics training for field grade officers.

(iv) Single-service and joint campaigns for senior officers.

(v) Training in real combat conditions and Mission-oriented training.

(vi) Strategic-level training and joint training at Theatre Commanders' level.

(vii) Simulated, networked and force-on-force training.

(c) **Intended Outcome:-**

(i) An expert strategic war fighter who always listens to orders.

(ii) Develop a new generation of human talent.

(iii) Develop broad traits: -

(aa) Political loyalty.

(ab) Strategic awareness and skilled in military affairs.

(ac) Appropriate military culture.

(ad) Adaptive and intangible traits.

Israel

(a) **Aim.** To shape and empower the professional cadre of Israeli military forces.

(b) **Method / Frame-work:-**

(i) Initial focus on military and leadership skills.

(ii) Analyse military battles and history.

(iii) Study of strategies and doctrines.

(iv) Varied levels of PME at Israel NDC, Command and Staff Colleges.

(v) Constant investigation and study of strategic and operational environment.

(c) **Intended Outcome:-**

(i) Develop intellectually high-quality officers.

(ii) Mental resilience and leadership.

(iii) Command and control.

(iv) Application of the combat doctrines.

(v) Decision making.

Australia

(a) **Aim.** To develop mastery in the profession of arms and cultivate an intellectual edge in warfighting.

(b) **Method / Frame-work.** Divided in three parts: -

(i) Developing a future intellectual edge.

(ii) JPME continuum – agile and adaptive.

(iii) Application of the curricula – outlines processes, structures and initiatives to implement JPME.

(iv) JPME conducted at varied levels.

(c) **Intended Outcome:-**

(i) Command, leadership and ethics.

(ii) National security policy and strategy.

(iii) Joint warfare – planning and execution.

(iv) Technology and capability.

India

(a) **Aim.** To optimally synergise training efforts to operate jointly and continuously evolve and maintain capability to do so, in keeping with the principle that "We ought to train as we shall need to fight as we will fight only as we would have been trained''.

(b) **Method / Frame-work:-**

(i) Focus on combat and leadership skills in PCT and BMT.

(ii) Single service PME till senior tactical level.

(iiii) JPME at mid and higher levels at Staff Colleges, CDM, War Colleges and NDC.

(iv) Joint exercises and cross attachments.

(v) Study of doctrine, strategy and tactics at varied levels of PME.

(vi) Grand strategy and civil- military fusion at the NDC.

(c) **Intended Outcome:-**

(i) Strategic awareness and professional competence.

(ii) Effective command & control and Combat abilities.

(iii) Military and National Security Strategy.

(iv) Tangible and intangible qualities.

(v) Science and technology.

(vi) Professional military ethics, perception management and civil- military fusion.

Addressing The Outcome Deficits

We Ought to Train as We Shall Need to Fight, as We Will Fight Only as We Would Have Been Trained.

"Joint Training Doctrine of Indian Armed Forces"

The multi-domain, complex wars of the future, with battle space extended beyond the land, air and maritime boundaries, opening of virtual fronts like cyber and electromagnetic spectrum, the imminent employment of autonomous lethal platforms and robots based on AI, along with hybrid content; demand a multi-disciplinary approach to military strategy. The future war demands a change in emphasis and urgency. What is needed is an agile and well trained mind, to envision, to prognosticate and propel change. The PME should, therefore, focus to develop military leaders as scholar warriors, armed with leadership traits to include Tangible qualities (combat skills, technical expertise, fitness etc), Command abilities (planning and conduct of operations at Tactical, Operational and Strategic level, as applicable; and visualise how a military situation may evolve in future), Intangible traits (creativity, leadership, communication, analytical abilities, cogent thinking, action in the absence of orders, leading from the front, quick decision making, pride in military customs and traditions, loyalty and integrity) and Strategic Awareness (recognise own role in the system, understand the bigger picture, possess breadth of knowledge – broad horizon and a coherent worldview). Besides, the commanders should be able to effectively carry out joint planning and seamless execution of joint operations. Recommendations to develop professional mastery, enhance the intellectual edge and promote jointness through JPME are discussed in subsequent paras.

Blend Realism and Intellectual Ability. The re-aligned curricula should facilitate to develop the military leaders as a 'Blend of Realism and high Intellectual Ability'. Combination of 'Ground Observation and Theory', to develop cogent thinking and enhanced operational effectiveness, must be emphasised.

Joint Training for Joint Operations. 'Train Together to Operate Together' is the mantra to maximise synergy in the future wars. Enhancing the number of joint exercises, increasing vacancies for sister services in War Colleges, cross attachments, joint planning of operations, sharing of logistics and training assets; should be immediately considered. Inter-Service Camaraderie, operational & technological orientation, sense of collective ownership and jointness in thought would be noticeable within

2-3 years of vigorous implementation of JPME at all levels. The Joint Training is a fundamental requirement to achieve jointness in operations. However, we require synergetic efforts across the Defence Forces to establish joint structures, processes and curricula to implement the JPME, which will result in cultural and intellectual shift from the single service norm.

Wargames and Exercises. The objective of wargames and exercises should be to explore innovative ideas on doctrine, concepts, strategy and tactics; and not merely validating the existing operational plans. The game should include not only combat commanders, but logisticians as well, to share their perceptions and value judgments. Besides, there is a requirement to evolve a methodology to assess the 'Measure of Effectiveness' of war games and exercises.

Soldier Scientists. Development of technical officers as 'Soldier Scientists' with core competencies in niche areas viz. PGMs, AI, Robotics, Quantum Computing, Cyber Technology, Mobile Communication Engineering, need to be focused upon. Besides, long attachments of qualified technical officers to the big multi-national defence companies would facilitate development of joint enabling futuristic technologies. Adequate focus on the enterprise resource management (ERM) for better management of military logistics and assets is recommended. Further, the institution of 'Idea Acceptance Awards' is recommended to encourage innovation and R&D.

The Research and Outcome Validation. The 'Electives' for fellowships and study leave in Think Tanks, premier military and civilian institutions; should be focused on Science & Technology, Military & National Security Strategy or fields that contribute to achieve the organisational goals. Besides, suitable methodology for validation of research outcome be formulated and plagiarism, in all forms, dissuaded.

Research Guides and Master Research Assistants. For research in War Colleges, CDM and NDC; the 'subject scholars' should be appointed as Guides and honorarium paid from a Central Defence Research Corpus, created under the aegis of HQ IDS. The corpus should also

facilitate purchase of the material for literature review. Further, the concept of 'Master Research Assistant' is recommended for providing professional assistance.

The Knowledge Bank. Setting up of 'Knowledge Bank' or 'Digitised Libraries', which are networked and accessible to all military-men, can give a fillip to the distance learning with both, push (e-mailing of reading material and modules) and pull (accessing digital libraries) models on digital devices.

Recommended Professional Reading List. HQ IDS and the Training Commands should articulate and publish 'Recommended Professional Reading List(s) to cover History & Heritage, Military Leaders, Military and National Security Strategy, Operational Art, Disruptive Technologies etc, to guide the military leaders in self-learning.

Accreditation to Renowned Universities. The military training establishments should be affiliated to the institutions of Global repute. The affiliation of management oriented military colleges viz. CDM and CMM Jabalpur to IIMs; the engineering institutions viz. MCTE, CME and MCEME to IITs; the NDC, War Colleges and Staff Colleges to IDU, will add value to the military education gained by the military commanders during service.

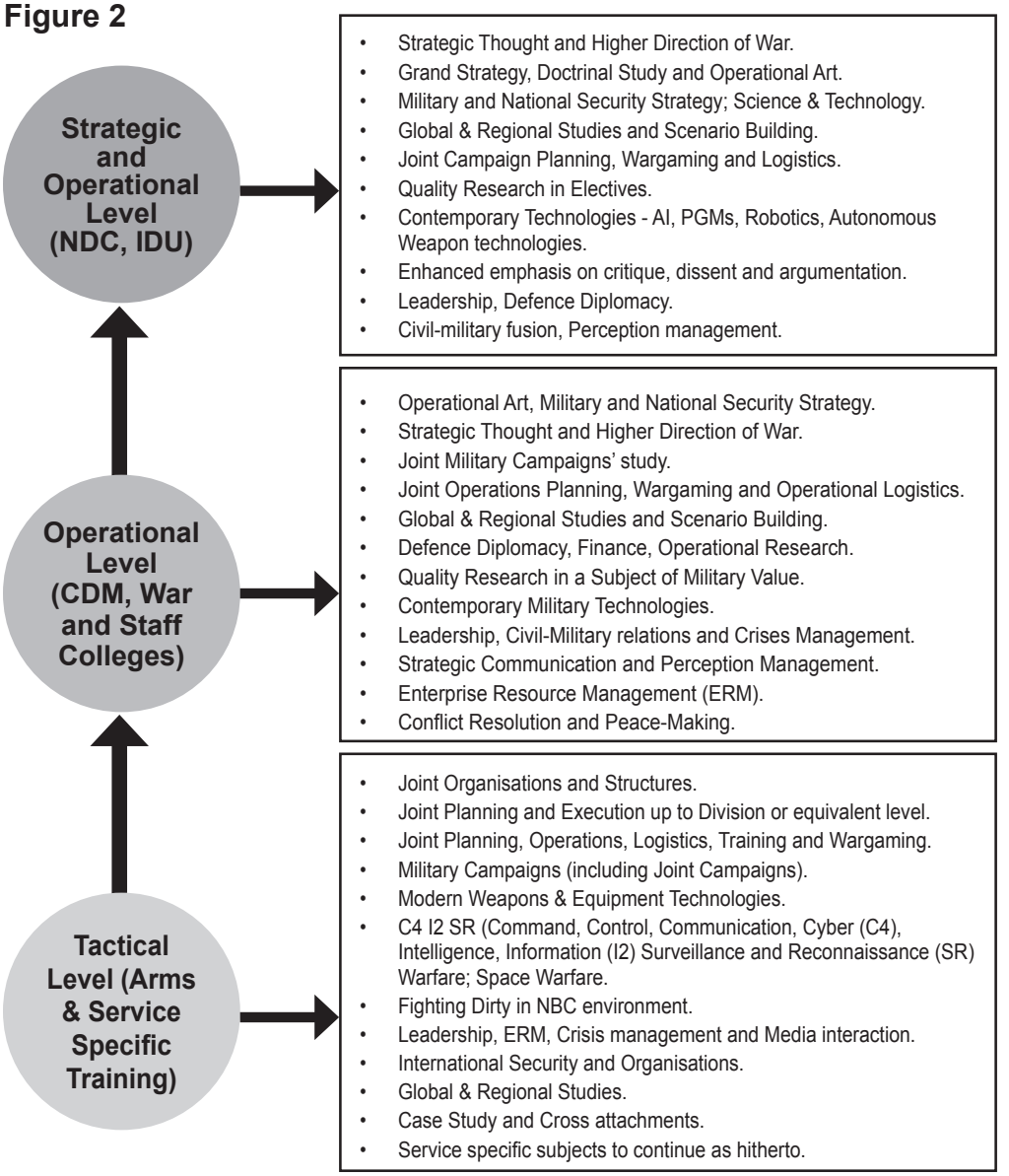
Education in Cyber Domain. The Staff & War Colleges and NDC need to formulate curricula to educate the military leaders to understand the cyber & information environment and the core concepts critical to the cyber domain. Commanders, across the board, should have fundamental understanding of cyber capabilities in both offensive and defensive operations.

Habits of Mind. The JPME should focus to inculcate the habits of the mind to include reading, critical thinking and cognitive ability; to outthink and outlast our adversaries in war amidst fog of uncertainty and disruptive change.

Designing the Curriculum: A Broad Framework

Creating strategic awareness, intellectual ability and mental agility that we require can be achieved by a balanced combination of education, training, exercises and rigorous practical application. Towards that end, a broad framework is suggested hereunder:-

Figure 2



Evaluation System. A system of evaluation, based on feedback, is essential to gauge the effectiveness of PME and determine how well the system as a whole will operate. Constant assessment, adjustment, modification and mid-course correction should continue as an ongoing process, in consultation with the environment, to address creatively our critical operational requirements.

Conclusion

Effectiveness of the current system of PME is fairly satisfactory; yet, the scope for further refinement and re-alignment exists. Change is the only constant and we must be ready to adapt to the changing requirements. Broad horizon, creativity, analytical thinking, appetite for calculated risks, quick decision making, agility of mind and strategic awareness; are the desired attributes of successful military leaders. Well balanced education and training during peace would keep the military leaders primed; and fetch us dividends in war. As the Integrated Theatre Commands are imminent, an increase in number of joint exercises, cross attachment of officers & troops in inter-service HQ, formations/ units and joint training from the lowest level; would strengthen the 'Spirit of Jointness', in thought, action and application. The re-alignment of PME, already in progress, must be pursued with speed and in right earnest. To jointly safeguard our National Security Interests with confidence, we must 'Train Jointly to Operate Jointly'.

***Lt Gen Atulya Solankey,** AVSM, SM, is DCIDS (PP&FD), HQ IDS.

ENHANCING PREPAREDNESS FOR CHALLENGES IN THE CYBER, EW AND IW DOMAINS

Brig (Dr) Navjot Singh Bedi*

Abstract

Mobile technology has integrated a number of technologies as multiple applications have converged into singular devices (ie mobile phone/ tablet/ laptop), with the ability to transmit wirelessly. However because of this, data based attacks can now impact the voice channels also, as voice over IP (VoIP) protocol allows voice to be carried over the data networks. On account of being a wireless device (and being the gateway to internet), mobile phone is therefore susceptible to exploitation of the Electro Magnetic (EM) spectrum. These mobile devices may have thus become a potent platform for propaganda (ie IW) as is often seen in the valley, for Cyber related activities but are consequently also susceptible to IW, Cyber Warfare and EW because the means to access & infect a computer network are now available at physical layer in the form of Radio Frequency (RF) linkages. Technologies like mobile phone, satellites, wireless backhaul radios, Software Defined Radio (SDR) etc in military networks are thus vulnerable to cyber-attacks through wireless channels also. Boundary lines between telecom, IT, Cyber, EW & IW domains have started blurring and there is a need to understand the role played by Cyber, EW and IW domains & the interplay between them.

Introduction

"War is but one of the ways of enforcing the political will of one nation upon another and is diplomacy by other means".

War is just an extension of politics and winning a war depends on achieving your political ends. More often than not, war is usually the last resort and since time immemorial, tribes and nations have waged wars. In times to come modern technology will enable warfare in many ways which were hitherto unimaginable. Technological growth includes incremental developments and disruptive technologies. The former is a development intended to follow on from the previous technology. For example the transition from flint lock and muzzle fed rifles to bolt action rifles and later on to semi-automatic rifles. Disruptive technologies however are those where a new method replaces the previous technology and make it redundant, for example the replacement of horse mounted cavalry by Armoured Fighting Vehicles (AFVs).Future warfare is likely to be Multi Domain Warfare (MDW) which is envisioned as a more complex concept that will expand the operational scope and reach of a nation's strategic-military establishment and will include a number of disruptive technologies. Though there are many such technologies which will drive these changes and which will play a major role in all future conflicts, this paper will only discuss the role played by Cyber, EW and IW domains and in Enhancing Preparedness for meeting Challenges in these domains.

Cyberspace & Cyber Domain

There has been a surge in the internet usage at not only the global level, but at the national level as well. The COVID pandemic since the last year and a half has seen an upsurge in the utilisation of internet for business, education, e-commerce and has consequently increased our vulnerability to Cyber-attacks. It's important to understand that cyber-warfare refers to the use of digital attacks by one country or nation to disrupt the computer systems of another, with the aim of creating significant damage, death or destruction, either directly or indirectly.

Cyberspace has acquired strategic position by virtue of its global reach and its rapid integration into the social, political and economic discourse and framework. Malfunctioning or breakdown of a well-knit web may have serious implications on social well-being, economic and business interests of a nation. This section of the paper explains the subtle difference between Cyber Warfare (CW) and what cannot be classified as Cyber warfare, various response mechanisms for the same and capacity and capability building as a means of enhancing preparedness to meet challenges in this domain.

History: Disruptions in Cyberspace. In 2007 cyber war went from theoretical to actual, when Estonia found itself under a furious digital bombardment that knocked banks and government services offline. However, the DDoS attacks on Estonia did not create physical damage and it was not considered to have risen to the level of actual cyber warfare. However, the Idaho National Laboratory proved, via the Aurora Generator Test, that a digital attack could be used to destroy physical objects; in this case a generator. Stuxnet malware in 2010 proved that malware could impact the physical world. In 2013 the NSA said it had stopped a plot by an unnamed nation to attack the BIOS chip in PCs, rendering them unusable. In 2014 the attack on Sony Pictures Entertainment, blamed by many on North Korea, showed that it was not just government systems and data that could be targeted by state-backed hackers. In Dec 2015, hackers managed to disrupt the power supply in parts of Ukraine, by using a well-known Trojan called Black Energy. In March 2016 seven Iranian hackers were accused of trying to shut down a New York dam in a federal grand jury indictment. Nations are rapidly building cyber defence Nations are rapidly building cyber defence and offence capabilities. NATO in 2014 took the important step of confirming that a cyber-attack on one of its members would be enough to allow them to invoke Article 5, the collective defence mechanism at the heart of the alliance. In 2016 it then defined cyberspace as an “operational domain” ie an area in which conflict can occur: the internet had officially become a battlefield. In Oct 20, the Cyber-attack that shut down the

electrical grid of Mumbai, plunging millions into darkness, was reportedly a Chinese cyber-attack (as suggested by the New York Times). The 07 May 21 ransomware attack on Americas Colonial Pipeline was reportedly carried out by a criminal hacking group, for which the ransom in crypto currency of 75 Bitcom ie nearly USD 5 Million was paid. After this attack the US President signed a Cyber security executive order, establishing a series of initiatives designed to letter equip federal agencies with Cyber security tools and encourages improvements in digital security standard across the private sector, which has been hit by a spate of Cyber-attacks.

Implications. Cyber warfare or Disruptions in Cyberspace is going to be a significant component of every present and future conflict. Future wars will also be fought by hackers using computer code to attack an enemy's infrastructure, as well as troops using conventional weapons like guns and missiles. But unlike standard military attacks, a cyber-attack can be launched instantaneously from any distance, with little obvious evidence in the build-up, and it is often extremely hard to trace such an attack back to its originators. Modern economies, underpinned by computer networks that run everything from electricity, transportation sanitation to food distribution and communications, are particularly vulnerable to such attacks, especially as these systems are in civil domain, and are rarely designed to be secure against hackers. Thus digital attacks against vital infrastructure like banking systems or power grids, give attackers a way of by-passing a country's traditional defences. As per some experts, it's a case of when, not if.

Cyberwarfare vs "Not Cyberwarfare". Whether an attack should be considered to be an act of cyber warfare depends on a number of factors to include the identity of the attacker, what they are doing, how they do it and how much damage they inflict. Like other forms of war, cyber warfare is usually defined as a conflict between states, not individuals. As cyber war is best understood as conflict between nations, then that excludes a lot of attacks which are sometimes described as cyber warfare. For example attacks by individual hackers/ groups of hackers, would not usually be considered to be cyber warfare, unless they were being aided

and directed by a state (which is however a dangerously common trend). For example, cyber-crooks who crash a bank's computer systems while trying to steal money would not be considered to be perpetrating an act of cyber warfare, even if they came from a rival nation. But state-backed hackers doing the same thing to destabilise a rival state's economy might well be considered so. The nature and scale of the targets attacked and weapons used is another indicator of the differentiation. Defacing an individual company's website is unlikely to be considered an act of cyber warfare, but disabling the missile defence system at an airbase would certainly come at least close.

Continuum of Conflict. A moot point is that Cyber warfare does not take place only during actual hostilities! In this hyper connected digital world of ours, Cyber warfare is an everyday reality and without formally realizing it or acknowledging it, Cyber warfare related activities are already being carried out by various parties, (ie Individuals, Hack-activists, Non State Actors, State Supported Actors/ Direct State Involvement) during Peace, Low Intensity Conflict, Mid Intensity Conflict, High Intensity Conflict. Live cyber threats are in fact an ongoing process and all our actions need to be aligned to it. There is thus a pressing need to put in place response mechanisms to address these emerging challenges.

Present Capacity & Capability Building for Emerging Cyber Challenges

Cyber Capabilities of Two Nations. The best way to arrive at a figure on the Cyber qualified HR required is to take a cue from the capability of few nations. It is in comparison to all these that India needs to put in place a credible Cyber Force. Details of the same in respect of two nations are as listed below:-

(a) **China**. It has an established PLA Cyber Command & Strategic support Force (SFF). It can bank upon a dedicated force of 7000 persons but the strength may increase to 130,000 persons including the Cyber militia (which could be banked upon to augment the Cyber Force in times of hostilities). The

Mandaint Report lists out the Cyber capabilities of China. The Chinese JSD4 is a specialized unit dedicated for this activity. In the Chinese Philosophy, Electronic Warfare (EW) and Cyber Network Attack (CNA) are inter-mixed and they even talk in terms of Electro Magnetic Space Operation (EMSO). The EW and Cyber Operations are thus addressed in a combined manner. The Chinese also have a specialized unit i.e. Unit 61398 which is a part of JSD3 Deptt. A large number of Advance Persistent Threats (APT) (e.g Titan rain, Aurora etc.) have been rumoured to have been developed there.

(b) **USA.** US Cyber Command unifies the direction of Cyber space ops, strengthens DoD Cyber Space capabilities and integrates & bolsters DoD's Cyber expertise. As per literature available in open source, the cyber mission force available with the US Cyber Command is 133 Cyber Mission Teams (CMT's). The composition of these teams varies from 50-100 members each. The USA has approximately 6000 Cyber warriors. Their Cyber force is divided into 133 teams of which 60 are Defensive Cyber Warrior Teams and 73 are offensive in nature. These 133 Cyber Mission Teams are further sub divided into five different types of teams. These teams and their role and tasking, is equally applicable in the Indian subcontinent. These five types of teams are :-

(i) **National Mission Team (NMT**). Specialized Cyber Operations teams which would execute plans having implications at the national/ strategic level i.e. they provide support to Strategic Operational Plans.

(ii) **National Support Team (NST)**. These would provide analytical support to NMT and would be a team of highly skilled Cyber Technicians who would be employed to develop the cyber weapon to be launched by the NMT. Taken together, we may loosely assign the role of NMT and NST to the role

that is currently being performed/ envisaged to be performed by National Technical Research Organisation (NTRO) at strategic level, in India.

(iii) **Cyber Mission Teams (CMT)**. The CMT will be closely associated with the Operational plans at the Combatant Operational Command level and will provide cyber support for the same i.e. for the various theatre commands.

(iv) **Combatant Support Team (CST)**. The CST will provide analytical support to the CMT i.e. akin to analytical support being provided by NST to the NMT.

(v) **Cyber Protection Team (CPT).** The cyber protection team will have a primarily defensive role, which may be akin to the role of ESM (Electronic Support Measures), in the context of Electronic Warfare.

Present Capacity /Capability. Approximate 1500-2000 Cyber trained personnel are available with various Govt agencies and in private sectors the approximate capacity available would be about 15000 to include National Security Data Base (3000 plus), InfoSec Community (5000), Talent at School\Colleges & IIT's etc (3000 plus), Start-ups involved in new tech like AI\Robotics (1500 plus), and Independent Actors\Freelance Cyber Security Analysts (2000 plus).

Capacity Required. There is a need to put in place a frame work to bring clarity in the capacity required for various cyber security roles which are:-

(a) Undertaking R&D in new technology.

(b) Implementing existing technologies.

(c) Managing existing ICT infrastructure.

(d) Securing ICT infrastructure.

(e) Managing ICT infrastructure.

(f) Having adequate HR to fill all cyber related posts to undertake the tasks listed above is a practical way to put a figure on the HR required and a figure of 50,000 is a good figure to work with. However putting a cap on the type of Networks/ systems needed is rather difficult. It is thus evident that as on date, the force available with India needs to be considerably augmented.

Capability and Role. It can be seen that we need developmental teams to develop a Cyber weapon and operational teams to optimally launch the exploit. Since these are specific task oriented special units, hence their equipment profile and manning norms will be different, will be dictated by their role and are likely to be dynamic. However, as per the template being followed internationally, it can be safely assumed that each unit would require between 50-100 personnel. The availability of highly skilled cyber trained personnel and their retention is another issue which needs to be addressed.

Knowledge Sharing. Though individual groups of experts in this field often share knowledge / experience but these are exceptions rather than the norm. There is negligible expertise in development of Operating System (OS). The Service Sector needs to step in this field and if we have to be taken seriously as a nation, then like China, we must develop and use our own indigenous Operation System

Capability Demonstration. Of late there has been no capability demonstration to showcase our potential. Such a capability demonstration (as was witnessed in the Cyber-attack on Estonia), is essential and akin to a controlled nuclear explosion as it acts as a deterrence and wards off adversaries/ potential adversaries. There is apparently a lack of developmental activities to produce a “Stux Net” type of weapon (which possibly entailed four million man hours of research work by a joint team of personnel from two developed nations). Such a weapon, if indigenously developed is a game changer. This was an ideal Cyber weapon which was intended for re-use and gave three to four zero day

exploits. It was a type of Cyber weapon which is developed once in a century and was not intended to be exposed to the world. However its effect beyond anticipated reach, led to it being analysed in detail and to its subsequent exposure.

Human Resource. This is the “Achilees Heel” of this programme as the required number of skilled personnel are neither readily available nor have they been tapped. As explained, approx 6000 personnel are required to man and equip 133 functional Cyber Operations units of USA, which works out to roughly the strength of two infantry brigades. This figure may seem miniscule compared to the 1.2 million strong standing Army that India possesses but it may come as a surprise to many that it is extremely difficult to identify, recruit, train and retain this limited pool of manpower in such a niche field.

Identification & Recruitment of HR Talent. The people gifted in this field (yes gifted & not trained or skilled) are few and far between & hard to find. These are not your stereo type academically inclined individuals who will crack the UPSC exam for selection into Cyber Command. Nor would they be the type who conforms to the standard norms of military discipline. Such individuals would more often than not be rebels or non-conformists. They would be brilliant (possibly bordering on the edge of eccentricity) and focused only on cyber related activities (hacking, cracking, launching exploits, trolling the web etc).They might even be adjudged as misfits in society. An ideal Cyber warrior would not necessarily only be young teenage kids who are cyber savvy. An ideal Cyber Warrior would in fact be a person who has at least 10 years of experience in this field and who has moved on beyond the thrill of cracking a password or hacking into an account or defacing a website. However age and conventional experience would be required to be disregarded if we intend to nurture & recruit talent. This is so because its quite likely that the young disinterested teenager, who is forever busy on his play station PSP-3 or is a social misfit (preferring PC’s & on line face book chatting rather than face to face talk), might be a potential recruit to be one of your potential cyber warriors. It is in a way akin to the lateral

induction of JS level officers into the bureaucracy, as proposed by our Hon'ble PM, which was opposed by the entrenched lobby-but the moot point is are we ready for that in the Armed Forces?

HR Capacity Building. The approach should be long term. It must be analysed as to who would be the people in the field 15 years from now and the effort to train them should start from today. This is not just about recruiting people from the private sector and altering QRs to suit them to serve in sensitive government agencies. Instead, an effort should be made to develop them within the respective government agencies. The best example of one such long term recruiting programme is the SSB/ NDA exams and recruitment for the defence services. A similar approach should be carried out in identifying the Cyber specific talent very early and building up and nurturing the same. There is no better agency than the defence services to do this job. The Recruitment & HR policies to attract and retain suitable talent in field of Cyber space can be structured suitably.

Israel Model. Israel's programme of conscription for two years for serving in the **IDF** is for all citizens. However from amongst this pool of HR, the best talent who show technical capabilities, is supposedly identified and provided with an extended tenure of nine years, during which period they build the best systems for the Defence Services. The Israel govt identifies new technologies where R&D and manufacturing capability (ie Business requirement) exists and people with these skill sets leaving the IDF are given responsibility to create start-ups in these niche fields. The recruitment programme for India should thus incorporate both technical aspects to Capture. The Fire (CTF concept), as well as psychometric tests to discern the passion quotient of the prospective candidates.

Technology Capacity Building. India could identify a couple of high technology areas like IC fabrication, 5G & IoT, Propriety Communication Technology, AI, Cryptography & Pure Mathematics and pump in money into R&D to develop indigenous models of the same. An economically priced model of this could be mass produced for commercial supply,

in order to capture the market and generate profit. The profit could be used to further improve the product, which could then be priced slightly higher for supply to elite group of customers and possibly later compete at the global forum also, thus generating more profit. Hopefully the cycle would make our product manufacturing self-sustaining and perhaps even profitable. In order to achieve this, there is a need to develop new R&D facilities and nurture new faculty and suitably reward, acknowledge & retain talent in order to build indigenous items as per global scenario.

Immediate Mitigation Techniques. While capacity & capability building may take time, measures pertaining to People, Processes &Technology can be taken immediately. These are:-

(a) **People**. Continuous awareness campaign, trained system administrator, operational & functional Security Op Centre (SOC) & periodic engagement with LEAs.

(b) **Processes**. There should be a regular Cyber drills including Business continuity Plans (BCP) and Disaster Recovery (DR) plans must be in place and rehearsed.

(c) **Technology**. All internal PCs must be scanned thoroughly with end point protection and AI based behavioural detection platforms should be used to monitor probable suspects. Honeypots could be used to lure and find Red Flags and one can consider using VMS/ appliance for internet browsing. In addition measures be addressed for hardening of devices.

Research & Development (R & D) Support Wing. Offensive Cyber Ops Units can't be expected to develop Cyber Weapons (as is generally expected of various Cyber organisations). For development of graded cyber weapons we are not looking at tapping "Script Kiddies". We need to develop and carry out hard core research. These developers would be distributed amongst various Cyber Operations Support units/ teams and each unit will be unique and different and will be involved in development of a Cyber weapon for use by a Cyber Operations Unit. This wing is in fact

a key enabler of the capability of cyber agency to translate the intent into action. The range of R & D activities will be very wide and will start from the requirement to evolve platforms to fire and control Cyber Weapons. Development of indigenous Penetration Testing tools (of the standard of Core Impact, Impact Canvas, Metasploit etc) would be another key task of the R&D wing. The entire "exploit" should to be properly packaged and should facilitate ease of use by the Cyber Operations Unit.

Cyber Doctrine. A Joint Cyber Operations Doctrine needs to be promulgated at the earliest. Guiding principles for such a doctrine should include that the following: resources for Offensive Cyber Operations must be deployed down to tactical levels. In any scenario involving state-to-state conflict which may not necessarily imply declared hostilities but also hostile actions attributable to adversary state, the primary authority/ responsibility for Cyber Ops should rest with the MoD/Armed Forces, including authority over cyber resources available with other ministries. In addition a completely fresh HR and training philosophy should be evolved to meet the unique needs of Cyber Ops.

Cyber Training. Structured training for Defensive Cyber Ops is already being carried out by the three Services. Extensive training for Offensive Cyber Ops, right up to post-graduate level, should be carried out at respective premier training institutions within the three Services (for example, Naval Signals School Kochi for Navy and AFTC for IAF and Military College of Telecommunication Engineering for the Army). Efforts should be made to sponsor specialist post-graduate courses in Cyber Ops, including ethical hacking, to be conducted at leading educational institutions within the Country and abroad.

Electronic Warfare & Information Warfare Domain's

EW being a precursor to IW but now comprises part of IW, hence both are being discussed together, with the aim being to suggest Information Warfare (IW) and EW structures which are effective enough to match up to the challenges of 21st Century warfare. However, given the existing

status of EW & IW preparedness of our Armed Forces, the viability requirement is, perhaps, the greater challenge. Thus, in order to move pragmatically from where we are to where we wish to be, this analysis adopts a transformational, as opposed to a revolutionary approach towards achieving the desired capabilities. Though EW is an old and established concept, yet is still evolving. However IW being a nascent, complex and dynamically evolving field of warfare, developing the conceptual and doctrinal basis for IW structures is an important first step. Equally important, in this highly specialist field, identifying the right human resource (HR) philosophy is at least as important as arriving at optimum organisational structures and should, in fact, be a driving parameter while arriving at choice of structures. *[1]*

Concepts Doctrine & Existing Organisational Structures

EW. There is an on-going debate in the US Department of Defence (DoD) whether or not a sixth domain, namely the Electro-Magnetic (or EM) Domain, needs to be added to the existing five-dimensional battle space construct.[8] The motivation for such thinking is the increasing importance being accorded in the US to developing Electronic Warfare (EW) capabilities after decades of neglect, perhaps spurred by the rapid advancements made in this field by formidable potential adversaries, particularly China.

IW in 21st Century Battlespace. IW was previously nothing more than just a supporting means for conducting a kinetic multi-domain battle in the physical domain. Today, however the scenario is radically different, with the US having established a Cyber Command in 2010,[2,3] China working with fervour to achieve dominance in the information domain by building capabilities, notably its Strategic Support Force (SSF),[4] and most significantly, Russia demonstrating an increasing degree of maturity in the IW field, going by the success of its information campaigns in Estonia, Georgia and Ukraine.[5] The powerful role of social media in the de-stabilisation/overthrow of established regimes during the Arab Spring (which in Russian perception, was the result of “subversive information

technologies of the West"), brought in a new dimension to war-waging in and through cyberspace.[6,7] The concept of *Information* Warfare took root in the 1990s and has matured remarkably after the turn of the century.

IW Doctrine. The first Joint IW Doctrine was issued in 2005, which was revised in 2010, the current version. The first Indian Army (IA) IW Doctrine was issued in 2004. A revised doctrine was subsequently promulgated in 2010, which is the current version.

Tri Service IW Establishments. At the tri-services level, there are two organisations related to IW: the erstwhile Defence Information Assurance and Research Agency (DIARA) and the Defence Intelligence Agency (DIA), both functioning under the aegis of HQ Integrated Defence Services (IDS).[9] Originally established as the Defence Information Warfare Agency (DIWA), DIARA subsequently got re-designated with it's focus being on Cyberspace Operations. DIARA has recently been upgraded to the Defence Cyber Agency (DCyA), which is hopefully a precursor of the Cyber Command proposed by the three Services. The DIA coordinates the intelligence effort of the three Services and provides a common interface with the civil intelligence community. DG DIA is a member of the Intelligence Coordination Group, which works under the NSA. He is also a member of the National Information Board (NIB) as well as the Apex Committee on Satellite Surveillance Board. He controls the strategic assets like Defence Imagery and Photo Analysis Centre (DIPAC) and Signals Intelligence (SIGINT).

Individual Service Specific IW Establishment. Integrated employment of Information Operations (IO) is being carried out as a staff function at various headquarters. At Army Headquarters level, the Additional Director General Military Operations (ADG MO) (IW) is responsible for all aspects of Cyber, EW and PSY Ops. Similarly, the Indian Air Force (IAF) has the Directorate of IW. The ADG Public Information (PI) is an ad hoc organisation in the Army chartered to carry out the Public Affairs / Information function. As regards field formations, specific IW related staff set-ups exist at some higher headquarters, while at others this function

is carried out by the operations staff officers in addition to their other duties. As regards individual IO functions, establishments exist for the Cyber Ops and EW functions, but not for Psy Ops. The defend function for Cyber Ops and EW is the combined responsibility of all users of the network end-points and of the EM spectrum respectively. The specialist task of defence of common user networks (for both Cyber and EM spectrum aspects) is primarily the responsibility of the Corps of Signals in the Army (and its equivalents in the other two sister services).IW & Cyber establishments which are presently in existence are as under:-

(a) **Cyber**. The Army Cyber Group (ACG) is mandated to carry out all aspects of Cyber Ops for the IA, less the implementation of offensive measures. It also functions as Cyber Emergency Response Team (CERT)-Army. Some of its primary functions include cyber audit, cyber forensics, cyber evaluation of new systems, etc. Policy formulation and cyber audit in the field formations is carried out under the aegis of IW staff, with the primary manpower resource for the audit teams being provided by Signals.

(b) **EW**. Army EW resource being scarce, EW groups/ sub-groups are presently placed directly under Command Headquarters from considerations of efficient utilisation. Notwithstanding this, their employment is entirely at tactical levels in close support to the fighting formations. The application of this resource is primarily for execution of the “Attack” and “Exploit” sub-functions. In the IAF and the Indian Navy (IN), EW effort mostly focusses on platform based non-communication (anti-radar) capability. There is a major capability building required to be undertaken in this domain.

(c) **IW/PSYOP**. Presently, there are no formal PSYOP establishments in existence.

(d) **Public Relations Organisation (PRO)**. Public Affairs (PA)

is the purview of Ministry of Defence (MoD) & its PR machinery ie PRO Defence. Regional PROs posted at various stations report to the PRO Defence and are not under local formation commanders or staff, thus remaining largely out of sync with the needs of our Armed Forces.[10]

Human Resource Development (HRD). Some of the main highlights of the HRD philosophy being followed by individual Services are as given below:-

(a) **Cadre Management**. In the case of officers, postings to all IW assignments (Cyber, EW, IW) are on tenure basis. For other ranks a special trade, common for SIGINT and EW tasks, exists in the Corps of Signals.

(b) **Training**. IW training for officers is conducted by Army War College, with some participation from the IN and the IAF. EW and Cyber Security training for Army officers is conducted by the Military College of Telecommunication Engineering (MCTE), Mhow which is the declared Centre of Excellence (C of E) for these disciplines. For the IAF, IW training is being conducted by their IW School at Bangalore. For subordinate ranks in the army, structured training for EW/SI is being conducted by the Signal Training Centres. Joint training is being carried out presently only on EW, on a rotation basis, by Army, Navy and Air Force and at their respective training establishments at Mhow, Kochi and Gwalior. There is some participation by the Navy and the Air Force on IW courses being conducted by the Army for officers at the Army War College, Mhow. PsyOP exposure is being given to officers as part of command oriented courses at various levels, or capsule courses at civilian institutions mostly on a volunteer basis. There is no specialist training being conducted within Services specifically for PSYOP or Strategic Communications.

Limitations & Suggested Remedial Measures

IW Doctrine. There is a need to substantially update existing IW doctrines at the Joint Services as well as individual Service levels. In view of the ambiguity in the definition of IW terminologies worldwide, these doctrines must make a deliberate effort to rigorously define terms as applicable in the Indian context. The doctrines must emphatically endorse the operational imperative that conflict in this artificial and virtual dimension is at par with the traditional notion of conflict in the physical realm and not is merely in support of it. The doctrines should characterise and classify Cyber Ops, EW and Psy Ops as the major streams of IW and as being distinctly different. An unequivocal stress must be laid on the critical importance of achieving specialisation in each of the IW functions, and a viable HR philosophy spelt out to meet this end.

EW Doctrine. *Joint Doctrine For Electronic Warfare: 2010* published by HQ IDS, Ministry of Defence (MoD) lays down the doctrinal concepts in EW domains. This document merits a review in light of the overwhelming advances in improved communication, information, surveillance, reconnaissance capabilities and net-worked command and control elements, which must be gainfully exploited to fight a high-tech warfare. A revised Joint Doctrine on EW, followed by separate EW Doctrines by each of the three Services, needs to be promulgated. The doctrines should emphasize the critical role of EW in 21st Century battle space, as well as the degree and manner of coordination with cyber resources, in order to achieve the desired synergy in military Infospace.

EW Organisation. The recently concluded Armenia – Azerbaijan conflict has brought to light the efficacy of Drones and a soft kill option against the same is through ECM using EW. With the ever expanding use of the EW spectrum for diverse weapon platforms, there is a need to enhance the number and capability of EW units. The quantum of Army EW units/formations needs to be significantly increased with the aim being to provide an EW Group per Corps HQ in order to provide the requisite EW support to fighting formations. Once additional EW

formations are raised, these should be placed under Corps Headquarter for integrated functioning, with EW Sub-Groups being placed in support of Divisional Headquarter. The model of Integrated Control Centres Blocks (Communication plus Non-Communication) is recommended to be adopted for optimal utilization of EW resources. ELINT resources should ideally be merged with the EW Groups. Strike Corps EW elements should be equipped to have matching mobility and be deployed well forward (within combat groups) for achieving a tangible force-multiplier effect. Specific requirements of providing EW support in mountainous and High Attitude Areas needs to be addressed.

EW and SI Units. The EW organisations are best structured to acquire tactical SIGINT through its ESM function. However, in Counter Insurgency (CI) scenarios within the country, SI units too, under the direct control of the Tri-Services SI Directorate, are deeply involved in this activity. Existing command and control structures are not conducive for achieving the requisite synergy between these two capabilities. Thus lateral sharing of intelligence at various levels in the hierarchy of these two organizations is recommended. Likewise, ELINT resources are currently placed under the Military Intelligence (MI) Directorate, whereas radar signatures collected by ELINT units are primarily meant to be exploited for ECM by EW units on outbreak of hostilities. Thus merging ELINT resources with the EW Groups would be an optimal solution.

EW HR Philosophy. HR philosophy for EW is recommended to be modified based on the following considerations:-

(a) **Cadre Management**. In general, a much higher degree of specialisation than what is presently existing is considered essential. In the case of officers, the postings policy must be modified to ensure repeated tenures in EW establishments. For instance, criteria for command of an Army EW Sub-Group/ Group must require at least one/ two prior EW tenures respectively. For other ranks, EW specific trades (operators/ mechanics) must be created and rotated strictly amongst EW units/ establishments (and not in SI units).

(b) **Training**. The quality and quantum of structured training at all levels, including through conduct of joint services courses, needs to be significantly upgraded. Also, specialist components of IW courses should be conducted by designated centres of excellence in the respective disciplines and select personnel be sent abroad to attend super specialization courses.

(c) **R&D and Project Management**. Skill development for execution of EW tasks is equally challenging as for cyber skill development. However project management for EW systems requires highly specialised expertise, especially as Indian R&D in this area is presently not comparable to global standards. A fillip to domestic R&D, can be given by including by private players, and by making special endeavours to obtain the best technology existing in the world market. The govt to govt procurement route be adopted for specialist technology as this may not be freely available. The quality of our Project Management Organisations (PMOs) in all three Services need to be improved and supported by giving project based long tenures to EW specialists in PMOs.

IW Doctrine, Cadre Mgt & Training. Future wars are likely to be characterized by ascendancy of technology. "Information Warfare Doctrine For The Indian Army: 2010" published by Headquarters Army Training Command (ARTRAC), lays down the doctrinal concepts in Information Warfare (IW). In order to develop IW to the desired degree of maturity, stiff resistance to modifying organisational charters as they exist today would first need to be overcome. Thereafter, considerable efforts will need to be devoted to developing expertise in all the IW disciplines, especially as regards building up narratives and management of social media, most of which happen to be in very nascent stages, especially in the context of the complex 21st Century battlespace.

(a) **IW Concepts and Training**.Limited exposure by way of short capsules on media management is being provided at the Institute of Mass Media, under aegis of HQ IDS and in some

of the command oriented courses at different levels of service. Commanders and staff entrusted with IW tasks, by virtue of their tenure-based assignments, carry them out mostly on the basis of their general military experience, as also on the strength of short-term institutional knowledge which might exist within their establishments. This ad hoc approach to Perception Management (PM) & IW disciplines needs to be improved upon, especially in today's information intensive world. Suitable steps be initiated for developing these disciplines to a degree of professional maturity, duly adapted to our strategic environment. A joint doctrine for IPO, covering concepts and employment modalities for individual functions as well as the interplay amongst them, needs to be promulgated. To the extent feasible, it is desirable to issue a similar doctrine (if not same) separately for the Army IAF & IN such that all the three services are in synch and reinforce each other's efforts. In this field, time is of essence and one cannot be found to be reacting. We should in fact have narrative ready for various situations/scenarios, with well laid out timelines / triggers for taking various actions. To the extent feasible, the authority to take action/ release media bytes, as per the planned & rehearsed narrative needs to be delegated to the GSO1 / Col (and equivalent rank officers) manning the desk at the instant, as time is of essence.

(b) **IW Cadre Management**. Although trained manpower for the IW disciplines is required by all the three Services, presently there is no specialist manpower available with any of the Services barring a handful number of people trained in capsule courses. A suitably structured tri-Service training institute should also be established as a centre of excellence under aegis of HQ IDS for the IW discipline of PM, Social Media & Info Ops. Initially training in these fields could be conducted at the Army War College. PSY Ops demands staff as well as ground resources for executing operational tasks. Specialist training needs to be imparted for

all personnel involved in PSY Ops tasks. Cadre management at officer level could be based on providing repeated tenures In IW / PI /PRO, after suitable specialist structured training has been imparted. The Defence PRO needs to be recast as per the operational needs of the Armed Forces to rise up to the challenges of the Social Media & Information Age. PRO should be placed under command of the Armed Forces and additional cadre may be recruited if needed. The ADG PI as an organisation should carry out its tasks through the IW cell/section at each formation Headquarter, down to the Corps Headquarter. The activities of these cells should be coordinated by the Operations staff at all levels. These cells must carry out 'truth projection', and be involved in the PSYOP functions of shaping the narrative in the Social media. Being a national effort, close coordination with the Ministry of Home Affairs (MHA) as well as Ministry of External Affairs (MEA) is needed for effective execution of IW tasks.

Conclusion

The potency and overwhelming lethal effects of Cyber warfare, Electronic warfare & IW has outpaced the technological development in conventional military weapons space, changing the very character of future wars, and the role of cyber warfare in them. A conceptual understanding of the large number of disciplines involved between Cyber, EW & IW and, more importantly, the interplay amongst them, is key to evolving optimum organisational structures. The key driver for bringing about the requisite improvement / transformation would be the conviction that the nature of warfare in this Information Age is changing in fundamental ways. The EW, Cyber & IW Ops do not merely support operations but at times lead / shape the conventional operations and may even preclude the use of conventional boots on grounds. All this demands, more than merely organisational changes, radically new models of HR philosophy, covering recruitment, training and career progression aspects for the technically inclined EW, Cyber & IW specialists. For this to happen, a

change in existing mind-sets is essential, which by far is the greatest challenge.

***Brig (Dr) Navjot Singh Bedi** is a former Senior Fellow Centre for Joint Warfare Studies (CENJOWS), New Delhi

Bibliography

1. Mathew S. Cohen, Charles D. Freilich and Gabi Siboni. "Israel and Cyber space : Unique Threat and Response". International Studies Perspectives (2015)0, 1-15.
2. Keir Giles. "Information Troops"- a Russian Cyber Command? Conflict Studies Research Centre Oxford, UK.
3. James A. Lewis and Katrina Timlin. "Cyber security and Cyber warfare.Preliminary Assessment of National Doctrine & Oganisation Center for Strategic and International Studies.
4. William Slater and Matthew Crosston, "A Brief Arief Analysis of Russian Cyberwafare Capabilities – Past, Present and Future".
5. Gil Baram. "The Effect of Cyber war Technologies on Force Buildup : The Israeli Case". Military and Strategic Affairs/Volume 5/No. 1/May 2013.
6. Colonel Deepak Sharma. "China's Cyber Warfare Capability and India's Concerns". Journal of Defence Studies.
7. Charles Billo. "Cyber Warfare : An Analysis of the Mean and Motivations of Selected Nation States". Institute for Security Technology Studies at Dartmouth College.
8. Joseph E Sission. "Fleet Cyber Command/Tenth Flee: Enabling Cyber Unity of Effort". July 2016 91
9. John.F.Sarkesain, Thomas W. O'Brien. "A Framework for Achieving Dynamic Cyber Effect through Distributed Cyber Command Control/ Battle Management (C2/BM)". The Aerospace Corporation.
10. Noman R Howes, Michael Messino, John Sarkesain. "On Cyber Warfare Command and Contrl". Institutes for Defence Analyses.
11. Thomas.C. Wingfield. "Integrating Legal and Policy Factors in Cyber Preparedness".
12. Jean-Loup Samaan."The RUSI Journal, Cyber Command". Royal United Services Institution.
13. Hans_LngeLango. "The Academic Debate on Cyber Security". Internasjonal Polikk 71(2).
14. M.C. Libicki. "Conquest in Cyberspace National Security and information Warfare". Cambridge University Press.

15. Tipping the Scales: the attribution Problem and the Feasibility of Deterrence Against Cyber Attack". Research Article.

16. Rechard Baskerville. "Agile Security for Information Warfare: A Call for Research". Research Gate Publisher.

17. Brig Navjot Singh ; Proposed Role and Organizational Structure of Cyber Command and Cyber Operations Units, published in July 2016 issue of SYNERGY, journal of CENJOWS; https://cenjows.gov.in/upload_images/pdf/Layout%20Inside_Synergy.pdf

18. Mathew S. Cohen, Charles D. Freilich and Gabi Siboni. "Israel and Cyber space : Unique Threat and Response". International Studies Perspectives(2015)0, 1-15.

19. James A. Lewis and Katrina Timlin. "Cyber security & Cyber warfare. Preliminary Assessment of National Doctrine & Oganisation Center for Strategic and International Studies.

20. William Slater and Matthew Crosston, "A Brief Arief Analysis of Russian Cyberwafare Capabilities – Past, Present and Future".

21. Gil Baram. "The Effect of Cyber war Technologies on Force Buildup : TheIsraeli Case". Military and Strategic Affairs/Volume 5/No. 1/May 2013.

22. Colonel Deepak Sharma. "China's Cyber Warfare Capability and India's Concerns". Journal of Defence Studies.

23. Charles Billo. "Cyber Warfare : An Analysis of the Mean and Motivations of Selected Nation States". Institute for Security Technology Studies at Dartmouth College.

References

1. Toward an Effective and Viable information Warfare Structure for the Indian Armed Forces* Lt General RS Panwar, AVSM, SM, VSM, PhD (Regt)

2. The Department of Defence Cyber Strategy, Office of US Secretary of Defence, Washington, Apr 2015, pp. 5.

3. Cyberspace Operations, US DoD Joint Publication 3-12 (R), 05 Feb 2013.

4. The Strategic Support Force: Update and Overview in China Brief, Volume 16 Issue 9 The Jamestown Foundation, Dec 2016.

5. Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, CNA's Occasional Paper, March 2017.

6. Keir Giles, Handbook of Russian IW, Fellowship Monograph No 9, NATO Defence College, Nov 2016, pp. 9, 36.

7. Keir Giles, Countering Russian IO in the Age of Social Media, Digital and Cyberspace Policy Program, Council on Foreign Relations, New York, Nov 2017.

8. Sydney Freedberg, Spectrum (EW) Should be a Domain of Warfare: Rep. Bacon, Breaking Defence, 29 Nov 2017, https://breakingdefense.com/2017/11/spectrum-ew-should-be-a-warfighting-domain-rep-bacon/

9. Brig Vinod Anand, Integrating the Indian Military: Retrospect and Prospect, Journal of Defence Studies Vol 2 No 2, Winter 2008, IDSA, pp. 36-37.

10. Lt Gen S A Hasnain, Image Challenge for The Indian Armed Forces, Vivekanand International Foundation Blog, Mar 2016, http://www.vifindia.org/article/2016/march/14/image-challenge-for-the-indian-armed-forces-take-it-by-the-horns.

JOINT C6ISR AND EXPLOITATION OF SPACE DOMAIN - A ROADMAP TO ADDRESS THE CAPABILITY GAPS

Lt Gen Anil Kapoor, AVSM, VSM (Retd)*

Abstract

The New Tech World Order is defined by Four Ds – Data, Digitization, Digitalization and Disruption. While these have fueled digital transformation globally giving rise to a large number of dual use technologies which are drivers of automation & autonomous applications, it is disruption which is not only transforming technologies at an unprecedented pace, but also transforming business concepts, models, processes and practices. While automated systems are rule based, the autonomous systems are designed and programed to take decisions and act. Supported by AI, IoT, Augmented Reality (AR), Virtual Reality (VR), big data analytics and block chain technology and driven by cloud and quantum computing, 5G, the ICT based system of systems have revolutionized military and dual use technologies. Convergence of Info-Communication Technologies and their combination has fueled Disruption in Military Affairs (DiMA).

DiMA has transformed automated decision support systems (DSS) to autonomous DSS and resulted in the design and development of Command, Control, Communication, Computers, Cyber and Combat Intelligence, Surveillance and Recce (C6ISR). C6ISR is a combination of technologies to generate an autonomous integrated Tri Services decision support system. Concurrent with C6ISR is the Space Domain which is the mainstay for geo-spatial enabled situational awareness, and uses satellites and other outer space technological applications to support

civilian, military and dual usage operations. Presently, India has around 15 military-application satellites, with the latest GSAT-7A dedicated to the Air Force and shared by the Army, with a revisit time of up to 96 hours. This is proposed to be reduced to six hours approximately by a number of satellite launches in the next five years. While high resolution imagery facilitates a number of military and disaster management applications, there are immense dual use applications.

Given the C6ISR and space domain technology driven pay offs, the counter measures for cons in terms of cyber, EW and anti-satellite (ASAT) threats are equally important. The paper analyses the technology landscape for creation of C6ISR and exploitation of the space domain and development of counter measures. This calls for a National and Tri Services Technology Strategy to achieve the paradigm of C6ISR as future technology landscape for future warfare.

Introduction

General. Over the past decade, technology has given the flesh to an age old product adage, 'whatever can be defined can be designed', albeit in a shorter time frame, in intent, context and content, given the unprecedented technological disruption. The manifestation of the technology outreach whether obtrusively or unobtrusively, by kinetic and non-kinetic means, has redefined on what constitutes an act of war. That said, the New Tech World Order is defined by Four Ds – Data, Digitization, Digitalization and Disruption. While these have fueled digital transformation globally giving rise to a large number of dual use technologies which are drivers of automation & autonomous applications, it is disruption which is not only transforming technologies at an unprecedented pace, but also transforming business concepts, models, processes and practices. While automated systems are rule based, the autonomous systems are designed and programed to take decisions and act. Supported by AI, IoT, Augmented Reality (AR), Virtual Reality (VR), big data analytics and block chain technology and driven by cloud and quantum computing, 5G, the ICT based system of systems have revolutionized military and dual use technologies.

The Revolution in Military Affairs, powered by digital transformation and niche disruptive technologies which impact the entire bandwidth of military activities be it info gathering, intelligence, recce, surveillance, training, logistics, decision support, control of resources both for defensive and offensive operations, has given rise to Disruption in Military Affairs. Further, the spectrum of conflict has enhanced from land, sea, air to cyber, space, psychological (Informational / mis-informational) and hybrid. In an overall analysis, the disruptive technologies, with or without man in the loop, is about enhancing velocity of OODA loop, as the driver of decisive proactive actions for enhanced situational awareness and combat effectiveness. The paradigm of future warfare is best defined as C6 ISR – Command, Control, Communication, Computers, Cyber, and Combat ISR in a close knit autonomous loop. This Disruption in Military Affairs has ushered an era with the concept that "Victory is measured by Digital Footprint", for all those of us who would still like to believe that victory is measured by foot.

In the recent past events, military actions have demonstrated that the VUCA of military or military-like interventions have been executed by embracing disruptive technologies. To recount a few major ones, the explosion damaging a centrifuge assembly plant last July and the recent large-scale blackout at Natanz, which the country's Atomic Energy Agency acknowledged had damaged the electricity grid or the killing of Iran's chief nuclear scientist, have portrayed the shape of things to come, in the spectrum of conflict.[1] In a similar vein, though by non-state actors, Yemen's Iran-backed Houthi rebels attack on Aramco refinery in the Saudi capital on 12 Apr 21 (and earlier on 14 Sep 19), using bombs and missiles laden drones, is an offensive act on the Kingdom's energy and security installations[2]. These drones reportedly flew more than 500 kms in an autonomous mode and hit their targets with precision. But

1 Chulov Martin, Israel appears to confirm it carried out cyberattack on Iran nuclear facility, The Guardian, April 11, 2021

2 Mohammed Hatem and Zaid Sabah. Houthi rebels attack Saudi Aramco sites for the second time in a week, World Oil, April/15,2021

an apt example of a decisive war through technology is the Armenian -Azerbaijan War. It is, in effect, the first war in the history of modern warfare that has been won almost entirely on the strength of drone warfare[3]. While Armenia only fought with tanks, artillery and air defence systems, Azerbaijan relied heavily on drones, specifically the Turkish-made Bayraktar TB2 and the Israeli-made Kamikaze drones.

Aim

The aim of this paper is to cull out the technology stack for adoption of joint Command, Control, Communication, Computers, Cyber, Combat ISR (C6ISR) and exploitation of space domain in Indian Armed Forces.

Scope

The road map for embracing C6ISR and space domain must be driven by a well-defined technology strategy with milestones over a decade of marathon. This calls for a programme akin to Integrated Guided Missile Development Programme, for curating a Tri Service integrated C6ISR plan. Accordingly, the paper is laid out in the following salient technology stack:-

(a) Military Small Satellite Geo Spatial Programme.
(b) Military ICT Transformation Programme.
(c) AI as a Service Programme.
(d) C6ISR Programme.
(e) Military Cyber Programme.
(f) Technologies roll out – the way forward.

C6ISR Technologies & Space Domain

C6ISR is a combination of exponential disruptive technologies of game changing small ideas with a big physical and psychological impact. These

3 Gupta Shekhar, How drones helped Azerbaijan defeat Armenia, and the implications for future modern warfare, The Print, Nov14, 2020

technologies have a dual civil-military application, a Tri Service flavor, align for a joint and integrated military applications and create a paradigm shift in the character of warfare, and design, means, and methods of war fighting, thereby creating an asymmetric advantage through application military power. In the recent past there is an ongoing arms race based on disruptive technologies for military applications, with USA, Russia and China in the lead. The 2018 US National Defence Strategy has echoed the view that the US national security will likely be affected by rapid technological advancements and the changing character of war, " *……..New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future……"*[4]. That said, there is a need for India to identify disruptive technologies, their military applications and a capability matrix based on a work time for acquisition/ research, design, development and induction plan. This could be based on a capability based mission priority programme akin to Indian Integrated Guided Missiles Development Programme. The intent should be to achieve technology sovereignty over the next decade.

Technology Lens I: Military Small Satellite Geo Spatial Programme (MSSP)

Satellites offer huge ISR advantages, which is the centre of gravity of military planning and execution. Military satellites as a part of communication and other application based satellite systems and leasing satellites has been a need based part of military perspective planning. No wonder then, there are satellite for Indian Air Force, Navy, Army and various info systems of systems including AWACs and strategic recce missions and programmes. Presently, India has around 15 military-application satellites, with the latest GSAT-7A dedicated to the Air Force and shared by the Army. By end 2022[5], the $225 million

4 US Congressional Research Service, Emerging Military Technologies: Background and Issues for Congress, Updated November 10, 2020, https://crsreports.congress.gov

5 Neelam Mathews , "India Ramps up Military Satellite Plans", Defence Notes, Shephard

GSAT-7R, an Indian Navy communications satellite, will replace GSAT-7 Rukmini launched eight years ago. It is the last of the Indian Space Research Organisation's seven fourth-generation satellites with a 2,000nmi coverage range over the Indian sub-continent. As the need for maritime domain awareness grows, and as border tensions with China and Pakistan increase, vulnerabilities in Indian space security have made it mandatory to look to build up its minuscule number of military satellites.

With the proliferation in miniaturized small satellites and ease of their launch, an eye in the sky as a low earth orbit satellite is a huge disruptive technology. Given the need to defend vast borders delineated by volatile international border, line of control and line of actual control and the coast line, deep and shallow look capabilities through a technology solution is a dire necessity. A large number of surveillance devices are deployed, but given the porosity and the sheer length of the borders and areas of interest and influences, for round the clock surveillance, Indian Military must develop capability to launch Nano - tech enabled Low Earth Orbit Satellites and have a GIS platform duly integrated as a MSSP. One rationale for miniaturizing satellites is to reduce the cost and being lighter, require smaller and cheaper launch vehicles, which can sometimes be launched in multiples. They can also be launched 'piggyback', using excess capacity on larger launch vehicles. Miniaturized satellites allow for cheaper designs and ease of mass production. A number of academic institutions, startups and private sector are currently developing small satellites and launch mechanisms (vehicles) to perform the increasingly targeted launch requirements of microsatellites. Accordingly, MSSP could be launched, as an adjunct to National Disaster Management Programme, to monitor avalanches and other natural calamities to facilitate disaster relief as a, but primarily keep continuous watch in the areas of interest and influence for military targets of interest. The Programme is recommended as a Joint ISRO – DRDO - Armed Forces Programme, as Public Private Partnership

Press Limited, 31 May 2021

Project by integrating startups and private industries in the field of satellite technology. Given the provisions of DAP 2020, in the short term, key private players may be approached for leasing Space Infrastructure as a Service to empower space based applications and as a long term a dedicated Programme be collaboratively generated[6] . The platform ground station would be geo spatial enabled for accurate position fixes. This Programme could be the vanguard to unleash the Tri Service Space Command.

Pay Offs Envisaged. The following pay offs are envisaged for 24/7 situation awareness:

(a) Red Force Tracking and intelligence collection in real time including tracking key military targets of interest.

(b) Blue Force Tracking in real time thereby facilitating C2.

(c) Seamless all weather EM and satellite communication.

(d) Platform for electronic warfare – electronics surveillance, electronics counter /counter-counter measures.

(e) Weather and met data for artillery and long range vectors though autonomous software systems.

(f) Effective disaster management through proactive forecasting and follow up actions.

Technology Lens II: Military ICT Transformation Programme

Digital transformation can be best accomplished as a Tri Service Programme. The three Services have varied standards, capabilities and capacities of automation. There is a dire need to create a Tri Services ICT Digital Platform with mega data centres duly networked by Network for Spectrum (NFS) currently under execution. The power of digital transformation can be best harnessed by joint Armed Forces Integrated Information System comprising management information

6 Website dhruvaspace.com

systems, operational logistics information systems and operational / combat information systems. There are stand alone information systems that each Service has configured and some of these need to be and can be integrated through well thought through automated programme interfaces (APIs). A case in point is the IAF, Integrated Air Command and Control System (IACCS), which can be combined into a Tri Service Air Defence Combat System which can be integrated with other operational combat management information systems. Given the cyber threats, and ICT convergence a holistic approach to address major voids need a long term action plan are as follows:-

(a) Major information technology voids exist in terms of the Armed Forces Operating System (AFOS). There is a need to revamp a Linux based OS like BOSS which can be scaled up as an exclusive AFOS.

(b) A Tri Service GIS needs to be created for effective geo referencing through digital maps.

(c) A Tri Service Data Base is yet another building block. Blockchain technology based systems for enterprise resources planning need to be designed and developed.

(d) A Tri Service software defined radios (SDR) – hand-held, man pack and vehicle/ship/aircraft based.

(e) **Quantum Computing Technologies.** Quantum computing systems are the mainstay of design and development of future SDRs, software defined radars and ICT systems for military and space applications. As an extension, chip and nano technologies need to be developed to produce miniaturized man pack and mobile platforms for effective military exploitation of state of the art technologies.

(f) **Laser Based Communication System (LBCS).** The VUCA of electronics warfare environment calls for design and development of LBCS. This could be used for creating

redundancies in critical communication links voice, data and video. The laser wave is coherent, line of sight and agnostic of any interference.

(g) HAM Radios as a formal means of communication with encryption could also be developed in select areas of operations for effective communication. There is a need to develop theatre based HAM clubs for augmenting all weather communication.

Technology Lens III: Artificial Intelligence (AI) as a Service Programme

AI is best exploited as a multi-faceted platform offering algorithms and deep learning systems for voice, text and video data[7] as a service, AIaaS. A systemic platform would typically choose algorithms and deep learning combinations to analyse data, structured, unstructured, for pre-defined or online queries and actionable outputs. There is a dire need to develop AI as a Tri Service platform which can run applications to include the following:

(a) **Imagery Interpretation.** The manual process for a satellite image with a raster of 64 sq km takes approximately six hours of laborious slog. AI based platforms can list out the military targets of interest in less than 10 minutes. This can be enhanced to identification and image processing on the fly for manned aircraft or unmanned aerial platforms on the fly.

(b) **ISR.** AI can be effectively used for intelligence collation, analysis and synthesis from all sources electronics, optical, thermal and human to create an actionable intelligence picture both augmented reality (AR) and virtual reality (VR). This capability can help in identifying military targets of interest and build operational scenarios. As an example, seek and strike missions based on target-shooter mapping and post-strike damage assessments.

7 Kai-Fu Lee, AI Super-Powers China, Silicon Valley and The New World Order, PP 140-141

(c) **War Gaming.** AI platforms can be best configured for Tri Service scenario building and net assessment exercises and create contingencies from tactical to strategic levels through AR and VR.

(d) **Swarms of Unmanned Systems.** AI platforms are being used to configure ground based unmanned systems (robots), aerial unmanned systems and both sea based and under-water / submersible unmanned systems and hybrid systems like, ground and aerial swarms. These technologies are game changers in future warfare and a paradigm shift from automation (business intelligence) to autonomous systems.

(e) **Asset Management and Operational Logistics.** Operational logistics and supply chain in the Tri Services are based on manual and just in case methods which are location based and cost prohibitive, The time dimension of inventory, assets and supply chain management could be electronically driven for huge optimization and cost effective solutions using e asset systems, Block chain and AI. Blockchain technology is best suited system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A Blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Convergence of Blockchain and AI can enhance machine learning and enable AI to create and trade financial products. While Blockchain enables secure storage and sharing of data or anything of value. AI can analyze and generate insights from data to generate cost effective value[8].

Technology Lens IV: C6 ISR Programme

Future warfare is autonomous technology based action interspersed with

8 Raj Shroff, When Blockchain Meets Artificial Intelligence, Start it Up, Feb 14, 2020

military troops intervention, based on criticality of the mission. With man in the loop and man out of the loop missions, in effect, C6 ISR based autonomous weapons systems are lethal devices that have been empowered by their human creators to survey their surroundings, identify and track potential enemy targets, and independently choose to attack those targets on the basis of sophisticated algorithms. These systems typically comprise a *seek and respond* system. *Seek* is an autonomous pivot which could be land, ship or aerial platform with computer based systems, application software configured as C6ISR based decision support tightly integrated with the *respond* strike autonomous system mobile maneuver arm comprising combat platforms both kinetic and non-kinetic in automated system with man in the loop or autonomous systems with man out of the loop. Such systems require the integration of several core elements: a mobile combat platform, such as a drone aircraft, ship, or ground vehicle; sensors of various types to scrutinize the platform's surroundings; processing systems to classify objects discovered by the sensors; and algorithms directing the platform to initiate attack when an allowable target is detected. The U.S. Department of Defence describes an autonomous weapons system as a "weapons system that, once activated, can select and engage targets without further intervention by a human operator."[9]

C6ISR, is, therefore, a programme which will encapsule a number of disruptive technologies. Many semi-autonomous weapons in use today rely on autonomy for certain parts of their system but have a communication link to a human that will approve or make decisions. In contrast, a fully Autonomous Weapon System (AWS) could be deployed with an established communication network and would independently respond to a changing environment and decide how to achieve its pre-programmed goals. AWS may create a paradigm shift in how we wage war. This revolution will be one of software; with advances in technologies such as facial recognition and computer vision, autonomous navigation in congested environments, cooperative autonomy or swarming,

9 US Department of Defence, "Autonomy in Weapons Systems," Directive No 3000.09, November 21, 2012

these systems can be used in a variety of assets from tanks, ships, submarines to small commercial drones. They would allow highly lethal systems to be deployed in the battlefield that cannot be controlled or recalled once launched. Unlike any weapon seen before, they could also allow for the selective targeting of a particular group based on pre-defined target parameters. In effect, AWS will facilitate a deep strike with precision, thereby reducing collateral damage. Viewing AWS from a technology lens, it comprises almost all niche disruptive technologies, sensor technologies and IOT, unmanned autonomous aerial and ground based platforms, cyber, electronics warfare, directed energy weapons, quantum technologies, big data analytics, nanotechnologies, geo- spatial technologies an AI . The ongoing conflict between Israel and Hamas is an apt example in the use of C6ISR and precision in targeting.

Technology Lens V: Military Cyber Programme

Digital eco system is essentially creating a virtual platform of info systems with many points of vulnerability increasing the attack surface, thereby giving rise to growing cybersecurity concerns. In fact, cyber has been major disruptor – a cyber warrior may be a bermuda clad professional who can execute cyber maneuvers at anytime from anywhere. According to the annual IBM X-Force Threat Intelligence Index, India reported the second highest number of cyber-attacks after Japan in the Asia-Pacific region in 2020, accounting for 7 percent of all cyber-attacks observed in Asia in 2020. Likewise, organizations have also incurred heavy financial losses due to disruptions and data breaches. A 2019 report by IBM revealed that cyberattacks cost India ₹12.8 crores on an average between July 2018 and April 2019. During the same period, the average cost globally of a data breach was ₹ 27 crore. Besides these financial losses, cyberattacks can and have caused huge dents in an organization's overall brand value. With digital adoption breaking grounds especially in the Armed Forces, the corresponding cyber maturity must keep pace with the technological strides – greater exposure to cyber risks calls for a greater focus on cybersecurity.

That said, cyber threat is a 24/7 phenomenon globally. The report titled, 'Shadows in the Cloud', in 2010, documented a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the United Nations and several other countries. The investigation recovered a large quantity of stolen documents which included sensitive and classified info belonging to the government, business, academic, and other computer network systems and other politically sensitive targets. The report analyzed the malware ecosystem employed by the Shadows' attackers. The system leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report provides evidence that the attackers operated or staged their operations from Chengdu, PRC[10]. Given the invisible nature of a cyber threat, its huge proliferation and the capability to disrupt C2 and compromise operationally sensitive info (data), Tri Services Cyber Command has been planned. The following technology landscape is imperative to energize the cyber command:-

(a) There is an increasing need for businesses to adopt a proactive cybersecurity strategy that encompasses everything and helps organizations protect sensitive operational data, personally identifiable information and military information systems, from theft and damage attempted by cyber-criminals.

(b) All Organizations must observe a rigorous enforcement of security policies. This means ensuring and implementing adequate training and awareness on data protection, implementing appropriate security software and keeping it updated, ensuring data encryption, and backing up data regularly.

(c) Adopting a zero-trust security architecture can also help manage cybersecurity incidents. Zero Trust is a security concept

10 https://itlaw.wikia.org/wiki/Shadows_in_the_Cloud:_Investigating_Cyber_Espionage_2.0.

that requires access control for all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validate security configuration and posture, before being granted or keeping access to applications and data.

(d) **Cyber Defence in Depth.** There is a need to protect the data centres and IT assets using encryption for data in rest, software security protocols and cyber security hardware, firewalls and IT asset security systems on the edge, This multi-layer approach would entail new security protocols that every digital soldier should embrace, even if slightly inconvenient.

(e) A Security Operations Centre (SOC) and Network Operations Centre are specialized central teams focusing on protecting the digital assets of organizations. The team comprises cyber-security experts who continuously monitor and analyse the Information & Communication Technologies (ICT) infrastructure as well as the threat landscape. A combination of practices and tools can help assessment, prevention, detection and response to incidents on websites, application/database servers, and networks among other systems. Military organizations must set up SOC - NOC to manage the security of their digital infrastructure and systems. This will enable significant improvement in security preparedness by timely detection of and response to security incidents, by driving preventive and predictive actions.

(f) **Offensive Cyber.** Attack is the best form of defence. Offensive cyber is the key to achieving informational cyber ascendancy over an adversary. There is a need to harness the potential of young IT enabled graduates to create a ready pool of cyber offensive invisible warriors with an aggressive cyber intent. With the next generation of cyberattacks being carried out with greater scale and sophistication, organizations, now more than ever, have a greater responsibility to protect people who have access to essential data.

Technology Roll Out – The Way Forward

There is a huge opportunity in futuristic niche disruptive technologies. Aatmanirbharta, Make in India (MII), Start Up India, industrial corridors and defence industrial bases are Government initiatives to drive consciousness for self-reliance. It is like putting a finger on the jugular vein of technology development for diagnosis, but the answer lies in prognosis and prescription.

Knowing what to do and getting things done are twos sides of the management coin and India has the will and ability for both. The best model to self-reliance is creation of our own unique model which gives homegrown indigenous solutions. The Moot Question is - Do we have a technology strategy to make Aatmanirbharta and MII happen? This requires a well-articulated National Technology Strategy (NTS). Some thoughts on plausible key determinants of the NTS are analysed in succeeding paras.

Tri Service Technology Strategy. A number of initiatives have been taken under the National Technology Development Board to create technology verticals and Centres of Excellence (CoE) in identified technologies. Each Ministry has a few CsoE. These efforts need to be vectored and drawn into a cogent technology strategy with a clear technology forecast, technology development work time action plan with clearly articulated deliverable milestones and end state of each vertical. As a part of this National Technology Strategy, a Tri Service Technology Strategy with a tech forecasting and development implementation plan for C6 ISR must be prepared.

Consortium Approach. A number of R&D Orgs within the Govt, private sector and academia exist, employing subject matter experts (SMEs) and deploying huge amounts of funds on R &D. These resources can be optimized through a two pronged strategy.

(a) Build synergies between academia, public sector, private industry, startups, R and D Orgs and Government Institutions like CoE, STPI etc dealing with technology development where

technologies are incubated and churned out as prototype use cases.

(b) Create a legislation and control regime to synergize the efforts of these R and D synergies with the concept of One technology One team (OTOT). R and D efforts must become a meaningful engagement through agencies complementing and not competing with each other. As an example, all agencies dealing with space applications need to register with an appropriate vertical under the Technology Development Board for creating synergies and jointness among SMEs. Based on the areas of research and development, consortiums of SMEs will reduce the chances of reinvention of the same wheel and facilitate faster development and quick impact utilization of each wheel optimally. In any case this is the need of the disruptive times – think big, start small, fail fast, recover faster – be first, be agile.

Corporate Professional Responsibility (CPR) Funding R &D. R&D and technology development is a painstaking exercise of design and redesign - an exercise requiring huge funds to go through iterations of trials and errors bereft with failure cycles in an arduous journey to fruition. There is, therefore, a requirement of large funds to develop and sustain niche disruptive technologies. Govt would do well, in the interest of the Aatmanirbharta, to institutionalize a fund titled CPR Technology Development Fund under Companies Act 2013 for technology development as a National initiative. This fund, in effect, would be akin to Corporate Social Responsibility Fund- two percent which Companies deploy based on turn overs and profit margins. The Technology Incubation Centres, Technology hubs, start ups need to be funded by industrial houses and Government in joint ownership and guided by identified sub matter experts.

Conclusion

The New World Order respects Nations with the strength to manage VUCAD (Volatility, Uncertainty, Complexity, Ambiguity and Disruption).

Bewildered and worried by the struggle, a child opens the cocoon to let the butterfly fly off. Alas, the butterfly failed to fly and died since the wings did not develop the intrinsic strength afforded by the Nature in the struggle moments of decocooning. With a good intent but inadequate knowledge of hows and whys of the child, a potential creation was dead. Aatmanirbharta and MII is a great strategic intent. In the backdrop of a strong tech base provided by ISRO, DRDO, Technology and Innovation Centres of industries & PSUs, Startups and T Hubs, the time is ripe to strengthen the cocoon through a well thought through technology strategy and fly out the indigenous technology butterfly globally.

Towards this end, the industrial corridors pan India and two defence industrial corridors need to be developed with the thought of Made in India. The C6ISR is a tech sojourn for future jointness in warfare and must become an illustrious lasting tech journey. Let us do it!

***Lt Gen Anil Kapoor,** AVSM, VSM, is a former Director General Electronics and Mechanical Engineering (EME), Indian Army

Bibliography

1. Chulov Martin, Israel appears to confirm it carried out cyberattack on Iran nuclear facility, The Guardian, April 11, 2021
2. Mohammed Hatem and Zaid Sabah. **H**outhi rebels attack Saudi Aramco sites for the second time in a week, World Oil, April/15, 2021
3. Gupta Shekhar, How drones helped Azerbaijan defeat Armenia, and the implications for future modern warfare, The Print
4. Raj Shroff, When Blockchain Meets Artificial Intelligence, Start it Up, Feb 14, 2020
5. US Congressional Research Service, Emerging Military Technologies: Background and Issues for Congress, Updated November 10, 2020, https://crsreports.congress.gov
6. Neelam Mathews , "India Ramps up Military Satellite Plans", Defence Notes, Shephard Press Limited
7. Kai-Fu Lee, AI Super-Powers China, Silicon Valley and The New World Order
8. US Department of Defence, "Autonomy in Weapons Systems," Directive No 3000.09, November 21, 2012
9. The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower Paperback ,31 May 2019
10. https://itlaw.wikia.org/wiki/Shadows_in_the_Cloud:_Investigating_Cyber_Espionage_2.0
11. Website dhruvaspace.com

SPECIAL OPERATIONS - A CAPABILITY ROADMAP FOR INDIA

Maj Gen AK Dhingra, SM (Retd)*

"Special Forces represent the best of human resources of any armed forces and operate in all domains of conflict with daring and self-sacrifice. They provide the effortless link between the unconventional and irregular forces. Application of Special Forces provides a nation exponential strategic gains, along with deniability."

- Lt Gen HS Lidder, PVSM, UYSM, YSM, VSM (Retd)

Abstract

India's rise as a major economic power with increased strategic stakes in its immediate and extended neighbourhood can best be safeguarded by enhancing role of Special Forces to meet our national security interests. Leading nations of the world have employed Special Forces as a highly flexible and low-cost tool of statecraft to achieve political outcomes without resorting to use of conventional forces. The highly successful surgical strikes executed in 2017 brought to fore the potential of Special Forces to deliver at the politico-military strategic level. With the establishment of the Special Operations Division, the willing support of the political leadership to exploit the attributes of unconventional forces is inevitable. By virtue of being a joint force, it needs to be empowered with dedicated intelligence, strategic mobility and advance weaponry to fulfil its mandate to face crisis situations and execute its strategic role in future. In keeping with the security threats posed by our two inimical nuclear

armed neighbours and regional constraints, the restructured Special Forces can achieve enhanced operational efficiency in conventional and hybrid warfare scenarios to meet the emerging challenges.

Introduction

India faces unique security challenges across the entire spectrum of warfighting, ranging from the collective conventional threats posed by hostile nuclear armed China and Pakistan due to unresolved borders, and the continuing internal security threats of proxy war and insurgency in many parts of the country. With multiple threats as above and the nature of conflict itself undergoing major changes by acquiring more dimensions every few years, India's Armed Forces experience the litmus test of their proficiency and professionalism regularly.

Special operations by Special Forces can be characterized as those in support of regular conventional forces at one end, to politico-military sensitive missions executed in hostile environments at the other end of the operational continuum. Leading powers of the world have employed Special Forces as a flexible low-cost tool to achieve desired outcomes without resorting to expensive escalatory armed conflicts. Special operations are aimed to achieve psychological dislocation of adversary's critical assets and being sensitive in peace time, need political oversight at the highest level. They are 'high risk, high gain' missions focused to deliver disproportionate results.

The operational scope of warfare is being transformed by rapid technological progression in computing, cyber, communications, artificial intelligence and aerospace. Further, as we rise to become a major economic power with enhanced strategic and security objectives, our military capabilities will also need to grow proportionately to address the concerns in our areas of interest and influence in the Indo-Pacific and Indian Ocean Region (IOR). Whatever the future holds, our nation will always require elite forces who can stare danger in the face and overcome the myriad of challenges, to conduct the vast range of special operations and ensure a high degree of national security pro-actively.

Special Operations in the Indian Context

Special Forces of any nation are its elite and are selected, trained and equipped for undertaking tasks across the entire spectrum of conflict on high-risk missions. They are highly skilled to focus on unconventional special operations in politico-military sensitive environments. As their employment is characterized by surprise, low visibility and clandestine nature, they are tools of state-craft ideally utilized below the conventional threshold to meet hybrid and asymmetric challenges.

India's Special Forces trace their origin to Meghdoot Force, an ad hoc Commando unit that was organized with volunteers from various infantry units by Major Megh Singh. This unit conducted successful raids behind the enemy lines in the Indo-Pak War of 1965, and was formally raised as 9 Para Commando in July 1966 with focus of operations in mountainous terrain. In June 1967, the unit was split to form 10 Para Commando and mandated to specialize in desert terrain. Both the units excelled in Indo-Pak War of 1971 with their daring raids at Mandhol (Poonch) and Chachro (Sind).

In 1978, 1 Para, an over 200 years old unit, was converted as an Experimental Commando Wing to become the first Special Forces unit of the Indian Army. These three units were employed extensively in all major operations to include Op Pawan (1987-89), Op Vijay (1999), and regular counter insurgency operations in Jammu & Kashmir and the North Eastern states since the eighties. 1996 saw the formation of the fourth Special Forces unit, 21 PARA (SF) and with the changing operational environment necessitating the felt need for more Special Forces units, 2 PARA, 3 PARA and 4 PARA were converted from their erstwhile airborne role in the early years of 21st century.

Special Forces have conducted successful counter-insurgency operations in Jammu & Kashmir and North Eastern States with renewed vigour and proficiency for more than two decades. Their role, tasking and expectations have increased substantially as a counter-terrorism force, executing clinical pro-active raids and hostage rescue missions. The effective special mission destroying militant camps along the Indo-

Myanmar border in 2015 and the pre-emptive surgical strikes across Line of Control (LoC) in Pakistan occupied Kashmir in 2016, have proven the distinct ethos and motivation of these gallant teams. The brief history of our Special Forces is a saga of courage and valour, led by young professionals with risk-taking abilities and ingenuity in critical missions.

The Indian Army Doctrine defines Special Forces as “Specially selected troops who are trained, equipped and organized to operate in hostile territory, isolated from main combat forces. They may operate independently or in conjunction with other forces at the operational level. They are versatile, have a deep reach, and can make precision strikes at targets of critical importance”. However, the past few years has brought out a realistic assessment that our Special Forces have been utilized sub-optimally on tactical missions routinely, rather than strategic and unconventional missions for high-value targets.

Today, we have a plethora of elite forces within the three Services, National Security Guard, Special Frontier Force and para-military forces with no central authority, leading to duplication of efforts and making them incapable as an effective politico-military tool. These units have valuable combat experience at the tactical level, but their continuous employment has been detrimental to act as a ‘force multiplier’. To optimize the special operations capability in the policy realm, the integration of all Special Forces under a Special Forces Command is inevitable. Lt Gen PC Katoch, a war veteran of the Special Forces has stated that “In sharp contrast, in India, we have been simply looking at battlefield victory. Special Forces units are deployed more on tactical missions rather than the broader, strategic and unconventional missions that should be their charter’’.

The potential of Special Forces to serve as an instrument of national policy has not manifested itself mainly due to lack of appropriate command & control structures, rapid proliferation of units, absence of special aviation unit, inadequate high technology equipment and state of the art training facilities. The Special Forces truth that ‘Quality supersedes Quantity’ appears to have been overlooked by planners,

leading to their diluted employment. The raising of a Special Operations Division (SOD) signifies the tremendous support of political hierarchy to undertake major reforms in tasking and employment of Special Forces. Like the 'Lone Sniper', Special Forces can bridge the gap as a political-strategic military tool, provided they are afforded opportunities to execute the mandate to address asymmetric warfare challenges.

Special Operations and Asymmetric Warfare

The US Doctrine for Joint Special Operations defines Special Operations as "Operations conducted by specially organized, trained and equipped military forces to achieve military, political, economic or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. These operations are conducted during peacetime competition, conflict, and war, independent or in coordination with operations of conventional, non-special operations forces".

Special Forces play an important role in furthering own national interests and nations have employed them extensively at strategic and operational levels. A foolproof degree of planning, accurate intelligence and detailed preparation is mandatory to ensure desired outcomes. Special Forces employ both direct and indirect approaches to execute allotted missions, maintaining a fine balance between security of plans and extensive coordination with various agencies. A high level of individual, terrain related combat expertise with proficiency in cultural and language skills is inescapable for mission success.

In the recent times, the US Global War on Terror with their Special Forces in the lead in Iraq, Afghanistan, Libya and Syria have defined the conceptual approach of employment coupled with extensive intervention and power projection techniques. Their unconventional warfare efforts even during the Cold War included psychological and civic action operations throughout the varied interventions. Russia's irregular warfare targets an adversary's weaknesses and avoids direct confrontation with ambiguity and deception as the main strategy that was also implemented in Crimea and Ukraine recently.

Closer home, the Chinese concept of 'Unrestricted Warfare' is well known and its Special Forces are even embedded in Belt and Road Initiative (BRI) economic ventures. And Pakistan's Special Services Group (SSG) has demonstrated its adeptness in sub-conventional wars in close coordination with Inter Service Intelligence (ISI), ranging from covert operations supporting Taliban inside Afghanistan to fueling terrorism in India, and its integral participation with Border Action Teams (BAT) on the Line of Control (LoC). The concept of 'Dirty Wars' has blurred the distinction between professional warriors and non-state actors with lack of ethical standards submerged in multiple layers of hybrid warfare.

The Indian experiment in utilizing asymmetric warfare began with the initial raising of Special Frontier Force (SFF) by recruiting Tibetans for 'behind the enemy lines' activities after the 1962 war, but the aim could not be sustained due to a variety of reasons. The birth of Commando battalions after the stupendous success of operations by Meghdoot Force in the 1965 Indo-Pak War has already been amplified. The Indian Peace Keeping Force (IPKF) intervention in Sri Lanka during the years 1987-89 led to intense fighting with the Liberation Tigers of Tamil Eelam (LTTE), when trying to demobilize them.

The capacity to wage and combat sub-conventional wars has become an accepted currency of geo-political power, as an adjunct to a nation's foreign policy. Our experiences in utilizing the Special Forces in the sub-conventional domain clearly brings out that we have miles to go before organizing and optimizing their full potential. The rapid expansion of the Special Forces without centralized control, interface with political decision-making and fusion with strategic intelligence is akin to exercising strategic restraint, which is detrimental to our national interests in hybrid war.

Also, the firm response to proxy war by cross-border raids on insurgent camps and launch pads few years ago has been reactive, more as an after-thought than achieving long term strategic dividends. There is little cohesion with intelligence agencies at the apex level, and it

is a proven fact that challenges posed by unconventional threats cannot be met by pure application of conventional forces or diplomacy, further increasing our vulnerabilities.

We need to develop a vision beyond shallow cross-border raids as a credible deterrence by employing Special Forces to meet our strategic interests. Special Forces, in coordination with Cyber, Space and Artificial Intelligence capabilities can provide us a reliable response mechanism to deal with emerging challenges comprehensively. They have the ability to maintain viable surveillance in areas of strategic importance, counter asymmetric wars, control our adversaries' fault-lines and deter them from exploiting irregular warfare, and provide the cutting edge to our decision-makers for strategic force projection as 'Warrior Diplomats'.

Special Operations in Conventional Role

The employment of Special Forces in war is focused on 'shaping the battlefield' with reconnaissance, disruption and dislocation missions to increase friction for the enemy by disproportionate damage to critical assets. The aim to achieve relative superiority through surprise and shock action is the raison d'etre for Special Forces to execute significant missions in support of conventional operations, by addressing enemy's centre of gravity. However, with conventional wars receding as an option, limited short duration engagements below nuclear threshold with punitive strikes are emerging as likely conflict scenarios.

Against China, the Doklam standoff in 2017 and the Galwan bloody skirmish that spiraled out of control last year have presented the same escalatory risks as India-Pakistan LoC, leading to uneasy co-existence and the relationship becoming overtly conflictual in a matter of weeks. Add to this its all-weather support to Pakistan, the friction in maritime domain in the IOR and our hosting the Tibetan government in exile, the current military state of play along the Line of Actual Control (LAC) is complete. In the near to medium term, conflict with China will be limited in scope and duration due to a variety of factors. The differences between our territorial posture, climate, terrain, infrastructure differential

and the overall command structure brings out the contrasting approach to warfighting paradigm by the two nations.

China's War Zone Strategy is based on pre-emptive military action with jointness, trans-theatre mobilization, rapid concentration with air, cyber and electronic measures as the backbone of warfighting. We have also augmented our force structure with Mountain Strike Corps and focused on improving the border infrastructure to face a short duration, limited border conflict as the more likely contingency. The nuclear overhang will restrict the scope of scale of conflict and a third-party intervention will be inevitable. Our operational philosophy is to be agile, respond rapidly to developing situations, adopt offensive defence and incorporate area denial measures. The manpower focused approach of a large conventional positional force has to give way to the essential tenet of manoeuvre warfare, by utilizing complementary forces on different axes, trading space for time in the difficult mountainous terrain.

In the above contingency, the Special Forces can be employed for above roles aggressively to act as enablers and launch special warfare in Tibet Autonomous Region (TAR). We can implement a nimble pro-active strategy by integrating forward deployed Special Forces teams for Intelligence, Surveillance and Reconnaissance (ISR) and extensive network of Scouts to focus behind the enemy lines to delay, disrupt and interfere with their build-up. However, the Special Forces face challenges to implement strategy of pro-active defence due to lack of centralized control and terrain specialization with operational hurdles. Lack of organic air platforms makes them dysfunctional and their intelligence along with training and procurement needs immediate restructuring.

The political decision makers require to be risk tolerant, as surgical strikes were shallow thrusts but China calls for deeper and extended missions by capable Special Forces. We need to exploit Tibet as a 'trump card' during significant escalation. The uniqueness of Special Forces as shock troops demands to be exploited, as our military structures are tailored for linear attrition warfare compared to manoeuvre

as the hallmark of unconventional warfare campaign. Our operational concepts and approach towards territorial defence with overt reliance on conventional forces calls for re-assessment, as the rugged terrain with lack of infrastructure on the LAC favours more reliance on the Special Forces. In other words, we need to become more of Pakistan and China in our mode of thinking to employ Special Forces as conventional deterrent on LAC.

Way Ahead

India's volatile neighbourhood hemmed with China-Pakistan nexus poses serious hybrid threats to our national security. The US withdrawal from Afghanistan, strategic implications of China Pakistan Economic Corridor (CPEC), tensions rising in the IOR and Indo-Pacific needs continuous assessment and a flexible response with credible deterrence. While the National Security Strategy (NSS) will foster integrated approach to war fighting, promote national interests and counter weaknesses in long-term procurement and budgetary allocations, a detailed policy to counter sub-conventional threats with timely implementation, monitoring and periodic updating based on changing threat scenarios is inescapable.

As highlighted, both China and Pakistan possess advanced sub-conventional capabilities and are utilizing their Special Forces to great effect to achieve their security objectives. The decision makers need intellectual understanding of strategic value of covert special operations. As an erudite India-Pakistan expert Stephen Cohen said, "The task of Special Forces is proxy application of force at low and precisely calculated levels, the objective being to achieve some political effect, not a battlefield victory."

Special Forces should be central to our asymmetric responses to achieve strategic objectives in hybrid and unconventional missions. The military hierarchy does not see the Special Forces as a substitute for conventional operations and is unable to utilize it as an effective political-military tool because of its focus on internal security. Just as the Goldwater-Nichols Act of 1986 brought about reorganization and

integration of US Armed Forces in a firm time bound manner, we also need to overhaul our archaic security structures. The elephantine pace of reforms and capability build up for executing special operations to counter the current challenges will leave us severely vulnerable in the intervening years.

The early application of SOD can help us to overcome our inability to operate in ambiguous environments to derive maximum political, diplomatic and military outcomes. SOD gives us options to overcome the adverse symmetry by conducting special missions of strategic interest to the country. This force needs to be reinforced with national intelligence agencies, dedicated aerial platforms and advance training facilities with hi-tech special operatives' gear but most importantly, a rightful place in the national hierarchical decision-making structures to oversee its optimal employment.

Looking ahead, a functional Special Operations Command needs to be organized under the National Security Advisor (NSA) to be utilized pro-actively as an effective force multiplier for strategic outcomes. We need to have advisors for special operations in Ministry of Defence, External Affairs and Home as only such positions manned by specialists can optimize our potential. Multiple benefits can be accrued for the nation with the operational philosophy putting greater emphasis on rapidly seizing initiative at the high end of asymmetric warfare. Only a resolute political will and a plan to optimize Special Forces prospects by creating a Special Operations Command to meet multiple challenges of hybrid wars and cross-border terrorism, will create internal stability and meet our long-term strategic interests.

Conclusion

The potential of India's Special Forces to serve as an instrument of national power has not manifested itself appropriately due to a variety of

reasons, and their utilization has been restricted to tactical missions in the last few decades. While the Special Forces have proved their mettle in the challenging combat environments over the last few decades by virtue of their ethos and commitment, they now need to 'reset' their operational philosophy to counter the current challenges. As India grows its national security interests and assets beyond the regional framework to attain its foreign policy objectives in spite of our adversarial neighbours, it will need synergized Special Forces to protect and project our strategic capacities.

Raising of a Tri-service agency has aligned the need for a robust joint force to address multiple security challenges in India's sphere of influence and meet our strategic aspirations. We now need a functional Special Operations Command to exercise centralized command and control over all Special Forces with dedicated intelligence, versatile training, terrain specialization and effective equipment for their optimal exploitation to meet our security, foreign policy and economic interests. The foreseeable uncertain geo-strategic environment therefore, implores India to optimize its Special Forces potential and reinforce it with appropriate foundations of doctrine, policy, structure, organization and employment to meet its national security challenges assertively in future.

***Maj Gen AK Dhingra,** SM (Retd) is former DG AFSOD

TRANSFORMATION TO HARNESS DISRUPTIVE TECHNOLOGIES

Lt Gen Sanjay Verma, PVSM, AVSM, VSM** (Retd)*

Abstract

*A **modern day 'Blitzkrieg'** without any overwhelming force concentration and not an iota of involvement of conventional forces is a reality today with definite outcome in the form of demonstration of the intent to break through the opponent's lines of defence, dislocate the defender and unbalance the enemy.*

The capability to carry out precision attacks at a fraction of cost compared to a conventional strike penetrating and exposing the vulnerabilities in impregnable defence systems is just the tip of iceberg of potential capabilities and threats enabled by technology and an imaginative mind alone.

Emerging disruptive technologies such as artificial intelligence, big data, quantum technology, advanced robotics, autonomous systems, new advanced materials, blockchain, energy storage, hypersonic weapons systems and biotechnologies applied to human enhancements amongst many others are expected to have a disruptive impact on defence and revolutionise future military capabilities, strategy and operations. The manifestation in the form of the drone attack in Saudi Arabia was just one of exploitation of capabilities available. And these are clear indicators that this is an inflection point where transformation to meet the new challenges is inevitable however the level and scope of this transformation needs to be defined.

Introduction

The event of 14 September 2019 wherein drones were used to attack the state-owned Saudi Aramco oil processing facilities at Abqaiq and Khurais in eastern Saudi Arabia causing large fires at the processing facility thereby cutting Saudi Arabia's oil production by about half – representing about 5% of global oil production – and causing some destabilization of global financial markets can easily be termed as the ***modern day 'Blitzkrieg'***. Without any overwhelming force concentration and not an iota of involvement of conventional armoured, motorised or mechanised infantry formations or close air support associated in the classic understanding of the Military Doctrine the outcome in the form of demonstration of the intent to break through the opponent's lines of defence, dislocate the defender, unbalance the enemy by making it difficult to respond, and bring about complete desired annihilation was loud and clear. The capability to carry out such an insertion with precision and fraction of cost compared to a conventional airstrike penetrating and exposing the vulnerabilities in impregnable air defence systems is just the tip of iceberg of potential capabilities and threats enabled by technology and an imaginative mind alone. Stealth, surveillance, avionics, sensors, communication amongst many others with innovation were the basic ingredients of carrying out such an act causing the resultant disruption aka the modern-day Blitzkrieg!!

The world over now there is a buzz centred around the advent of Disruptive Technology which is making waves across all spheres and interestingly has started shaping Military too though much divorced from the deep-rooted hypothesis of Revolution in Military Affairs. Intriguingly this draws away the Military from the familiar hunting ground and comfort zone of remaining embedded in evolution of weapons technology, information technology, military organization, military doctrine as a consequence of evolving doctrines, strategies, tactics and threat perceptions. ***A totally new dimension is staring at the possible ways of exploiting these technologies and waging warfare in different domains and dimensions.*** This not only requires but necessitates a transformation which is transcending from sustainable to disruptive technologies in an extremely dynamic and evolving matrix.

An understanding and evolution of the new paradigm with its possible ramifications and challenges the security forces will face when using disruptive technologies to counter emerging threats is therefore imperative. Rightly so the Indian Army Chief Gen Naravane commented that the Indian armed forces need to invest heavily in "disruptive technologies" that are becoming critical in modern day fighting calling for an overarching National Mission in the arena[1]. This was on the occasion of a seminar conducted on the 'Impact of disruptive technologies on the fighting philosophy in future conflicts' indicating that the concern has been taken note at the highest echelons and thought process initiated to invite adequate emphasis. ***What stands out from the statement is the call for an overarching National Mission*** in the arena which typically does not happen so in preparing to combat a conventional threat.

The Advent

The Fourth Industrial Revolution (4IR or Industry 4.0) is the ongoing automation of traditional manufacturing and industrial practices, using modern smart technology. Large-scale machine-to-machine communication and the internet of things (IoT) are integrated for increased automation, improved communication and self-monitoring, and production of smart machines that can analyse and diagnose issues without the need for human intervention[2]. The fourth Industrial revolution what it means and how to respond was the subject of an article by Klaus Schwab, published by Foreign Affairs[3] in Dec 2015 and introduced to the world at large during the World Economic Forum Meeting in 2016. He goes on to say that it is the ***'brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another***. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before'. However, in essence it is not really a new form of technology, but in fact a revamped

1 Times of India 26 Aug 2020

2 https://www.techradar.com/news/what-is-industry-40-everything-you-need-to-know 16 July 2021

3 https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution 16 July 2021

approach inspired by new advancements to achieve results that weren't possible with same technologies years ago. Looking back at the third industrial revolution from the late 1950s to the late 1970s which marked a profound change from analogue, mechanical, and electronic technology to digital technology, the fourth is the move towards digitisation. Industry 4.0 uses the Internet of Things and cyber-physical systems such as sensors to collect vast amounts of data that can be used to radically change the way business is done in virtually all spheres of life. There are a large number of components but the driver has been digitisation and automation over processes such as Internet of Things, Cloud computing, artificial intelligence cognitive Thinking and Cyber physical systems. Innovations in the physical, digital, and biological spheres is transforming entire systems of production, management, and governance in the businesses. The advent of 4IR has resulted in disrupting industries worldwide and living in a connected world and disruption anywhere creates a ripple effect. So, the manifestation of this revolution is the emergence of disruptive technologies.

Spectrum of Disruptive Technology

While surmising that the Fourth Industrial revolution is leading to disruptive technology it would be appropriate to trace the origin of this word. It was Clayton Christensen who popularized the idea of disruptive technologies in The Innovator's Dilemma, published in 1997. It has since become a buzzword in start -up businesses that seek to create a product with mass appeal. A disruptive technology to simply state supersedes an older process, product, or habit with definite superior attributes and finds least resistance for adaptation in innovative and flexible enterprises rather than those entrenched in sustained technologies and rigid mindsets. To simply quote Clayton ***"Disruptive Technologies bring to market a very different value proposition than had been available previously"[4].*** So, what are the components of this disruptive technology leading to the violent disruption. Building on

4 Clayton M Christinsen, The Innovator's Dilemma (Harvard Business Review Press 2016) pp. xix

the basic technology base of Internet, Digitisation, Mobile Connectivity, Cloud Computing, Big Data Analytics the innovations leading to Internet of Things, Block Chain, Cognitive Thinking, Robotics, Nanotechnology, Drones, Next Generation Genomics, Renewable Energy, 3D Printing, Artificial Intelligence, Autonomous Vehicles, Virtual and Augmented Reality, Hypersonic Systems, Smart Grids resonate with Claytons statement that these bring forth a value proposition not thought of earlier.

These emerging disruptive technologies such as artificial intelligence, big data, quantum technology, advanced robotics, autonomous systems, new advanced materials, blockchain, energy storage, hypersonic weapons systems and biotechnologies applied to human enhancements amongst many others are expected to have a disruptive impact on defence and revolutionise future military capabilities, strategy and operations. The manifestation in the form of the drone attack in Saudi Arabia was just one of exploitation of capabilities available. And these are ***clear indicators that this is an inflection point where transformation to meet the new challenges is inevitable*** however the level and scope of this transformation needs to be defined.

Threat Matrix and Defence Preparedness

Countries all over the world have gone back to examine the defence strategy in face of disruptive technologies emergence and implications for Military Organisations. While the US has routinely been redefining, the landscape given their role in Global Context it was in a very well brought out research article by Bulgarian Defence Institute “Prof Tsvetan Lazarov” which comprehensively examines the changing strategic environment and global technological trends with their implications in the defence domain[5]. There is a brilliant analysis of the impact spanning across all EU & NATO nations and concludes that while the future will see significant change in the nature of war but the new emerging technologies do not necessarily have the same effect on all layers and dimensions. A very brief recap of

5 https://www.jdst.eu/publications/defence-strategy-and-new-disruptive-technologies-nexus-implications-military 17 July21

the threat matrix and defence preparedness in our context will be essential to understand the implications of the disruptive technologies.

The complex threat spectrum in our context ranges across nuclear to sub conventional coupled with the terror canvas extending the whole gambit from asymmetric warfare to hybrid in nature. There is no sign of early resolutions of territorial differences with either of the neighbours and the increasing belligerence reflected in the events unfolded in Jun 2020 only go on to make the threat potent and real. Aspirations of China in the Indian Ocean with all the economic and technological might is impacting the global security concerns too. With all resources at its command the stance is aggressive and only indicates that not much has changed or will change. On the other hand, Pakistan in the present state continues to aid terrorism and insurgency and recent events in Afghanistan with the US withdrawal will only further embolden its mischievous intents. The collusion angles between the neighbours are equally worrying and something which cannot be overlooked. Across the eastern borders too there is not much which is going to change though the manner it will be dealt is already shaping up. There are likely implications for us. ***Notwithstanding the above the emerging security environment will still be radically different from what it has been significantly in marking a departure from the era of large scaled protracted conventional conflicts.*** While not reducing the relevance of conventional force levels whether it is Land, Air or Sea, there will be a need for faster swift and decisive capabilities dominating Cyber, Digital, and Space and building capabilities to mitigate asymmetric and hybrid threats as well. To that extent the setting up of the integrated Cyber, Space and Special forces divisions as also the recent restructuring and ongoing validation of the Army Integrated Battle Groups is timely and reassuring. So, to sum up while the threat of a large-scale war may diminish but the threat scenario continues to be same and in fact become more complex with the new dimensions highlighted.

Defence Preparedness and Disruptive Technology

The aim of any defence preparedness is to close the capability gaps

and a continued strive for modernisation to meet the future threats and challenges. It is a continuous process marked by inductions, upgrades, innovations, technology infusion in a balanced manner for near-, mid- and long-term readiness of the armed forces. In a volatile, uncertain, complex and ambiguous environment digital readiness with timely accurate reliable information flow will play a pivotal role. ***Time has now come that we adopt a mixed strategy of retaining the traditional platforms and adopt disruptive transformational technologies leveraging innovations and opportunities available.***

A look at the technologies and their applications will illustrate the host of options and opportunities across all combat platforms: -

TECHNOLOGY	**APPLICATIONS**
Wireless technology, Cloud Computing, Block Chain, Quantum Computing	A revolution in automation and streamlining of processes leading to digital distribution and decision making over range of devices from multiple location options in extreme terrains, Reduction of form factor, signatures, Cyber domains. Diffusion of power and rapid decision cycles.
Small low-cost computing and storage devices	
Big data and advanced analytics	
Internet of Things - High speed Networks and Data centred hardware	
Advanced Low-Cost miniature smart sensors	Communication, surveillance, detection, deception and integrated decision making
Artificial Intelligence and Machine Learning, Computer Vision	Rapid Decision making, quantum change in human and machine behaviour, Predictive Maintenance
Advance display technology with Enhanced Natural user interfaces	Provide real time imagery and possibility of 360° display
Advanced Robotics and Robotic Exoskeletons	Access to areas without risks and enhance efficiency
Virtual and Augmented Reality	Provide a digital real-life experience, enhanced Simulation
Wireless and RFID devices	Reduced footprints, signatures

Autonomous Vehicles	Enhance the reach with low threats to own forces, unhindered access
Renewable Energy and New Generation Battery Technologies	Sustained exploitation of devices at extreme conditions and reduced dependence
Advanced material Technology, Nanomaterial, Memory Metals, Self-Healing Materials	Enhanced Mobility, Survivability of Platforms, reduced payloads, longer exploitation avenues
Selective Laser Sintering	Directed Energy weapons
3D Printing Additive Manufacturing	Availability of solutions in near time frame and in remote locations.
Hypersonic Technology	Launch from standoff platforms

The application spectrum virtually affects man and machine in a manner never comprehended in the past. From enabling an Infantry soldier by empowering him with real time information and decision-making tools, providing him battlefield transparency and ability to unleash lethality against any form of threat to light weight, agile, extremely mobile, connected platforms with enhanced survivability attributes. This is true for Mechanised assets, Artillery Guns. Radars, Aviation, Battleships, Space Crafts, Communication, Command Control Centres, Logistic Network and Infrastructure and Battlefield Sustenance & Predictive Maintenance. ***Compressed OODA cycles will demand from the Commanders a dynamic and complex mind set change to respond to these technology enabled systems in a real time frame marking another form of preparedness for which a transformation is not only essential but imperative***.

Disruptive Technology and Transformation

Interestingly world across the mantra doing rounds today is 'Transform or Perish' as a consequence of the impact of these disruptive technologies and is not industry specific but all over be it manufacturing or service sectors such as banking, tourism, medicine, hospitality, education, cyber security, communication, media or entertainment amongst host of many

others. However, the same when it comes to our threat perception, preparedness, organisational structures and future modernisation the impact is not in the same measure though still alarming. To adopt any technology the foremost requirement is a shift in mindset which is not academic but a personal adaptation. ***Further implementing a technology alone does not produce a transformation till the time the organisation is not convinced of taking advantage of the potential of that technology or in other words fully internalise what it means.*** Further as evident the impact of these technologies has two dimensions one being on the entire force structure and the other on selected applications.

When it comes to the entire force structure it implies a mid to long term roll out as it finds a place in upgrades, plug-in solutions, acquisitions, and modernisation. There is an element of inherent risk aversion in adapting to new solutions being familiar with set technologies and being confident and assured of the performance so it will be a tardy process. These would virtually include new generation platforms fully networked, with enhanced capabilities in the form of mobility, lethality, enhanced survivability capable of exploitation in extreme conditions over protracted employment cycles. This would necessarily force a transformation towards leaner, agile, theatre and threat-based capabilities rather than holding a conventional force for catering to any eventuality. The theaterisation and integrated battle groups are good start points to move towards the transition. However strategically the intent shall remain same the difference being in the radical tactical gains provided by these technologies.

The short-term diffusion is more intriguing. These will ***need re-shape in thought process and will follow the technologies with imagination, innovation which will cause disruption.*** Therefore, structurally there is a need to raise a viable force compact in composition but empowered with operational knowledge and experience, technically competent and with full flexibility. It should be a ***homogeneous mix of combatants, technocrats, cyber experts, research scientists, young systems engineers and academic experts. They will not own***

assets or command troops but constantly look at opportunities to be exploited in all domains be it space, communication, cyber, surveillance, data processing, artificial intelligence in a collaborated environment. They will be problem solvers and sharp shooters armed with technology and hungry for opportunities to counter emerging threats, Domain specialisation with limited relevance is the need. Examples of Drone strikes, cyber warfare, spoofing, disruption in communication networks, data breach, psychological warfare, disabling surveillance grids, mapping of terrorist network, cognitive modelling, disabling control centres, penetrating decision networks are just a few scenarios which can be made live. A broad array of low-cost, unsophisticated technological advancements such as drones and robotic technologies are readily accessible and can be employed innovatively as weapons. This is easier said than done. The forces need to think in this direction critically whether it is integrating in Operations, Cyber division or perhaps a new de novo structure. It is Special Forces Division in a totally different dimension armed with a variety of skill sets and hence the need of a cross functional dynamic team. So, in essence an ***'Emerging Defence Technology Bureau'*** comprising of an integrated structure under the CDS will be an optimum requirement with a National Mission footprint.

Another significant transformation is to realise that this time this revolution is not being driven by the Forces, but it is ***being driven by the market and commercial ventures and they must follow and adopt soon*** before the emerging and disruptive advantage is seized by someone else, or it is no longer in the realm of disruptive technology. The pace and rate of technological change is neither under control of the defence forces nor responsive to what the forces want. This is not about designing and building systems that can adapt and align to threats. The conventional emergence of the likes of Internet, Radar, GPS etc through Defence R&D and applications is past and now the equation goes a change and clearly the curve has tilted. A related challenge is therefore adaptation and become fast followers of these technologies. They will not be driven by the Forces in the form it can serve the end means but means will have to be invented to meet the ends. The commercial

enterprises too which have been quick to adapt are emerging winners and others struggling even to retain their place. If Zomato and Uber can virtually drive a service out of a room without owning the assets and yet be effective in their venture it is just the human intelligence, creativity, innovation and an imaginative application. Yet another challenge is finding an anti-dote in a near time frame – there is a drone threat – we need anti-drones, there is jamming we need jammers, there is malware we need healers, and this is a new world for the forces. It is the mind of wars in the most intense form armed with technology. The disruptive impact is in the hand of the user.

A fall out of the above is ***how to acquire this disruptive technology in a process driven bureaucratic framework.*** The solutions are in the form of innovations, start-ups, cross functional, non-platform based and often in the cognitive domain. They will also not necessarily be in the military domain and will invariably be associated with be a great element of risk in their ultimate utilisation, sometimes the ultimate utilisation too may be hazy and hence an integrated and empowered structure is essential. It will also mark a departure from monopoly suppliers and impinge on the conventional sources and methods. The bright side of all this is however that ***these do not carry the baggage of old entrepreneurial model and are neither capital, equipment, platform or infrastructure intensive and have noticeably short gestations and relevance*** and hence an agile and empowered framework should be able to deliver.

So, while working out an acquisition reform concurrently there are related issues of Regulatory Reforms, Intellectual Property Reforms, Security Collaborations and a continuous engagement with industry to be positioned back as drivers rather than as followers. This is feasible through investments in innovation and exploring alternative strategies and provide an ecosystem to deliver technologically advanced solutions towards modernizing. The ***initiatives like Innovations for Defence Excellence, Technology Development Fund, Invest India, promotion of start-ups, incubation cells in leading academic institutions are fine examples*** and need to be earnestly followed up. Ideally, they

all should be structured around a composite structure rather than be fragmented under different verticals and here is the connect with the structural reform discussed earlier.

In Summation

The fourth industrial revolution has unleashed a fundamental change in the way we live, work, think, communicate and operate by bringing forth a host of technologies capable of disruption to the established norms and processes. ***And we are not talking about breakthrough technologies but innovative technologies with easier accessibility but profoundly different in outcomes***. Driven on computation, data analytics, artificial intelligence, nano material, smart sensors, advanced human-machine interface, augmented realities coupled with imagination, human intelligence, cognitive processes the scope has no boundaries,

This characterises a new chapter which is tending to merge the physical. digital and biological worlds in a way that creates huge promises and the speed, breadth and depth of this is forcing all to realign and create values in whichever space we operate. It is more than tech driven and opportunity lies to look beyond these technologies and create value proposition***. For the defence forces it brings forth an opportunity to augment the military modernisation without impinging on the fiscal constraints.*** The new emerging technologies do not have the same effect on different layers and dimensions of defence strategy neither do they have the same impact across all operational and tactical domains. Hence, an incremental and calibrated adaptation is necessary to prepare for tomorrows warfare dominated by digital battles interconnected in networks without compromising on the defence preparedness in light of our long-term security threats and concerns.

The ***clear challenge for the leadership is to create an environment which facilitates the transformation*** because this needs a new soldier to think differently and behave differently something the mindset is not used to. People and not technology alone are the most important piece in the digital transformation puzzle. And to quote Steven

Johnson “If you look at history innovation doesn’t come just from giving people incentives, it comes from creating environments where ideas can connect”. So going beyond technology and people it is the environment and space which is critical.

We are at a cusp where options are closed and there is no alternative and while it is not question of transform or perish but it is at the peril of losing out an opportunity to find ways and means to wage warfare in a manner never comprehended earlier, so the sooner we get on board the better it is for our quest of modernisation and capability enhancement and addressing security concerns across all spectrums and domains.

***Lt Gen Sanjay Verma,** PVSM, AVSM, VSM** (Retd) is former Director General Capability Development IHQ of MoD. He is presently Consultant to DRDO.

COLLABORATIVE PATHWAYS FOR DEFENCE R&D TOWARDS ATMANIRBHARTA

Dr Sateesh Reddy, Secy DoD R&D and Chairman DRDO*

"Making India self-reliant is the only way to ensure that the 21st century belongs to India."

—Prime Minister Narendra Modi

Abstract

Development of systems based on advanced technologies in all domains of defence like missiles, ground based combat systems, ammunitions, aeronautical systems, naval systems, computing and electronics systems, cyber technologies and life sciences requires the adoption of multiple development approaches. System engineering is to be supported by the growth of all segments of science, technology and industry, leading to the production by the Indian industry. Collaborations with these segments in an integrated and systematic way is the only way to achieve the dream of self-reliance. Multiple strategies are being implemented to increase the pace of defence research and development in the country. Collaborative efforts taken up during the COVID-19 pandemic paid rich dividends in bringing out products and technologies to combat COVID. Learning the new normal and simultaneously keeping the timelines of the project taught us to be more resilient and focused. New policies and methods to engage Users, Academia, other Scientific Organisations and Industry were quickly introduced and streamlined. These consist of increasing both depth and breadth of collaborations with all stakeholders. Implementation of new policies and increased

interactions has resulted into multiple projects showing promising results. Building on our existing strengths and working on the advanced and futuristic technologies, DRDO is leaving no stone unturned to achieve its goals of providing cutting edge technologies to armed forces and steadfastly moving towards the goal of AtmaNirbhar Bharat.

In this era of exponential technology transformation, it has become imperative for research and development organizations to adopt to the new normal of rapid prototyping, accelerated product development and compressing deliverable time lines. Research to mass production needs to be achieved in shorter time spans, meeting the requirements and maintaining the quality. Reduction in the time for product deployment has to be achieved while working towards the national imperatives of Atmanirbharta. As the nation's premier defence research and development organization, DRDO plays the preeminent role in addressing the demanding challenge of not just innovative defence systems towards comprehensive national security but raising to the challenge of meeting the needs of the nation at times of need such as the ongoing COVID pandemic. DRDO being at the forefront of technology and process innovation has leveraged hyper collaborative pathways to achieve significantly compressed timelines.

DRDO has been undertaking the unknown challenges as well as research related to improving known capabilities. Research in areas of cutting edge technologies ensures development of the long term capabilities and assets while incremental research and indigenisation efforts are critical for the present. Both these research perspectives are important and their co-development is necessary for the creation of credible deterrence and maintaining a potent operational defense capability. DRDO has developed processes and mechanisms to create actionable collaborative pathways between Academic Institutions, Labs and Industry to achieve accelerated and tangible output for both the research perspectives.

Balancing the basic and applied research in pursuing technological advances is the most important factor for defining the directions of

defence research. Today's basic research lays the foundation for tomorrow's product developments. For creating maximum options and harnessing majority of technological directions, efforts are required to plan the broad as well as promising focus areas.

With these principles, DRDO is on the mission to design, develop and enable the production of state-of-the-art sensors, weapon systems, platforms and allied equipment for armed forces. DRDO also provides technological solutions to the services to optimise combat effectiveness and to promote well-being of the defence personnel. Development of infrastructure, committed quality manpower and building strong indigenous technology base is taken up for achieving these objectives.

DRDO is a network of 43 laboratories which are deeply engaged in developing defence technologies covering various disciplines, like aeronautics, armaments, electronics, combat vehicles, engineering systems, instrumentation, missiles, advanced computing and simulation, special materials, naval systems, life sciences, training, information systems and agriculture.

Today country is self-reliant in technologies related to Missiles, Radars, Sonars, Main Battle Tank, Fighter Aircrafts, Electronic Warfare Systems, Guns, Torpedoes, Communication Systems and many other defence systems. This has led to the indigenous development and production of these defence systems within the country. DRDO is developing technologies for all major defence domains and with its vast design and development capability, it has formed a strong foundation for Atmanirbhar Bharat. Some of the noteworthy defence products developed by DRDO are Light Combat Aircraft, Tejas; Main Battle Tank, Arjun; Air-borne Early Warning and Control System, Netra; Multi-Barrel Rocket Launcher, Pinaka; Surface-to-Air Systems, Akash, LRSAM/MRSAM and QRSAM; Beyond Visual Range Air-to-Air Missile, Astra; world's longest range artillery gun, Advanced Towed Artillery Gun System (ATAGS); many advanced Armaments and Ammunitions; and a wide range of Radars and Electronic Warfare Systems. These have given quantum jump to India's military might generating effective deterrence and providing crucial leverage.

Several major projects for the development of defence systems are going on with significant milestones already achieved. While defence systems are being developed for the use of armed forces, there is continuous thrust on cutting-edge technologies which have defence applications. Technology demonstrations are the path to adoption into the defence application. Anti-satellite missile test, Hypersonic technology demonstrator vehicle, Quantum communication and Quantum Key demonstration, and LCA landing on Aircraft Carrier Vikramaditya are the mileposts which very few countries in the world have scaled.

The work in multi-disciplinary domains is undertaken as an integrated organisation with the help of various development partners in the country. DRDO has enabled an excellent eco-system within the country wherein it collaborates with academia, industry for the development of systems and sub-systems, armed forces, sister organisations in scientific areas and think tanks to design and develop the systems within the country. DRDO has not only taken up design and development, it has taken up all initiatives to streamline and support the production of systems by the industry.

It was during the pandemic that DRDO team across the country rose to the occasion for the social cause under the circumstances of exigency. DRDO contributed in making many products, technologies, designing innovative hospital aids, drug and diagnostics, providing infrastructure like hospitals and operating test laboratories. DRDO also continuously monitored and did hand holding of industry for realising the crucial systems and equipment. DRDO has worked shoulder to shoulder with departments of central health ministry, state government bodies, industries and medical practitioners in a seamless way to realise covid specific aids, facilities and systems. DRDO while supporting India's fight against corona pandemic never lost the sight of its goals to empower India with cutting-edge defence technologies.

Intense Collaborative Efforts during Pandemic

DRDO by virtue of its expertise and experience in various engineering domains and work in nuclear, biological and chemical (NBC) defence at various life sciences laboratories, has specialised set of equipment as well as expertise which was utilised for Covid testing, PPE testing, Mask design, drug development and many other activities. DRDO scientists also undertook the design of various equipment to arrest the spread of the pandemic. These products and technologies are mostly spinoffs of the existing technologies of defence, or utilizing the expertise of scientists in various fields like electronics, control flow, software and hardware design. A few of the products and the collaborations undertaken thereof are brought out.

Under the aegis of Society of Bio Medical Technology (SBMT) indigenous Critical Care Ventilator (CCV) was developed by DRDO way back in 2004. This expertise and knowhow were utilized to design, develop critical ventilator components and software in a very short period of time. DRDO's facilities were utilized 24X7 during the months of April and May'20 to ensure the final design with all advanced features required for Covid-19 ICU treatment. The production of 30,000 ICU Ventilators was done by BEL along with other industry partners. DRDO also headed the Ventilator Technical Specification clearance committee for MoHFW, to assist the ministry for taking decisions on procurement of ventilators.

DRDO PPE test facility was used extensively to test various indigenous PPEs at a very crucial juncture when only one such facility was available in the country. DRDO developed PPE technology was transferred to industries and production was ramped up to meet the emerging demand. The intense efforts of April-May'20 by Ministries of textile, health along with DRDO made India self-sufficient in the production of PPEs.

DRDO developed a five layered N-99 masks using a nano-web-filter-layer developed and tested in biothreat mitigation project was upscaled during COVID-19 outbreak. DRDO also aided in testing the face masks. Aerosol protection units and face shields were also

designed. DRDO also helped in testing of Sanitizer formulations as per WHO guidelines.

Utilizing the expertise in mist technology for fire/dust suppression and sensor technologies, contactless sanitizer dispenser was developed to meet the prevailing needs of COVID-19 prevention at workplaces/ hospitals. Personnel, vehicle and closed/open area sanitization equipment based on different sanitization methods like UV-C, thermal, Microwave, H_2O_2, Ozonation and Hypo solution using various dispersion technologies have been configured and realized. Shoes and driveway sanitizers were innovated to aid the prevention of COVID-19. Innovative accessories like pocket sanitizers, touch pen sanitizers and multi-purpose access tools were also developed.

DRDO coordinated with PSA to GoI office and worked with Israel MoD for the conduct of clinical trials of four diagnostic modalities in more than 10,000 subjects. DRDO was also a lead participant in operation 'Khula Asman', which intended to open Indian Sky for foreign travellers amid ongoing pandemic. DRDO built a fully equipped 1000 bed Covid-19 hospital in Delhi within 11 days and set a benchmark.

Surge of second wave of Covid–19 in April'21 assumed a proportion which once again unsettled the medical infrastructure posing serious challenges to the health care sector. It was when the complete lockdown was ordered by the states, DRDO was at the helm of providing scientific solutions to the country in combating Covid pandemic. Role of collaboration with scientific organisations and industry became more prominent during this wave, since the tasks were mammoth and interaction was longer rather than just transferring the technology and expecting the sales to be undertaken by them. DRDO worked hand in hand with many industries of various domains to undertake these mammoth tasks.

DRDO was once again directed by the government to make COVID hospitals at various locations across the country. The specifications of the hospital infrastructure on the ICU Beds, Oxygen Beds, and Normal Beds were worked out in consultation with the Ministry of Health and Family Welfare and state health authorities. Supported by the PM Cares, State

governments and CSR funding, these hospitals were built as per the specified medical standards. DRDO has made a total of 11 hospitals and managed the operations with the support of local administrations, medical care staff was made available by AFMC, CAPF and state governments.

As part of PM Cares funding DRDO was tasked to establish oxygen plants. Pressure Swing Adsorption (PSA) based Medical Oxygen Plant (MOP) technology is an offshoot of the On-Board Oxygen Generation System (OBOGS) project for medical grade oxygen generation. India is the 4th country to develop this technology in the world. A total of 866 plants are being installed by DRDO, out of which 120 are being realized through CSIR-IIP industry partners. A low-cost high-performance zeolite alternative for the plants is brought out after extensive testing and benchmarking. Now low-cost, continuous and reliable oxygen supply is available round the clock not only for Medical Oxygen Plants but also for oxygen concentrators.

To avoid the wastage of oxygen from the cylinder-based oxygen support system, an SpO_2 based regulated oxygen cylinder has been designed. Under the PM Cares fund 1,00,000 numbers of manually controlled, 50,000 numbers of automatic control and 10,00,000 Non-Rebreather Masks have been ordered.

An anti-COVID-19 therapeutic application of the drug 2-deoxy-D-glucose (2-DG) has been approved for emergency use. This work was taken up by Institute of Nuclear Medicine and Allied Sciences (INMAS) of DRDO in collaboration with Dr Reddy's Laboratories (DRL), Hyderabad in April 2020 and the approval for use of this drug as adjunct therapy for Covid-19 patients was given in May 2021. The drug is being used to cure moderate to severe patients on prescription.

DRDO has developed SARS-CoV-2 IgG specific ELISA kit, a rapid and reliable antibody test kit. This kit is useful for ascertaining the sero-prevalence against SARS-CoV-2 and for epidemiological purposes in large population of symptomatic/asymptomatic individuals including vaccinated/infected population.

During the time of Pandemic more than 190 number of Technology Transfers (ToTs) have been done for the Covid related products. The process was made easier by empowering directors of the laboratories to clear the ToT documents without Headquarter's intervention. Industries are producing these products in large numbers and supplying them in India and abroad.

The coming together of R&D organisations, PSUs and Private Industries has resulted in increasing the capability and strength of the country. It has established the confidence in the country that unified efforts with unique capabilities of the teams can handle any such future challenges. A vibrant ecosystem has been created within the country for meeting the objectives of "Atmanirbhar Bharat". A zeal to contribute to the society made DRDO scientists go out of their comfort zones and worked shoulder to shoulder with doctors, industry, academia, other ministries and government departments seamlessly and achieved many firsts while serving the Nation during one of the worst calamities of recent times.

Technical Milestones of 2020

Like the entire country, DRDO personnel and its entire ecosystem was affected by the pandemic and disturbances due to lockdowns, but DRDO kept its sight focused on its goals. The year 2020-21 has been extraordinary for DRDO in terms of giving push to the indigenous technologies and products manifestation, of which are the successful test trials of the niche defence systems like, Hypersonic Technology Demonstrator Vehicle (HSTDV), New Generation Anti-Radiation Missile (NGARM) Rudram I, BrahMos Extended-Range Missile with indigenous boosters, Control and Guidance trials of Stand-off Anti-Tank Guided Missile (SANT), Quick Reaction Surface-to-Air Missile (QRSAM), Supersonic Missile Assisted Release Torpedo (SMART) Weapon System, third generation Helicopter-Launched Anti-tank Guided Missile (HELINA) Dhruvastra, Anti-tank Guided Missile (ATGM) for MBT Arjun Mark 2, Man-Portable Anti-Tank Guided Missile (MPATGM), Tactical Missile Prahar, High Expendable Aerial Target Abhyas, Pinaka Rocket System with enhanced range, technical sea trials of Mine Influence Ground Mine (MIGM), Advanced

Lightweight Anti-Submarine Torpedo and Active Electronic Scanned Array Radar 'Uttam' onboard fighter aircraft LCA LSP-2.

Tripod-mounted compact 2 kW Anti-Drone System integrated with jammer, EOTS and NSG radar was successfully demonstrated to representatives of Ministry of Home Affairs, Indian Air Force, Indian Army and Indian Navy. Ground Acceptance Tests of Internal Radar Warning Jammer System for Jaguar DARIN III Upgrade Aircraft was completed in June 2020. Phase-3A trials of Digital Radar Warning Receiver, Dhruti, were successfully completed with satisfactory detection of all ground and air-borne emitters. User Assisted Technical Trials of Air Defence Fire Control Radar, Atulya, at high altitude low temperature were completed. Carrier landing and take-off of Light Combat Aircraft (LCA) Navy on INS Vikramaditya has been a major milestone for the country.

Nurturing Indian Industry for Defence Production

DRDO is working to make India an advanced technology nation meeting the Prime Minister Narendra Modi's dream of Atmanirbhar Bharat and is helping industry in a big way. New DRDO Procurement Manual PM-2020, released by Raksha Mantri Rajnath Singh, encourages more participation from Indian industry, especially start-ups and micro, small and medium enterprises (MSMEs), for achieving self-reliance in the defence sector.

Indian Industry is a valuable partner of DRDO in its endeavor. They play an important role as development partner and/ or Production agencies. DRDO, over the years, has substantially enhanced the technological capabilities of Indian industry through various policy initiatives, sustained engagements and intense technology transfers. DRDO is taking these efforts to next level to transform India into a hub of advanced defence technologies developing state of the art defence equipment and systems. Recently DRDO has launched a scheme to encourage the defence technology startups in the country.

DRDO has been nurturing as well encouraging industry to take up defence manufacturing. Today, more than 2000 industry partners have joined hands with DRDO in delivery of components, subsystems,

systems, platforms and technologies for Indian Armed Forces. Many industries have achieved the capability and the capacity to become the lead system integrator. The technology of all systems is transferred to the Indian Industry for production and supply

Many of the defence technologies developed by DRDO have good potential and utility for application in commercial market too and are transferred to the industry for commercial exploitation. DRDO nurtured industry partners have become part of global supply chain and have started exports of DRDO developed systems to friendly countries. Some of the initiatives to nurture Indian industry for defence production are mentioned here in brief.

Transfer of Technology

DRDO provides the relevant 'know-how' in the form of Technology Transfer Documents (TTD) and handholding support to Indian industry. Technology is transferred to Development cum Production Partner (DcPP) / Development Partner (DP) / Production Agency (PA) without any ToT Fee and to other industries with a one-time ToT Fee @5% of total project sanction cost. Royalty is not charged on net sales to Indian Armed Forces and other Govt Departments. 2% royalty is applicable for sales in Indian commercial market and exports. Details are available at website https://drdo.gov.in/transfer-technologies.

Technology Development Fund (TDF)

In TDF, a corpus fund of Rs. 100 Cr has been created to enable Indian industries, especially MSMEs, for indigenisation of the defence products, sub systems and components. The fund may also be utilised for developing new technologies as required by DRDO, Services and DPSUs. The cost of each project under TDF can be up to Rs 10 Cr. The industry can get funding up to 90% of the project cost. Details are available at website https://tdf.drdo.gov.in.

DRDO Patents for Indian Industry

All patents and relevant intellectual publications are available on DRDO website. These can be used by Indian industry free of cost. For any further support, DRDO is ready for handholding and for working out the modalities.

Development and Production Partner

DRDO engages industry as Development Cum Production Partner (DcPP) / Development Partners (DP) / Production Agency (PA) during the execution of its projects and programmes. The selection of industries is carried out based on procurement rules and procedures.

Testing Support

A number of advanced test facilities and equipment are available at the Labs for trial & testing of the products before acceptance by the User. DRDO provides access to the world-class high-end test facilities to Indian industries involved in designing, developing and manufacturing. The list of these Test Facilities is given on DRDO website. This assures development of high-quality defence products.

Evaluation and Certification Support

DRDO provides unique certification services to the niche industry for aerospace and crypto products. CEMILAC provides the certification support to industry for military airworthiness. SAG, Delhi provides testing and certification support for IT and crypto products developed by industries on request of Services.

SoP for Export

A Standard Operating Procedure (SOP) is promulgated to assist Indian Industry to export products developed with DRDO support. An export compendium, comprising of DRDO products having potential of export, has also been prepared along with details of manufacturing industries.

Technological and Scientific Support

Technological and scientific support will be provided to industry through deposit work route by DRDO on need basis. The interested industry may contact DRDO though our website.

Systems and Subsystems for Industry to Design, Develop and Manufacture

Indigenous design, development and manufacturing of advanced defence systems requires vibrant defence ecosystem with industry participation. In line with the aim of 'Atmanirbhar Bharat', it is appropriate that the industry takes over development of technologies and systems where it has developed the capabilities. To this effect, DRDO has identified 108 systems and subsystems which will be designed, developed and manufactured by industry only and will not be taken up by DRDO for development. DRDO may provide scientific/ technological support and testing support wherever required for the development of these systems and subsystems on case-to-case basis. In common terms we call it 'negative development list' for DRDO.

DRDO Products for Export

Many indigenously developed systems are inducted into Indian Armed Forces after extensive field evaluation. In the process, these systems attain benchmarks of international standards and, therefore, become potential systems for export. Export of indigenously developed defence products provides economic and political advantage to a country. In order to articulate the emerging geopolitical compulsions, more and more Nations are utilising "Defence Diplomacy" as a strategic tool. Concurrent to the recent challenges in global economy and geopolitics, India has taken those necessary steps towards converting itself from the world's largest defence importer to the exporter of indigenously developed Defence products. DRDO developed products have created an interest among several Nations. Some of the systems like radars, Akash missiles and simulation systems have been exported.

DRDO supports industry in evolving the specifications of the export variant of the products (based on DRDO technology) to enable industry to respond to the RFPs of friendly nations. DRDO also carries out customization of product to meet the requirement of customer countries. The "DRDO SoP for Export of Military Equipment" facilitates Indian industry and DRDO labs to provide necessary technical support for responding to request for information before necessary approval from MoD is obtained by the industry. The DRDO SoP for exports is in line with the MoD SoP for exports and provide assistance to Indian industry to address the export needs of the products designed and developed by DRDO.

Engagement with Academia

DRDO has been working with academia for more than 50 years. DRDO has networked with 300 Academic Institutes which work on the basic research problems of relevance to defence applications. Till date academic projects of approximately Rs 1100 Crores have been sanctioned under various mechanisms operated by DRDO. Various vehicles of research and development have been instituted to undertake the defence specific research. Contract for Acquisition of Research Services (CARS) is to enable Lab/Estt Directors to engage academia as per requirement and select the academia to acquire the specified R&D activity. Projects through Extramural Research Sanction are for strengthening and nurturing defence R&D capability to develop technologies in diversified fields, create suitable infra-structure and committed quality research manpower in the country for defence related domains.

Four boards namely, Aeronautical Research & Development Board (AR&DB), Naval Research Board (NRB), Armament Research Board (ARMREB) and Life Sciences Research Board (LSRB) have been operating multiple projects since multiple decades. Under these boards, many impressive contributions have been made by academia to solve various scientific and technology problems of defence domains. Our recent initiative for promoting M Tech in defence technologies in Indian universities is an attempt to lay a strong foundation for a vibrant defence R&D and manufacturing ecosystem.

DRDO has been strategically endeavouring to establish the ecosystem for Directed Research through academic collaboration with a vision to make India a global technology leader and attain self-reliance in next generation defence technologies. DRDO provides support to academia to carry out Directed Research in the identified research areas related to defence application through Advanced Technology Centres (ATC) and Centres of Excellence (CoE). These centres are established to harness & synergize the combined strength of academia, student community, research fellows, niche technology industries & DRDO scientists to provide impetus to research & innovations. These centres focus on conducting directed scientific and technology based research in the advanced areas of technologies with multi-institutional collaboration. Strengthening the research centres at various universities is for accelerating the research of TRL1 topics to TRL3 and TRL3 to TRL6.

Bracing the Disruptive Research

DRDO is working on the next generation defence systems in the areas of missiles, fighter aircrafts, tanks, radars, sonars, artillery and other warfare components. The advancements in the constituent technologies are being incorporated in the designs. Adoption of new technologies requires establishment of advanced testing facilities and ground work for this has started. Hypersonic wind tunnel, aeronautical test range and shore based test facility are some of the examples which are sound foundations for advanced defence systems development. Many other facilities are in pipeline for the testing of systems for higher performance and different parameters of effectiveness.

DRDO is also working on the disruptive technologies like artificial intelligence, cyber technologies, space defence and networking of systems for high level of integration. Adoption of these technologies to defence is of utmost importance while meeting the stringent operational requirements and quality. Efforts have been initiated to streamline the development of these systems and integration with the defence systems. Undertaking these activities requires skill development, infrastructure development for prototyping and testing, adopting new

paradigms of development specific to these new technologies and incorporating modern practices to accelerate the development. Whether it is the establishment of compute and data management expertise or the requirement of highly mathematical and analytical research expertise, many new initiatives are being taken in each and every laboratory which are being monitored closely to overcome hurdles and find the ways to achieve the tangible results.

DRDO has formed Young Scientist's Laboratories for undertaking the deep research into the advanced topics. DRDO has realigned its laboratories to take up the challenges of this decade such that the resources and efforts can be optimized. These young scientists have been given challenging assignments related to the areas of quantum technologies, advanced materials, cognitive systems, artificial intelligence and asymmetric technologies.

Formation of new laboratories, administrative merging of various laboratories undertaking similar research and revision of charter of various laboratories based on the Ram Gopal Rao committee are steps in the direction of optimal utilization of resources for undertaking new challenges. Encouraging startups in the area of defence technology developments is another step taken firmly to encourage the budding ideas and innovative thinking in the defence areas.

Conclusion

While DRDO is investing its efforts towards research and development of advanced defence systems, it is also strengthening the ecosystem by promoting industry, interacting with academia and engaging with other research organizations in the country. The resources required for the next leap are in terms of money for the technology development, advanced test facilities, trained scientific as well as technical manpower, investment by industry in defence production and promoting basic research in defence areas with academia. The requirement also spans the mature industrial support from the non-defence manufacturing. For example, cyber security and semiconductors are required by many

other sectors equally. Similarly, information technology, AI/ML, energy and materials are also common to many other sectors but specific customization is required to meet the defence needs.

In this time of geopolitical uncertainty, India is facing complex challenges as seen never before: internally, to maintain public health and control the spread of pandemic as also rejuvenate the economy; and externally to defend sovereignty and territorial integrity on land and sea both. During his address at CII, Prime Minister Narendra Modi listed out five 'I' to make India a self-reliant economy. The intent, inclusion, investment, infrastructure and innovation are utmost importance to make a self-reliant India.

Country is seeing a major shift towards indigenisation. Some of the important developments like approval of Akash Missile system for export to friendly countries, IAF Order of 83 numbers LCA Tejas on HAL worth Rs 83000 Cr, an order of 110 numbers of MBT Arjun Mk1 on OFB-HVF Avadi and SDR-Tac Order worth Rs 1000 Cr on BEL are due to strong foundations of design, development and production within the country. These will further accelerate the developments and will propel a technology driven economy.

While the industry and academia are tapped for helping the defence technology development, fresh talent is important for infusing energy into the new technology initiatives. The economic investment in defence research will result in better and faster turnaround of the projects which have been envisaged and are raring to go. The march towards becoming a developed nation is to be augmented with commensurate intent and efforts of all stakeholders. DRDO is proactively involved in fulfilling the vision of the Government by taking up challenging assignments of advanced defence technology development and will continue to evolve new initiatives for collaborating with academia and industry for a vibrant environment and inclusive development.

***Dr Sateesh Reddy** is Secy DoD R&D and Chairman DRDO, New Delhi

CRITICAL INFRASTRUCTURE AND RESPONSIVE JOINT LOGISTICS A ROADMAP

Lt Gen BK Repswal, VSM*

Abstract

A well-structured Joint Logistics Doctrine, leveraging varied logistics imperatives; and military infrastructure inclusive of the physical and organisational domains, are necessary for optimum application of combat power. With the understanding that our existing defence logistics systems leave adequate scope for improvement, there is an inescapable need for making an expeditious transition to a robust and comprehensive joint logistics architecture. This would need to be reinforced through resolute physical military infrastructure and capability building, dovetailed into the national infrastructure to address all criticalities, both existing and emergent. An appropriate and time-bound roadmap towards a responsive joint logistics framework is hence mandated as a key operational imperative to empower the Indian Armed Forces to be future-ready.

Critical Infrastructure and Responsive Joint Logistics a Roadmap

"Focus on critical infrastructure building through an integrated approach, right from a number of strategic tunnels and bridges to green expressways, is bound to place India in the league of advanced nations like the US, UK and Australia in the coming two years."[1]

Introduction

Recent path-breaking defence reforms entailing creation of Chief of Defence Staff (CDS), subsequent setting up of the Department of Military Affairs (DMA) and proposed creation of Joint Theatre Commands, have sent a strong signal of intent to the world at large and our adversaries in specific. A reappraisal of existing defence structures, systems, processes, is hence mandated in an expeditious manner. Resource mobilisation to achieve desired preparedness levels in a cost-effective and time-bound manner too is the need of the hour.

Evidently future battlefield milieu will see the employment of multi-domain operations perpetrated through new-age disruptive technologies, in short, intensive operations against a CBRN backdrop. The successful prosecution of operations demands jointness in concept, doctrine, organisation and execution. This would lead to optimal integration of resources and leveraging of innovative technologies, concepts, information networks, transportation and logistics systems.[2] The rapid strides by US, UK, Russia and recently China, in implementation of effective joint structures underscores the expediency required for adoption of same in our forces as well.

Military Logistics-Operations Dynamic

Unlike civilian interpretation of the term “logistics”, “military logistics” has a much wider scope. A widely prevalent definition describes it as “discipline of planning and carrying out the movement and maintenance of military forces.”[3] However, a more comprehensive way to define it would be as encompassing, “design, development, acquisition, maintenance, modification, upgrade, storage, distribution and disposal.”[4] Military logistics has historically yielded battlefield victories for nations possessing sound and superior logistics. Examples are numerous.

Infrastructure, both civil and military, is clearly the bedrock on which edifice of a nation’s Comprehensive National Power (CNP) is built.[5] Requisite military infrastructure facilitates optimum application of

combat power. Critical national civil infrastructure includes a robust road and railway network, airports/ airfields, ports, inland waterways, power, energy and transport infrastructure and more. In military parlance, critical infrastructure comprises of two domains; physical and organisational, wherein the former pertains to fixed structures necessary for war-waging capability and the later comprises of organisational systems and structures required for smooth conduct of military operations.[6]

Logistics Organisational Voids

Lack of integration in logistic processes of three Services, an over reliance on a defence logistics ecosystem built around a thriving culture of committees, absence of single point logistic advisor to Service Chiefs and CDS, and nearly 70% dependence on arms imports are glaring shortcomings which need urgent address. The cabinet approval for corporatisation of 41 Ordnance Factories,[7] promulgation of Defence Acquisition Procedure (DAP) in Aug 2020, and focus on indigenisation in defence needs through "Atmanirbhar Bharat" project (entailing release of two negative import lists covering 209 items[8] by MoD in Aug 2020 and May 2021), are welcome first-steps. However, grey areas remain like the need to evolve joint war fighting concepts, inadequate integration and weak existing logistics structures at HQ Integrated Defence Staff (IDS).

While some measures like the setting up of Joint Logistics Nodes (JLNs) at Mumbai, Guwahati and Port Blair, have materialised, logistics reforms at the apex level are urgently needed. These voids include lack of empowering presence in the National Logistic Council (NLC) at government level and a Defence Logistics Agency (DLA) at MoD level (like in the US). Absence of a fully networked and integrated logistic grid with real-time inventory visibility, standardisation of inventory amongst three services, adoption of life cycle costs concept etc merit attention of key functionaries and decision makers at all levels. Integration must commence top down as also bottom up simultaneously. To integrate the organization and procedures of the military services a National Security Act should be promulgated on the lines of Hoover Commission precedent of the US Govt.[9]

Organisationally the common features of sustainment viz subsistence, habitat, and all forms of troop support (even communication structures) lend themselves to jointness and can be easily built on common foundational planks for all military. As jointness evolves integration must concurrently happen within the Army. Army is singled out here is because 'on land' subsistence structures predominantly belong to and are operated by the Army, and logistical functions in other two services are executed right till apex levels by mainstream logistics cadre and not generalist oversight. Nonexistence of a uniform logistics cadre in the Army is a major void.

Physical Military Infrastructure & Voids

Physical infrastructure along international border (IB) and line of control (LC), is relatively developed and affords reasonable flexibility, however our infrastructure along Line of Actual Control (LAC) is dismal. In contrast, Chinese communication infrastructure build up in Tibet Autonomous Region (TAR) and Xinjiang Uighur Autonomous Region (XUAR), provides the adversary nearly two decades head start.[10], Notwithstanding belated approval for additional 104 roads 6700 km in length, under India China Border Roads (ICBR) Phase-II in year 2020 construction of 73 strategic roads 3323 km in length, approved in year 1999, under ICBR Phase-I languishes, even after 22 years.[11] Though completion of key projects such as Leh-Darbuk-Shyok-DBO road in Ladakh, Ghatibagarh-Lipulekh road in Uttarakhand, Damping-Yangtze road in Arunachal Pradesh, Atal Tunnel astride Manali-Sarchu-Leh axis, Bogibeel and Sadiya bridges on River Brahmaputra, and activation of forward Air Landing Grounds (ALGs) at DBO, Fukche, Nyoma, Ziro, Along, Mechuka, Pasighat, Walong, Vijaynagar[12] in Arunachal Pradesh, stand out as significant efforts, a lot remains to be done. Inland waterways with ample scope in the NE,[13] remain neglected.

Assured all-weather connectivity to Ladakh through Zojila and Rohtang axes is a major operational requirement of Indian Army. Therefore, strategic tunnels beneath Zojila Pass and Baralacha Pass,

Lachulungla Pass and Taglangla Pass astride Manali – Leh axis, assume importance for speedy implementation. Further, tunnel under Sela Pass, three major road projects viz 1800 Km Arunachal Frontier Highway (connecting Kameng Sector and RALP along LAC alignment), Trans-Arunachal Highway and East West Corridor[14] are key to reducing infrastructure differential with China. Also, since our existing communications in Central Sector and Eastern Sector prevent side-stepping of forces due to lack of laterals, it increases complexities for establishing Theatre-level logistics hubs like China has achieved at Naqu, Xining and Shigatse. Cross sector connectivity will optimise logistics costs through faster completion of projects to achieve year-round axial as well as lateral connectivity.[15] Recent experiences in Eastern Ladakh have demonstrated the need for construction of hardened underground ammunition/ FOL storage sheds, missile silos; blast pens for aircraft and long range vectors; fortified command and control centres, permanent defences and living shelters for troops at forward areas. Number of hydel projects have maintenance tunnels which can be used for storage of critical assets including ammunition but these arrangements need to be incorporated at the inception stage itself.

NLC Challenges & Recommendations

The NLC and crafting of a National Logistic Grid is aimed at addressing weaknesses of a system devoid of centralised planning and coordination. Nascent recent steps taken through designation of Division of Logistics, under Ministry of Commerce, as the nodal agency to coordinate issue of “National Logistics Policy (NLP),”[16] may not address defence needs, despite incorporation belatedly of defence recommendations, due to its basic premise to reduce logistics costs from 14 percent to less than 10 percent by year 2022.[17] NLP, only through integration of national and military logistics, is likely to address military requirements of faster mobilisation, improved ports, shipping and transport infrastructure, warehousing, shift to electric vehicles and clean fuels etc. While ministry of Commerce needs to take ownership for providing cholesterol free national arteries that facilitate conduct of commerce most cost effectively,

NLC must have robust representation from Ministry of Defence, Finance, Home, Road Transport and Highways, Railways, Civil Aviation, Shipping, Power, Petroleum and Natural Gas, IT and Communication, Water Resources, and NITI Aayog. The MoD component should have the mandate to evolve and formulate long and short term logistics and infrastructure development plans. It should be dovetailed with Integrated Capability Development Plan (ICDP) and Defence Capital Acquisition Plan (DCAP)[18].

HQ IDS : Major Structural Foundation

DACIDS (OL) at IDS reports to DCIDS (Operations) through ACIDS (Joint Operations). There is a need to create a separate logistics vertical at HQ IDS, headed by a new appointment of DCIDS (Logistics) with three other ACIDS (Logistics) under him to coordinate varied logistic functions. This will lend due weight and proactive thrust to overall jointness and integration efforts. Specific mandate of DCIDS (Logistics) is envisaged as overall ownership of joint logistics ecosystem, besides, formulation of tri-services logistic policies, identification of common use equipment, stores and their procurement, coordinate logistics training, exercise oversight and coordinate functioning of Joint Logistic Nodes (JLNs), Joint Logistic Depots (JLDs) and Workshops (JLWs), and recommending inter-se procurement priority amongst three Services. As our joint organisations and structures evolve, HQ IDS with requisite staffing and cross service pollination is likely to possess the capacity to provide structural foundations for raising a tri-services functional Joint Logistics Command headed by a three star officer holding the appointment of Chief of Joint Logistics by year 2032-33.

Integration Paradigms

Integration of tri-services logistics also involves provision of common IT enabled platforms, NFS enabled communication network, standardisation of sizeable inventory of each service, and test bedding and further expansion of identified JLNs. Intra-service integration of

inventory management systems, based on SAP ERP system and existing successful adoption of CICG of Army Ordinance Corps, is essential to achieve early and smooth integration. Early adaptation of existing systems of all three services and their branches through "Business Process Re-engineering" will achieve a common platform, with adequate communication, and smooth data management. Timely completion of ongoing two year test bedding of JLNs at Mumbai, Guwahati and Port Blair scheduled from Oct 2020/ Apr 2021 and additional 15 JLNs during next phase shall be critical to fast track the integration process.[19]

Plain Look at the DLA Model

Creation of DLA, to function as a Combat Logistics Support Agency under MoD, is necessary to support jointness.[20] Proposed mandate of DLA entails joint procurement and contracting; management of defence supply chains, integrated equipment management, maintenance, repair systems, transportation; and facilitation of augmentation of dual-use infrastructure and technology infusion in defence logistic structures. Here, an objective analysis of functioning of US DLA (raised 1961) and its mandate will be prudent to draw correct lessons in so far as its adoption in our context is concerned. Being an expeditionary force with evolved joint logistic structures since late 1980s, US military has functional commands such as Transportation Command and plethora of defence agencies such as DLA, DARPA, Defence Contract Management Agency (DCMA), Defence Contract Audit Agency (DCAA) and others to support US forces. DLA has 26,000 employees and manages the global supply chain for US Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, 11 Combatant Commands, other federal agencies, and even allied nations. Its mandate involves six main functions to include Aviation Support, Distribution Services, Disposition Services, Energy Services, Land and Maritime Support and Troop Support.[21] In effect, its acquisition programme covers procurement of 5.2 million items with nearly $34 Billion annual sales, wherein it buys stores and distributes food, fuel, clothing, pharmaceuticals, medical products, weapon and system repair parts for military and other customers worldwide. US DCMA, established in year

2000, further supplements the DLA functioning by undertaking entire contractual activities for US DoD. Keeping in view our nascent steps to achieve jointness and integration of defence logistics, a more nuanced and pragmatic approach would yield spinoffs with minimal disruptions. Hence, a gradual evolution of joint logistic structures with DLA functioning as a combat logistic support agency and undertaking entire procurement and contracting functions, besides specialist functions at single service level is worth examining.

Logistics Paradigms & Concept of Operational Logistics

Defence forces across the globe are constrained for resources and their optimal use. In such quest various modern logistic concepts such as Distribution Based Logistics (DBL), Third and Fourth Party Logistics, Performance Based Logistics (PBL) and Smart Logistics with their pros and cons are in vogue in both military and civil domains, it is the "Focused Logistics" concept which has found broader acceptance amongst professional military logisticians for formulation of Joint Logistics Doctrine for Indian Armed Forces. Professional military logisticians define it "as the fusion of information, logistics and transportation technology to provide rapid crisis response, to track and shift assets and to deliver tailored logistics package and sustainment at the strategic, operational and tactical level of operations"[22]. It aims at building a joint logistic system based on speed instead of mass through reliance on faster transportation of stores to achieve a balance between "just in case" and "just in time" logistic philosophies.

Operational Logistics, the term itself seems to sow confusion, as logistics is operational right from the drawing board stage or even before operations can be envisaged. Logistics and 'Operational Logistics' can never have any boundaries defined as it is one seamless organism. Perceived necessity invented this coinage for want of a coordinating body (which loses relevance totally as joint structures and a uniform logistics cadre is a growing reality), however in practice this emerged as a tool of oversight with apex at Command and above levels manned

by officers drawn from non-logistics streams, essentially as an oversight with neither responsibility nor accountability, thereby only leading to increased overheads, no value addition and trust erosion, and consequently the logistician lost his advisory mandate.

Thus time has come to forget this OL concept and revert to Logistics and usher in a Joint Logistic Doctrine based on 'Focused Logistics' which leverages civil military fusion, integration of national infrastructure, theatre based development of joint logistics infrastructure, suitably supplemented by new age, emerging AI driven disruptive technologies such as Blockchain, Robotics, Internet of Things and more.

Logistics Structure at Joint Theatre Commands

Logistic structures at Joint Theatre Commands may have leaner orientation at the top built upon the existing logistic set up at geographical commands of three Services. Logistics chain of each service will continue to function under their respective component commander with staff oversight, monitoring and coordination functions with IDS (Logistics Branch) being exercised by Logistics branch at Joint Theatre Command. At the functional level, besides, coordination actions by HQ IDS, requisite command and control over JLNs, JLDs and JLWs, till such time Joint Logistics Command is raised, should remain with service headquarters of the designated lead service for respective tailor made entities. For distribution of logistic processes, core competencies and domain expertise of each Service in diverse logistic fields covering ammunition, rations, fuel, oil and lubricants, movement and transport, clothing and general stores, engineering support for small arms, UAVs, aviation and specialist equipment etc should be the singular criteria for finalising responsibilities amongst three Services. Augmentation of joint logistics training under overall joint Professional Military Education (PME) framework is another key focus area. Existing capacities of tri services training institutes as well as service specific logistic training establishments, therefore, must be leveraged to train both officers and JCOs/WOs/NCOs with terminal objective of producing specialists

capable of handling all facets of a particular logistic field. Optimisation of resources, disruption in existing entities, downsizing, ushering in of embedded civilian entities are inevitable. However change management should be graduated to smoothen turbulence.

Summary of Recommendations

- **Infrastructure Voids.** Renewed push to fast track ICBR and related strategic infrastructure projects through enabling legislation, increased financial allocations, administrative urgency and tactful engagement of state governments and tribal communities to implement revised roadmap envisaging completion of delayed projects by year 2030. Ongoing construction of $ 48 bn, 1,011 Km new railway line to connect Chengdu in Sichuan province to Nyingchi, close to Tibet's border with Arunachal Pradesh etc, should act as a catalyst to ramp up our infrastructure along LAC.23

- **Joint Logistics Doctrine.** A responsive joint logistics framework to meet operational imperatives of highly intense, short duration future conflicts is a necessity. From this should flow the organisational structure.

- **Iterations and Studies**. Numerous iterations and deliberations amongst various stakeholders have facilitated crystallising of the broader architecture and ecosystem under which these structures will evolve, detailed analysis of relevant processes adopted by major military powers to achieve jointness over last three decades would be fruitful.

- **Emergence of Logistics Cadre.** Integration within the logistics cadres of respective Services is a prerequisite for achieving jointness at Apex. It will provide clarity on career progression and clear direction on all processes, skills development and manning of billets. In the Army various logistics related streams could be grouped into three viz

Quartermaster, Transportation and Ordnance verticals based on functionality. Officers from these streams after 4-5 years of service, on qualification could become part of the Logistics Corps. Further progression and manning of jointmanship billets or Logistics Branch at various levels will be contingent to qualification attained. Officers not qualifying for manning logistics corps/ jointmanship billets will continue to handle assignments related to parent vertical. Likewise integration be commenced in Air Force and the Navy too. Such integration must commence in earnest by December 2021.

- **Near Term Objectives.** For implementing joint logistic plans, planning process, with year 2022-23 as base year, should have three phases; near term, medium term and long term covering two years, six years and ten years gestation period respectively. In the near term, creation of DCIDS (Logistics) at HQ IDS and requisite support staff shall be the first step. Timely test bedding of three JLNs and a JLD/ JLW each and drawing right lessons along with finalising the framework for integrated networked inventory management system, common communication network, codification of minimum 40% inventory of all three services, joint logistics training and centralised procurement of identified common inventory items by lead service should also fructify in the near term by year 2024-25.

- **Medium Term Objectives.** In medium term, which is likely to witness creation of Joint Theatre Commands, Logistics branch at theatre commands with wider representation of service components and a leaner HQ should be established along with augmentation of HQ IDS (Logistics) branch. Provision of physical infrastructure of automated logistic network riding on NFS; conclusion of common contracts for identified common usage items by designated lead service; commencement of joint training at nominated training

establishments and codification of balance inventory of all three Services shall be achieved by year 2028-29. This will manifest in laying the foundations for bringing up a DLA like structure under the CDS.

- **Long Term Objectives.** A fully vibrant and functional joint logistic ecosystem capable of delivering in operations. It should manifest in creation of a Joint Logistics Command, based on augmented architecture of HQ IDS (Logistics Branch) and establishing of balance pan Indian JLNs and JLDs/ JWs as per approved framework. More significantly, creation of a DLA to execute wider procurement and support logistic tasks should be the major deliverable by year 2032-33.

Conclusion

Defence logistics per se is a critical domain, over which patch-work reforms may not generate the desired outcome. The infrastructural gaps in evolving and adopting joint logistics ecosystem pose formidable challenges. Logistics cadres integration within the services and evolution of a logistics corps to man jointmanship billets, as per service specific needs must commence earliest. Logistics should be provided specialist contours and not trivialised with generalisation, for it makes war winning happen. Adroit change management through meaningful iterations and in-depth deliberations between services domain experts and defence think-tanks, is called for. Innovation infusion including AI and quantum technologies will serve the cause of having a modern future-ready logistics support system. Need for concurrent augmentation of physical military infrastructure towards capability development is of paramount importance. Judicious and time bound implementation of proposed road map to achieve a responsive joint logistics framework, under evolving joint war fighting approach is, therefore, a key operational imperative to prepare future ready Indian Armed Forces to counter myriad national security threats.

***Lt Gen Basant Repswal,** VSM, is Commandant, ASC Centre & College, Bengaluru

Endnotes

1 Union Minister Nitin Gadkari, quoted in Economic Times, Aug 23, 2020.

2 Joint Doctrine Indian Armed Forces 2017, Integrated and Joint Structures, p.46.

3 AAP-6 2009, NATO Glossary of Terms and Definitions.

4 Athawale, Pramod Vasant, Core Concerns in Indian Defence and the Imperatives for Reforms, Logistics and Supply Chain Management, IDSA, (New Delhi: Pentagon Press, 2015), p.245.

5 Also see Comprehensive National Logistics Power, Logistics Paper No 1 published by ASC Centre and College (2017).

6 That organisational structures are very much within the ambit of infrastructure has been amplified in Cambridge Advanced Learner's Dictionary which defines it as "the basic structure of an organisation or system which is necessary for its operation."

7 "Why 240 Year Old Ordnance Factory Board Got the Axe, And What It Means"', News 18, June 17, 2021. https:/www.news18.com. Accessed 21 June 2021.

8 "Defence Ministry Notifies Second Negative Import List," The Hindu, 31 May 2021.

9 https://en.wikipedia.org/wiki/Defense_Logistics_Agency.

10 Narender Kumar, "Infrastructure Voids on India's Northern Borders: Implications for India" USI Project, Mar 2019, Page 3.

11 "India China Border Roads" and "Strategic Rail Projects" Jun 2021, https://www.wikipedia/.13 June 2021.

12 "IAF Reopens Advanced Landing Ground in Arunachal", Shaurya Karambir Gurung, Economic Times, Sep 16, 2019.

13 See www.iwai.nic.in for details of various ongoing IWT projects and their status.

14 "China Completes New Highway Near De Facto Border with India", Sudha Ramachandran, Diplomat Brief Weekly Newsletter, 25 May 2021.

15 n.9.

16 "Government Working on a National Logistics Policy", The Hindu, 28 May 2020.

17 Radhika Niphadkar, Sadhika Oberoi, Zeel Davda, Vanshika Bansal, Sejal, "National Logistics Policy, 2020: An In-Depth Analysis of the Policy Uniting the Logistics Sector", Legal Desire International Journal on Law, November 2020, p.9.

18 Behera, Laxman Kumar. Defence Acquisition Procedure 2020: Imperatives for Further Reforms. ORF Issue Brief No 440, Feb 2021.

19 "What Indian Armed Forces Must Do to Avoid Limping into War," Kuldeep Singh, The Quint, April 15, 2021. https://www.The Quint/. Accessed Jun 07, 2021.

20 Anand, Vinod, "Joint and Integrated Logistics System for the Defence Services", Strategic Analysis, IDSA Vol.25, Issue 1, 2001.

21 "What DLA Buys," http://www.dia.mil. Accessed June 15, 2021.

22 Antill P, "Focused Logistics" 22 Aug 2001, http://www.historyofwar.org/. Accessed 13 June 2021.

23 "China's Rail Projects: A Stratagem of Statecraft," Raghu Dayal, Financial Express, Mar 22, 2021.

PREPAREDNESS: ALIGNING OUTCOMES AND OUTLAYS

Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)*

Abstract

Preparedness of the Armed Forces to execute the assigned missions to engage, deter adversaries and, if necessary, fight to secure and promote National security objectives, presupposes desired joint and single service capabilities. These ***capabilities, in turn, need to be crafted through sophisticated long term defence planning, underwritten by affordable budgets.*** *For over three decades India's* ***defence enterprise has groped unsuccessfully with its defence conundrum,*** *supposedly "arming without aiming". This article traces the systemic irresoluteness in India's approach to long term defence planning and budgeting, contrasting it with best practices, and* ***offers pathways to ensure joint capability building by suggesting pragmatic pathways towards force structuring, modernisation, readiness and sustenance, underwritten by budgetary strategies to deliver the desired outcomes.***

Resurgent *India's stature as an influential global power with geo-economic and geopolitical heft in the emerging global order, brooks no argument.* India's national interests span continents. Therefore, t*he capabilities of* ***India's military instrument, the 3rd largest in the world,*** *must buttress the economic, diplomatic, informational, technological and political instruments of State power. Defence modernisation* in India's neighbourhood is continuing at an unprecedented scale and pace,

punctuated by ***military stand-offs and crises****, spurring fielding of new weapons and capabilities by adversaries.* Our adversaries are also leveraging grey zone activities, cyber operations, influence operations, together with economic measures, making ***coercive attempts to further their strategic national interests, without provoking conflict.*** Sharing two long disputed borders with nuclear armed neighbours *makes India's predicament extremely peculiar. Our armed forces, therefore, must* ***be prepared to shape the security environment, engage, deter, constrain and defeat the proximate and immediate threats to the National Interests "now",*** *while c****oncurrently modernising to meet the multi-domain challenges of "tomorrow".*** *This* ***dilemma of twin demands for substantive resources, has remained an endemic challenge for India,*** *as for most Nations.*

Defence Planning- Aligning Outcomes and Capability Development (CD)

Preparedness is about whether the forces can accomplish their missions. Preparedness audits must lead to resource informed trade-off decisions, *balancing the four elements of capability*[1]*: readiness, sustainability,* ***force structures and modernisation. Defence planning*** *essentially* puts together the political/military objectives (ends) and a strategy (ways & means). The ***ends are decided by the politicians based on National Interests*** (eg sovereignty, territorial integrity, domestic cohesion/peace/stability etc). Military planners ***recommend how the forces (means) will be used*** *to accomplish the* ***ends*** and the ***politicians approve the ways (eg deterrence by punishment or denial, defence postures, proactive operations, military coercion, balance between continental threats (now) vs growing maritime concerns, sea control or denial,*** etc). **Plausible scenarios** are chosen to outline the security environment, challenges and threats. Thereafter, ***full spectrum missions and objectives are arrived at, which help derive capabilities over pragmatic time-frames needed to field new force structures,***

1 United States General Accounting Office, Measuring Military Capability: Progress, Problems, and Future Direction, Feb 1986, https://www.gao.gov/assets/nsiad-86-72.pdf

doctrines and weapon systems. Shortfall ***between the required forces and funds creates capability gaps. To mitigate the associated risks,*** the planners ***prioritise competing requirements*** **to deliver a cost-effective force,** capable of ***accomplishing missions with acceptable risks.*** *Regrettably*, *sometimes planners* ***ignore the risks, downplaying the likelihood or the severity of impact of certain scenarios.*** CD is a *dynamic process and the bottom line is that the* ***ends, ways and means must be aligned iteratively, as shown below:***

Objectives->Strategy (ways & means)->Capabilities->Gaps->Risks->Objectives

Approaches to Long Term CD

There are several approaches to defence planning and each can be used independently[2]. However, In practice, long term defence planning invariably employs a combination of a few approaches described below:

- **Resource-Constrained planning.** The objective is to provide a viable capability that is *sustainable within the provided budget.*
- **Technology Driven.** The goal is to obtain operational and *strategic superiority through technology.* New technology is integrated as soon as available.
- **Risk Avoidance.** Traditional and *proven concepts and structures are extrapolated and current ways continue. Defence development adheres to current strategy, doctrines and structure and incorporates* ***new technology, when proven and available.***
- **Incremental Planning.** Existing capabilities form the foundation of *new capabilities. It aims to evolve new capabilities with proven improvements over existing capabilities,* exploiting near-term options, **avoiding risks.**

2 Bent Erik Bakken, "Handbook on Long Term Defence Planning", NATO RTO-TR-069 AC/323(SAS-025)TP/41, RTO Studies, Analysis and Simulation Panel (SAS), April 2003

- **Capability-based Planning.** This is performed in the absence of *specific threats or conditions and entails analysis of* ***likely future operations.*** Defence capabilities are identified based on the mission(s). *The outcome is not concrete weapons systems and manning levels,* ***but a description of the tasks to be performed in generic capability terms.*** Thereafter, ***the most cost-effective physical force option*** *to implement these capabilities is derived.*
- **Scenario Based Planning.** This approach utilises credible environmental and operational ***scenarios for assessing capability or system requirements against mission objectives.***
- **Threat Based Planning.** Capabilities of potential adversaries are evaluated with a ***view to outperform them*** using ***quantitative and qualitative solutions,*** a common *approach during the Cold War.* It is akin to scenario-based planning though *non-threat scenarios (eg humanitarian assistance) are excluded.*

Planners are invariably ***caught in dilemma*** to ***address the proximate threats with higher confidence levels (proven systems)or to accept risks and opt for alternatives which may impose time, cost and even performance penalties.***

Long Term Defence Planning in India

On independence, the Blackett Report of 1948[3] formed the basis of defence planning. Post the 1962 debacle, defence planning has witnessed several fledgling attempts to usher a disciplined approach, inter-ministerial collaboration and bureaucratic/political oversight. A ***Defence Planning Cell*** *(Post 1962) within the Ministry of Defence* ***(MoD)*** *was followed by creation of a* ***Committee for Defence Planning (CDP)*** *under the* ***Cabinet Secretary in 1977.*** The Directorate General of Defence Planning Staff

3 PMS Blackett, Scientific Problem of Defence in Relation to the Indian Armed Forces: A Report to the Hon'ble the Defence Minister (New Delhi, l0 Sep. 1948)

(DGDPS), **with members from other ministries, was later created under the Chiefs of Staff Committee (COSC) in 1986.** With an expansive mandate to arrive at ***balanced force levels to achieve military aims, perspective planning for 15/20 years[4],*** the ***structure proved sub-optimal[5].*** Consequent to the Public Account Committee in 1989, **MoD's defence procurement guidelines in 1992** ***embryonically embraced the concept of a long term perspective plan[6].*** However, the measures remained suboptimal. Analysing India's external security problems and the responsibility for responding to these, *for the period 1947 to 1992, Chris Smith concluded that* it is *not a well-informed or streamlined decision-making process;* the ***key actors are various and common interests few and far between; despite institutionalised rolling five-year defence plans, the process is chaotic and weapons are procured as much on an ad-hoc basis as on the strength of informed debate and planning.[7]***

The *Kargil conflict of 1999 provided the next course correction.* The **Group of Ministers (GoM) Report** (2001)[8] lamented ***the absence of a National Security Strategy (NSS), non-commitment of funds beyond the FY and lack of inter-Service prioritisation.*** It recommended the creation of a Chief of Defence Staff (CDS) with staff ***to prepare a Long Term Defence Perspective Plan for 15-20 years, including Inter-Service prioritisation*** **and a Joint Services Plan;** *a* ***firm indication of the availability of financial resources for the period of 5 years*** by the Ministry of Finance ***(MoF)[9].*** Post creation of Head Quarters Integrated Defence Staff **(HQ IDS) in 2001, the DGDPS was dissolved.** The ***first ever LTIPP (2002-17) was revised in 2007 to cover the period 2007-22, due to the shift from Equipment based approach to Capability***

4 Laxman Kumar Behera, Defence Planning in India, Journal of Defence Studies, IDSA, Vol 4. No 3. July 2010, pp 127-129; https://www.idsa.in/system/files/jds_4_3_lkbehera.pdf

5 ibid

6 Committee of Experts for Amendment to DPP-2013 Including formulation of policy frame-work, July 2015, https://www.mod.gov.in/sites/default/files/Reportddp.pdf

7 Chris Smith, "India's Ad Hoc Arsenal Direction or Drift in Defence Policy?", SIPRI, Oxford University Press, 1994, p. 2

8 "Reforming the National Security System", Recommendations of the Group of Ministers, February 2001, p. 98.

9 ibid

based approach, **adopted by the MoD in June 2006[10].** The MoD averred adherence to a ***'Top Down' approach by articulating NSS, National Military Strategy(NMS) and Military Security Objectives(MSO), for the first time[11]. In 2013,*** HQ IDS commenced promulgation of a Technology Perspective and Capability Roadmap **(TPCR) spanning 15 years, to align the R&D efforts and the industry.** The last one was issued in 2018 which covers the period up to late 2020s.[12]

In **April, 2018, Defence Planning Committee (DPC)** was created under the ***chairmanship of the National Security Adviser (NSA),*** intended to ***"facilitate a comprehensive and integrated planning for defence"[13]. It has four subcommittees: Policy and Strategy; Plans and Capability Development; Defence Diplomacy and Defence Manufacturing Eco-System.*** Its charter includes, inter alia, *defence planning,* ***defence acquisition and infrastructure development plans, including the 15-year LTIPP.*** It has been mandated ***to prepare several draft documents including NSS and Prioritised CD plans for the Armed Forces, in consonance with the likely resource flows[14].***

On creation of the Niti Ayog in 2015, the 13th Plan (2017-22) was dropped. However, ***the MoD prepared the Defence Plan for 2017-22 internally. DAP-2020 outlines a modified the LTIPP process,[15]*** which ***would evolve from the NSS/Guidelines (when promulgated)*** and ***Raksha Mantri's Operational Directive.*** The horizon has been shortened to a **10 years Integrated Capability Development Plan (ICDP),** comprising of two *five-year plans,* **prepared** by HQ IDS ***every***

10 Standing Committee on Defence (2006-07), Ministry of Defence, 14th Lok Sabha, Demands for Grants 2007-08, 16th Report, Lok Sabha Secretariat, New Delhi, pp 46-47; https://eparlib.nic.in/bitstream/123456789/62683/1/14_Defence_16.pdf

11 ibid

12 Technology Perspective and Capability Roadmap; https://www.mod.gov.in/sites/default/files/tpcr.pdf

13 SP Das, Creation of Defence Planning Committee: A Bold Step towards Defence Preparedness, CLAWS, Issue Brief, No 143, June 2018; https://www.claws.in/static/IB143_Creation-of-Defence-Planning-Committee-A-Bold-Step-towards-Defence-Preparedness.pdf

14 ibid

15 Defence Acquisition Procedure 2020, Government of India, Ministry of Defence, 30 Sep 2020, pp 6-8; mod.nic.in

5 years. A **five years Defence Capital Acquisition Plan (DCAP)** is to be prepared by HQ IDS ***based on recommendations of Services HQ,*** considering ***prioritised operational requirements.*** Both **ICDP** and **DCAP are to be approved by the Defence Acquisition Council (DAC).** A ***two years Roll-On Annual Acquisition Plan (AAP),*** **as in vogue,** will be prepared by the SHQ, based on the DCAP. *The consolidated AAP*, *listing* ***prioritised schemes, will conform to the yearly financial limits indicated by MoD (Finance). AAP will be approved by the Defence Procurement Board (DPB).*** **Part A** of the *AAP* will contain a list of **carry-over acquisition proposals** accorded **Acceptance of Necessity (AoN) the previous year and those for which AoN has been accorded during the year.** ***Part B will include acquisition proposals likely to be accorded AoN in the forthcoming year.*** Emergent requirements may be included in AAP on approval of the DPB.

The CDS, created in Jan 2020, **in his capacity as the Permanent Chairman COSC,** has been mandated[16] **to implement** the **DCAP** and **AAP and *assign inter-Services prioritise*** within the ***anticipated yearly budget.***

Long Term CD- The Process

India's current LTIPP (2012-2027), was believed to be amounting to over $223 Billion in 2016[17], 4 years after its formulation. Despite the ***proclaimed shift to a Capability based approach in 2006,*** **in absence of a NSS and planning guidelines,** the extant plan is a ***mere listing of the wish lists of the three Services, with no priorities.*** The inefficient process has drawn wide criticism, including from a former Chief of the Indian Navy[18]. Since the mechanics of the process under evolution by

16 Cabinet approves creation of the post of Chief of Defence Staff in the rank of four star General, Press Information Bureau, Government of India, 24 Dec 2019; https://pib.gov.in/PressReleseDetail.aspx?PRID=1597425

17 Vivek Raghuvanshi, "Source: India Needs $233B in Next 11 Years To Buy Weapons", DefenseNews, 8 September 2016, https://www.defensenews.com/global/asia-pacific/2016/09/08/source-india-needs-233b-in-next-11-years-to-buy-weapons/

18 Arun Prakash, "India's higher Defence Organisation: Implications for National Security and Jointness", Journal of Defence Studies, Vol. 1, No. 1, August 2007, p.28

HQ IDS - Integrated Capability Development System (ICADS), are not available in public domain, ***a process used by NATO countries, could serve as a frame of reference[19].*** Though ***capability requirements would be different for each force/Nation, given the nuanced contexts,*** **joint capabilities functions** invariably include Command and Control (C2), manoeuvre, firepower, protection, intelligence, information and sustainment[20]. Capabilities are a product of doctrines, organisation, training, equipment, leadership and personnel. ***Capability requirement determination answers the questions, "what" and "how much" for each required capability[21].*** The next step identifies capabilities which are **short, sufficient, or redundant.** For addressing the gaps, **non-material options are explored,** ***followed by material (equipment)*** requirements[22]. This **process is executed iteratively, till acceptance of risks by the politicians, where gaps still exist[23].** Prioritised options to fill the capability gaps are then compiled in a long term plan.

The Australian Model for CD[24] & Challenges

Since 2016, Australia follows a 10 Year funding model which provides long-term funding certainty to deliver the **Force Structure Plan (5 years), presented by the Prime Minister.** For the decade 2020-2030, the funding of $575 billion **includes approximately $270 billion for CD. The Force Structure Plan outlines** modernisation programs over a ***20 year timeframe, based on cost modelling tools.*** The Capability priorities and outlays, by themes, are spelt out unambiguously for five war fighting

19 Dejan Stojkovic and Bjørn Robert Dahl, "Methodology for long term defence planning", Norwegian Defence Research Establishment (FFI) 28 February 2007, ISBN 978-82-464-1147-7, https://publications.ffi.no/nb/item/asset/dspace:3318/07-00600.pdf

20 Thomas Crosbie, Getting the Joint Functions Right, JFQ 94, 3rd Quarter 2019, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-94/jfq-94_108-112_Crosbie.pdf?ver=2019-07-25-162025-397

21 Dejan, op.cit.

22 Dejan, op.cit.

23 ibid

24 Australian Government, DoD, "2020 Force Structure Plan", Commonwealth of Australia 2020 ISBN: 978-0-9941680-6-1, https://www1.defence.gov.au/sites/default/files/2020-11/2020_Force_Structure_Plan.pdf, accessed on 25 July 2021

domains and the Forces-wide Enterprise[25]. Besides allotting 72% between Land, Sea and Air domains, Australia has allotted 6% to Information and Cyber Domain, 3% to Space domain, 2% to ICT (Joint Cyber, EW, ISR, Strat Int & C4) and 6% to Armed Forces wide Enabler Programs, **across 35 capability programs[26]. Its *Defence Portfolio Budget Statements 2020-21[27], describe the budget initiatives and appropriations by outcomes and programs, domain wise. Australia has its challenges, too, and plans to reduce the outgo on workforce from 32% to 26% between 2021 to 2030,*** and increase the ***outgo on acquisitions from 34% to 40%.*** Australia uses an **Integrated Investment Program (IIP)** approach to **plan and deliver capability and its sustainment** over long time frames ***to manage budget risks[28].***

The US Model for CD & Challenges

For the Fiscal Year (FY) 2022, the modernisation funding request is $245.6 billion, which includes $133.6 billion for Procurement and $112.0 billion for RDT&E. Besides the traditional capabilities like aircraft, ships, land systems, niche capabilities have been allotted a fair share-***space (9%), C4I systems (5%), missiles and munitions (8%), Missile defence (4%) and S&T (6%).[29]*** *However, even the country with the largest defence expenditure is grappling with military budgetary woes. Mackenzie Eaglen[30] has **argued that without tackling the modernisation challenge, the DoD will remain stuck in an acquisition death spiral. The O&M costs have crowded out modernisation.** Compared to 1986, the FY21 military personnel budget remains roughly comparable, ironically for a smaller force.*

25 2020 Defence Strategic Update, Australian Government, Department of Defence, Commonwealth of Australia 2020 ISBN: 978-1-925890-26-6

26 ibid

27 Budget Related Paper No. 1.3A, Defence Portfolio, accessed on 25 Jul 2021, https://www.defence.gov.au/Budget/20-21/2020-21_Defence_PBS_00_Complete.pdf

28 https://www1.defence.gov.au/sites/default/files/2020-11/Factsheet_Budget.pdf

29 Program Acquisition Cost By Weapon System, US DoD, FY 2022 Budget Request, Office of the Under-Secretary For Defence, Comptroller/Chief Financial Officer, May 2021

30 Mackenzie Eaglen with Hallie Coyne, The 2020s Tri-Service Modernization Crunch, American Enterprise Institute for Public Policy Research, March 2021, https://www.aei.org/wp-content/uploads/2021/03/The-2020s-Tri-Service-Modernization-Crunch-1.pdf?x91208

Category	Reagan Modernisation 1986	Modernisation FY 2021
Military Personnel	28.81%	24.37%
Ops & Maint	28.41%	40.63%
Procurement	28.36%	19.20%
RDT&E	10.70%	14.93%
Construction, Housing & Others	3.72%	0.87%

To rectify end strength shrinkage and atrophied readiness (due to focus on two decades of Counter Insurgency operations), Eaglen has **recommended** enhanced investments, ***including the option of using Defence Working Capital Funds (refundable funds) for modernisation;*** seeking more conservative cost estimates; ***ensuring that new programs are more upgradeable; fielding innovative technologies faster and*** **restoring readiness selectively**[31]***. These measures are instructive.***

UK Approach to Modernisation and CD

UK follows integrated planning and the Defence Command Paper 2021[32], succinctly states that **modernisation aims to make the armed forces more agile, lethal and integrated,** *investing funds to improve* ***readiness, resilience and sustainability, through an*** **"Integrating Operating Concept".** R&D spending, experimentation and investments in **transformative and digital capabilities** are proposed **to enable multi-domain integration** to **compete more effectively in space and cyberspace.** Priority **areas** for **CD include-** Pervasive & full spectrum ISR; Multi-domain C4; Asymmetric hard power; Freedom of access and Manoeuvre. ***UK also proposes to withdraw few equipment and capabilities earlier than their life spans, including*** **Challenger** tanks, **Warrior** IFV, Typhoon aircraft, E-3D AEW&C and some Chinook helicopters.

31 ibid

32 Defence in a Competitive Age, Ministry of Defence, Mar 2021, ISBN 978-1-5286-2462-6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf

Creative CD Approaches for Indian Armed Forces

- **Survey By Delhi Policy Group**[33]. As per a limited sample survey carried out by the Delhi Policy Group, desirable distribution of resources for capability development in different domains could be: *land forces (24%), Navy (19%), Air Force (17%), situational awareness (ISR, Maritime Domain Awareness, Space) (11%), Asymmetric Domains (cyber, information warfare, legal warfare, etc.) (11%), R&D (10%), and CBRN (Nuclear) (8%).* The study recommends that this distribution could be taken as a broad guideline *for planning acquisitions (ICDP/DCAP).* The **suggested allocations, though a paradigm shift, are judicious and may be used *as a frame of reference while formulating ICDP/DCAP.***

- **A Heuristic Model- Takshashila Institution**[34]**.** The authors have suggested a framework for military resource planning which distributes military resources to four suggested Integrated Theatres, two each maritime and continental. For each theatre, 13 different military instruments (which may be modified) have been assumed, ranging from infantry brigades, ships, missiles to aircraft carriers. ***The model advocates a concept of usable power,*** and **assumes five distinct levels of escalation,** ranging from localised tension to full scale limited war, wherein force is to be used appropriate to the situation. *The **framework leverages two parameters for military planning - the employability of a military instrument (given the terrain & escalation level), and its operational importance (OI),*** which may be modified by experts. The model **helps arrive at the *net utility of a military instrument.***

33 Anil Ahuja & Arun Sehgal, "India's Defence Budget: Beyond the Numbers", Volume VI, Issue 4 February 10, 2021, accessed 25 July 2021, https://www.delhipolicygroup.org/uploads_dpg/publication_file/indias-defence-budget-beyond-the-numbers-2209.pdf

34 Prakash Menon & Pranav Valmeekanathan, "M-RAF 1.0 - A Model to Allocate Resources Across India's Armed Forces", Discussion Document 2020-11 V1.0 - 30 July 2020, Takshashila Institution, accessed 25 July 2021, https://takshashila.org.in/wp-content/uploads/2020/07/Military-Resource-Allocation-Framework-Discussion-Document-July-2020-v1.0-1.pdf.

The authors opine that this model is *designed for Long Term Integrated Military Planning and can provide a benchmark for allocation/investment for each military instrument and can assist in prioritisation for acquisition, trade-offs between instruments and distribution of capabilities between theatres.* The model is useful for prioritising inter-theatre allocation of military resources post due analysis. However, for *acquisition related decisions, the* ***model needs to be suitably modified to integrate Military objectives/missions and derived capabilities,*** *so as to surmise mitigation measures, including non-equipment solutions*.

CD for the Indian Armed Forces- Suggested Pathways

Comparing the extant practice in India with the above models, the following observations and recommendations are germane:-

- **Salience of NSS**. There is ***no articulated NSS and CD plans are not approved by the Cabinet/parliament, thus, the linkage between the Political/Military Outcomes (ends) and strategy (ways and means) is at best conjectural.*** Analysts have observed that a military solution to India's challenges is often difficult to implement due to lack of resources, ***yet the cost of increasing military resources is exceeded only by the bureaucratic and political resistance to providing the resources[35].*** The ***promulgated NSS must end India's strategic ambivalence.***

- **Parliamentary Buy-In. There is no budgetary assurance beyond the current FY,** in contrast to the recommendation of the GoM in 2001. ***MoF approved the 10th Defence Plan in its last year (2007), stopping the practice thereafter.*** The Annual Defence Budget fails to invite a debate in the Parliament. The DPC, mandated to develop CD plans ***in***

35 Stephen Coen and Sunil Dasgupta, "Arming Without Aiming: India's Military Modernisation", Brookings Institution Press, Washington, D.C. 2010, pp. 185

consonance with the likely resource flows, can at best assume the flows. Non-approval of the ICDP and DCAP by the CCS/Parliament will **dilute the political commitment, reducing these to bootless errands.**

- **Inter-Ministerial Synergy.** Creation of the DPC will finally ensure inter-ministerial collaboration. However, *synergy and role clarity between the NSA and the Defence Minister, will be critical.*

- **Parochial Service Interests. The MoD has struggled with long term CD since 1992.** The Services have been **plagued by the perceived immutability and primacy of their roles and primacy as a responder to national security challenges.** *Maximalist approaches to planning and prioritising* has **institutionalised their zero-sum approach.** This needs to change.

- **Balancing Ends and Strategy (Ways & Means).** The US has modified its strategy from fighting and winning in two major theatres of war to defeating an aggressor in one theatre, while denying the objectives or punishing an opportunistic aggressor in the second theatre (Ways). It has also reviewed her ambitions in the Middle East (Ends). The US is also downscaling few weapon programs (means). The UK is reducing land forces and retiring from service weapons before the expected life (means). **Such decisions are taken after due debate and approval of Congress/Parliament.** In India, big ticket deals ***spasmodically garner political attention, but no intervention to balance ends/ways and means.*** The **models suggested by the DPG and Takshashila Institution merit analysis** while formulating the ICDP/DCAP.

- **Projects and Programs with Cost Modelling.** Approval of the long term plans, with specific details of projects, programs and projected costs by the CCS/Parliament will ***ensure a whole of the Nation buy-in.*** *Allocating resources specifically*

for Space, Cyber, ICT, C4ISR, EW, Asymmetric Capabilities, Joint capabilities would addresses the emerging threats and align the industry and R&D efforts. Besides, specific timelines ensure ***outcome delivery with accountability.*** Financial prudence be ensured through **cost modelling**, a discipline we lack. Cost Audit and Balance of Investments[36] by the BAE Systems (UK) and the US DoD Cost Modelling Guide[37] provide a good insight.

- **Plan and Technology Horizons.** Though the horizon of the proposed ICDP has been reduced to 10 years, outlining **programs with costs over a 10-15 year horizon,** though challenging, is the **best way to align and incentivise indigenous R&D and private industry.**

- **Modernisation Vs Maintenance Costs.** Across the globe, **modernisation is being crowded** out by ever increasing expenses on operations and maintenance, largely due to increasing outgo on salary/pensions and upgrading the ageing systems. **This challenge requires innovative solutions. Prudent and validated manpower cuts could release human and capital resources for creation of new capabilities in domains like space, cyber, EW and joint structures/functions.**

Budgeting- Aligning The Outcomes, Outputs with Outlays

- **Past Endeavours.** To move from ***"inputs" towards "outputs", a performance budgeting system*** was introduced in **1969,** a ***performance review was sought,*** along with the annual Demands for Grants. **However, the MoD was exempted.**

36 BAE Systems, Our Capabilities: Cost Modelling, https://www.baesystems.com/en/corda-our-capabilities-cost-modelling

37 DoD Cost Estimating Guide, Office of the Secretary of Defence, Cost Assessment and Program Evaluation December 2020; https://cade.osd.mil/Content/CADE/files/MorinMemo/DoD_Cost%20Estimating%20Guide%20v1.0_Dec2020.pdf

In **2003-4, Defence Services Estimates (DSE) Volume-II** was introduced, which listed end user-wise sub-allocations. However, **this document does not reflect any programs or objectives[38].** An **Outcome Budget Concept** was introduced in **2006**, requiring Ministries to mention ***measurable outcomes with budget documents.*** *Some ministries, including* ***MoD, were exempted,*** *but were* **asked to carry out this exercise and voluntarily decide to place it in the public domain, fully or partially[39].** *Presently,* ***the MoD only provides an Annual Report for public information.***

- **India's Defence Budget Size-The Global Context.** India's defence allocation (including pensions) for FY 2021-22 is Rs.4.78 Lakh Crore (US$ 65.5 billion). It is approximately 2.15% of GDP, and **excluding pensions,** approximately **1.63% of GDP,[40] the lowest since 1962.** In 2020, the *US spent $778 billion, China $252 billion and India $72.9 billion, forming 39%, 13% and 3.7%* of global share, respectively[41]. Between 2011 to 2020, *China's and India's defence expenditures have grown 76% and 34% respectively[42].* It is, thus, **evident that India's defence outgo is transparent and modest, despite being spurred by its two revisionist neighbours. This is substantiated by the allocations on the Capital head, as follows:-**

38 CGDA, Army Manual, https://cgda.nic.in/ifa/manuals/army.pdf

39 P R Sivasubramanian, Defence Budget: Towards an Outcome and Programme Based System, Strategic Analysis, Vol. 30, No. 4, Oct-Dec 2006, https://idsa.in/strategicanalysis/Defence-BudgetTowardsanOutcomeandProgrammeBasedSystem_prsivasubramanian_1006

40 Pandit Rajat. Union Budget: Defence budget hiked by just 1.4%, but more money for military modernization. The Times of India. February 01, 2021. https://timesofindia.indiatimes.com/india/union-budget-defence-budget-hiked-by-just-1- 4-but-more-money-for-military-modernization/articleshow/80631424.cms

41 Diego Lopes da Silva, Nan Tian and Alexandra Marksteiner, Trends In World Military Expenditure 2020, SIPRI Fact Sheet, April 2021, https://www.sipri.org/sites/default/files/2021-04/fs_2104_milex_0.pdf

42 ibid

Service-wise Capital Allocations

Service	BE 2020-21 Rs Cr	RE 2020-21 Rs Cr	BE 2021-22 Rs Cr	% Change Over BE 2021	% Change Over RE 2021
Total	**113734**	**134510**	135060	18.8	0.4
Army	32392	33213	36481	12.6	9.8
Navy	26688	37542	33253	24.6	-11.4
Air Force	43281	55055	53214	22.9	-3.3

Trends in India's Defence Budget

- As per the **15th Finance Commission (XVFC), the overall *defence expenditure (including pensions)*** as a proportion of the Government expenditure varied between 15.5% to 17.8% during the period 2011-12 to 2020-21[43]. ***However, for FY 2021-22, it is only 13.73% of the Government expenditure (including pensions).***

- **Trend Growth Rate (TGR) for the period 2011-12 to 2020-21** for the **Defence Budget is 9.6%.** However, for the ***Revenue head TGR is 11%, largely due to higher outgo on salaries and pensions.*** For the **capital head TGR, is merely 6.1%[44].**

- **No Unspent Funds.** Since FY 2016-17, allotments on Capital head have been fully utilised[45], except for FY-2020-21, due disruption of deliveries attributable to the pandemic. In fact, **an additional expenditure of Rs.20776.00 Crore (US$ 2.84 billion)** had to be incurred on the Capital Head during the FY 2020-21, for operational reasons.

43 Finance Commission in Covid Times, Report for 2021-2026. Vol 1, Main Report, Oct 2020, Pg 335-336.

44 ibid

45 21st Report, Standing Committee on Defence (2020-21), 17th Lok Sabha, Demands For Grant (2021-22), 16 March 2021, https://eparlib.nic.in/bitstream/123456789/800867/1/17_Defence_21.pdf#search=null%20Departmentally%20Related%20Standing%20Committees%20[2020%20TO%202021]

- **Committed Liabilities (CL)**. *Approximately **90% of the defence capital budget in FY 2021-22 is likely to be utilised to meet CL.**[46]* As per details reported to the **Standing Committee on Defence (SCOD)** (2019-20), ***the shortfall in funds sought for meeting CL, despite being the first charge,*** were as under[47]:-

Year	Demand (For CL)Rs Cr	Allotted (For CL) Rs Cr	Shortfall Rs Cr
2016-17	73553	62619	**10993**
2017-18	91382	68965	**22417**
2018-19	110044	73883	**36161**
2019-20	113667	80959	**32709**

- **Non-Salary Revenue Expenditure.** The expenditure on **stores and capital procurements has reportedly declined from 35% in 2010-11 to 26% of the total in 2019-20,** due to rising manpower costs[48]. *Falling non-salary defence allocation will **adversely affect readiness.*** In fact, in FY ***2020-21, additional Rs 9286 Crore had to be allotted on the Revenue (Non-salary) head*** to meet operational requirements[49].

- **Aligning AAP to Outcomes.** ***Proposals in the AAP (Part A) can not exceed the allocated budget.*** As per DAP-2020, schemes under 'Make-II', 'Make-III' and 'Innovation' categories **are deemed to be automatically included**

46 Raghuvanshi Vivek. India releases details of new defense budget. Defense News.February 03, 2021. https://www.defensenews.com/global/asia-pacific/2021/02/02/india-releasesdetails-of-new-defense-budget/

47 Third Report, Standing Committee on Defence (2019-20) (17th Lok Sabha), Demand No 20, Dec 2019, https://eparlib.nic.in/bitstream/123456789/787668/1/17_Defence_3.pdf#search=null%20Departmentally%20Related%20Standing%20Committees

48 Armaan Bhatnagar, India's Defence Spending in 7 Charts, Times of India, 30 Jan 2021, https://timesofindia.indiatimes.com/india/indias-defence-spending-in-7-charts/articleshow/80600625.cms

49 21st Report, Standing Committee on Defence (2020-21), 17th Lok Sabha, Demands For Grant (2021-22), 16 March 2021, https://eparlib.nic.in/bitstream/123456789/800867/1/17_Defence_21.pdf#search=null%20Departmentally%20Related%20Standing%20Committees%20[2020%20TO%202021]

in AAP, after AoN. There are also **provisions to include emergent requirements. The outgo on CL, could vary, too,** due to delayed deliveries or exchange rate variations. **Though DAP provisions have the desired flexibility, the process inherently *defies predictability.*** Moreover, certain schemes in AAP may not even form part of the Five Year Defence Plan. Therefore, to ensure that procurement decisions stay ***aligned with NSS and priorities, the AAP, which finally drives acquisitions, should have a "before the act" oversight, rather than SCOD mechanism, which is retrospective.***

Underwriting Outcomes (ICDP/DCAP) with Outlays (Budget)

- **Budgetary Projections- Capital.** The **Ministry of Finance (MoF) has indicated an overall TGR of 10.3%** for defence expenditure **during the period 2021-26[50].** The MoD, while maintaining an overall **TGR of 10.5%, has assumed a TGR @16% on the Capital head, as against the last 10 years trend of TGR of 6.1% (XVFC),** with an **estimated allocation of Rs. 9.01 lakh crore against a projection of Rs. 17.46 lakh crore on the Capital Head for 2021-26[51].**

- **Budgetary Projections- Revenue.** However, the MoD has **lowered the corresponding Revenue TGR to 7% for the period 2021-26, as against the current trend of 11% (XVFC)[52]. *Adequacy of revenue budget*** to underwrite operations, maintenance and sustaining legacy systems ***is a critical requirement.*** While measures to reduce the outgo on salary/pensions are under serious examination, these are unlikely to have an impact in the near future. T**he Revenue TGR of merely 7% projected by the MoD to the XVFC needs to be analysed.**

50 Finance Commission, op. cit. pp 342.
51 ibid, pp 335-345
52 ibid

- **Non-Lapsable Capital Fund.** The MoD has indicated an existing shortfall **of Rs 2.47 lakh crore (Capital) for the period 2017-18 to 2020-21[53].** The ***anticipated shortfall*** on Capital head during **2021-26 is Rs 8.45 lakh Crore[54].** Based on the average shortfall on capital account for the period 2016-17 to 2020-21, ***the MoD has recommended an additional annual non-lapsable requirement of Rs 55000 Crores to the XVFC.[55]***

Fund Flows-Assumptions Vs Assurance

- With constraints imposed by a slow economic recovery post the pandemic, compounded by competing legitimate demands in health and infrastructure, it is axiomatic that ***assuring fund flows for defence over the next 5 years, though a critical necessity, is fraught with uncertainties.*** Nonetheless, a few pragmatic actions are summarised below.

- **Business as Usual- Accept the Risks. As per the Defence Minister, India plans to spend $130 billion (Over Rs. 9, 63,000 Crores)** over the **next 7 years** on defence **modernisation[56]**. This **indicates an average modernisation outlay of Rs137900 Cr per year, almost at par with BE for 2021-22 ie Rs 135060 Cr.** If this fund flow is indicative, it **falls Rs 2.1 Lakh Crore short of the MoD's anticipated Rs 9 lakh Crores over 2021-26,** and ***way below the TGR of 16% assumed by the MoD.*** The ***MoD needs to apprise the CCS/Parliament about the unmet CL, modernisation requirements, along with the associated strategic risks and mitigation measures.***

53 ibid
54 ibid
55 ibid, pp. 345
56 Press Information Bureau, GoI, "Aero-India 2021 gets off to a flying start", 3 Feb 2021, https://pib.gov.in/PressReleseDetail.aspx?PRID=1694848

- A**ssume Overall TGR Below 10.3%.** The report **"XV Finance Commission in Covid Times"** was submitted in November 2020. However, the **TGR of 10.3% for Defence expenditure indicated to the Commission may not be realised in the initial years,** and even assuming the TGR of 9.6%, as for the last decade, may not be feasible. Therefore, a **pragmatic assumption of TGR of 7-8%** be taken as a planning norm, and the CCS/Parliament be apprised of the **shortfall below the estimated/projected funds,** associated risks and mitigation measures.

- **ICDP/DCAP- Pragmatic Projections.** *The ICDP for the period 2022-2032 and DCAP (2022-27),* **may suggest a different force structure and capabilities, and hence realistic projections for modernisation, instead of the projected Rs 17.45 lac Crore for 2021-26 (XVFC).** However, it is **unlikely to have a major impact the outgo on CL for the period 2022-27, which will see realisation of delayed deliveries.** It is important that **realistic TGR be assumed for Capital and Revenue heads, and not 16% & 7% respectively,** which appear unrealistic vis-a-vis 6.1% and 11% of the last decade. **The adequacy** of fund flows with both assumptions explained above **should be assessed, and *the CCS/Parliament be apprised of the unmitigated capability gaps, unmet CL, with associated strategic risks.***

- **Assurance and Predictability with A Non-lapsable Fund.** Creation of such a fund in the interim budget in 2003, came to a naught as the Government fell. In 2016, the MoD raised the **necessity of such a fund with the SCOD.** In March 2018, the SCOD recorded that the **MoF had rejected the proposal,** citing several reasons, inter alia violation of Article 266 (1) of the Constitution[57]. Recognising the need

57 Ajai Shukla, "FinMin Shoots Down Proposal for Non-Lapsable Defence Modernisation Fund", Business Standard, 21 March 2018,

for a **long term commitment of funds to facilitate realistic planning, the XVFC** has recommended the creation of a **non-lapsable Modernisation Fund for Defence and Internal Security (MFDIS), to bridge the gap between projected budgetary requirements and allocations,** to be utilised for **modernisation of defence services, capital investment for police forces and welfare fund for soldiers and paramilitary personnel.** XVFC has **pegged the fund at Rs.2,38,354 Crore over 2021-2026, with an annual cap of Rs 51000 Crore[58].** *The Corpus, to be placed in a **Public Fund account commencing 2021-22,** is proposed to be sourced from the **CFI @**yearly 1% of revenue receipts; proceeds of monetisation of surplus defence land/ payment from State Governments for land taken already, and disinvestment proceeds of DPSEs.* **As per the clarification provided to the SCOD, the *MoF** has proposed the following mechanism[59], **which may defeat the very purpose:***

- The proceeds from **monetisation/disinvestments** be received in the CFI, of which **50% will be transferred yearly to MFDIS, after due appropriation by Parliament.**
- Funds be **utilised for Married Accommodation,** purchase of stores **under capital head** from **within India**, as ***per extant procedures.***
- Funds would be **expended only after the normal budgetary grant has been exhausted.** This could ***likely happen by Jan-March, leaving little time for complying with procedures.***

58 Finance Commission, ibid, pp 351

59 21st Report, Standing Committee on Defence (2020-21), 17th Lok Sabha, Demands For Grant (2021-22), 16 March 2021, https://eparlib.nic.in/bitstream/123456789/800867/1/17_Defence_21.pdf#search=null%20Departmentally%20Related%20Standing%20Committees%20[2020%20TO%202021], pp 11

- *In case of **non-utilisation for 3 years** from the date of crediting, the sums will be credited back to CFI.*

Nurturing the Defence Industrial Ecosystem

- **Make In India- Defence.** An inspirational target of 70% indigenous content (IC) has been pursued for decades. Though arms imports have reportedly decreased by 33 per cent between 2011–15 and 2016–20[60], India has been a leading arms importer for over decades. To curb import dependence, **procurement from the domestic industry has been enhanced from 58% to 63% (Rs 70,221 Crores) for FY 2021-22, of which, 25% is earmarked for the private sector.** In August 2020 and May 2021, two lists were promulgated, each containing 101 and 108 items respectively, **explicitly barring their import,** progressively over the period 2020-2025. ***It is a leap of faith to enhance self-reliance, with a hope that the defence forces will not have bear time, cost or performance penalties***. It also ***presumes that the yearly cash outgo on CL, over the next 5 years, will be broadly 63% indigenous.*** Analysis of details for the period 2010-11 to 2020-21 (11 Years) **indicates overall 71% indigenous capital expenditure, though for the Air Force and Navy, it is 53% and 39% non-indigenous,** respectively[61]. Based on its outstanding deliveries of systems/weapons, ***India's expenditure on foreign arms is expected to increase over the coming 5 years[62].*** Therefore, if *only* 2015-16 to 2020-21 are analysed, ***the Air Force share of non-indigenous expenditure is 69.7% and the Navy's 49.1%.*** Including schemes in the

60 International arms transfers level off after years of sharp growth; Middle Eastern arms imports grow most, says SIPRI, 15 March 2021, https://www.sipri.org/media/press-release/2021/international-arms-transfers-level-after-years-sharp-growth-middle-eastern-arms-imports-grow-most

61 21st Report, op.cit. pp 18

62 International Arms Transfers, SIPRI, 2021, op. cit.

pipeline, **the outgo could be on** Rafale fighters, M777 guns, S-400, AK-203 assault rifles, lease of the second SSBN, Kamov-226T helicopters, Mi-17 helicopters, MH-60R, MQ-9 UAVs, AWACS, AEW&C, 155mm Towed Howitzers and Light Tanks, besides expenditure on lease and on critical munitions. Commonalities with the *"Wish List" tabulated by Stephen Cohen in 2010*[63] ***underscore the glacial pace of modernisation.*** While ***ongoing efforts towards indigenisation are laudable, desirable and indeed promising,*** capital ***allocation for indigenous schemes should factor non-indigenous component of CL realistically,*** at least over the next 5 years. Moreover, *the choice of the defence systems must remain with the Armed Forces based on user preference and tactical and operational doctrines, as recommended by the Dhirendra Singh Committee*[64]*.*

- **Responsive Defence Industrial Base.** The global trend in weapon and systems is shifting away from traditional and legacy platforms towards convergent disruptive technology driven systems that enable Network Centric warfare and straddle Multi-domain operations. Defence planning, postures and doctrines of the Indian armed forces are also evolving to leverage "quality" (C4ISR, EW, precision and lethality) over quantity (numbers). However, given the looming threat of a collusive two front threat, force size trade-offs, **without due experimentation, could create new risks.** Our strategies need to be based on an **innovative mix of capacities and capabilities which include both *emerging technology driven systems as well as traditional platforms.*** The Indian *defence industry has come of age and is showing promise in both industrial age as well as the information age*

63 Stephen Coen and Sunil Dasgupta, "Arming Without Aiming: India's Military Modernisation", Brookings Institution Press, Washington, D.C. 2010, pp 21-22

64 Committee of Experts for Amendment to DPP-2013 Including formulation of policy framework, July 2015, https://www.mod.gov.in/sites/default/files/Reportddp.pdf

systems. Enhanced FDI of 74% in DAP 2020 adequately incentivises domestic production through collaboration with foreign OEMs. ***An early promulgation of the ICDP with budgetary assurance through MFDIS and revised TPCR would create the optimal civil-military fusion and synergy.*** Elaborate measures have been suggested by eminent analysts[65]. The Defence Production and Export Promotion Policy (DPEPP)-2020 has already ***cleared the decks for boosting the rising trend in defence exports.*** Recent **decisions to buy or lease systems of foreign origin only in small numbers,** whether rifles, LMGs, UAVs, helicopters or fighter jets, *is proof of the "risk" taken to safeguard future opportunities for indigenous solutions.*

Aligning Outcomes with Outgo- Suggested Pathways

Defence modernisation decisions have been historically spasmodic, driven by conflicts and crises. Nothing exemplifies the myopia better than the ***delayed raising of the Mountain Strike Corps till jolted by LAC intrusions (2013-14),*** *further* ***stretching the raising, freezing it in 2018 and finally resurrecting it in 2020, post the Eastern Ladakh stand-off***! *This must change.* ***The pandemic stricken economy must not under-write irrational defence planning.*** Faced with bourgeoning ***modernisation demands, recapitalisation of legacy equipment and voids in joint capabilities*** *like C4ISR, cyber, EW and space, we* ***need clear-eyed trade-off decisions*** *in defence planning and budgeting.* ***The challenge demands bold, innovative, risk-informed decisions, buttressed by an affordable outgo.***

- **Force Structure.** Meeting ever increasing commitments, with constrained budgets- **the cliched *"do-more-with-less" paradigm, has stretched the force.* Early promulgation**

65 Dhruva Jaishankar, "The Indigenisation of India's Defence Industry", Brookings India Impact Series 082019-01, 2019, Brookings Institution India Center; https://www.brookings.edu/wp-content/uploads/2019/08/The-Indigenisation-of-India-Defence-Industy-without-cut-mar-for-web.pdf

of NSS will ensure alignment of force ***structures with pragmatic strategies to deter our adversaries-*** *by denial or punishment (severity), objectives- territorial or counter-force; grey zone strategy & response; defence postures; sea denial or control, primary/secondary front; punitive strikes, air dominance or local superiority, information dominance/assurance etc.* ***Accepting "likely" scenarios over "worst case" ones, where the "severity of impact" is less, is also a choice.*** Structural changes in higher defence organisations to usher jointness be underwritten by ownership of all stakeholders, ***winning the "fight within".*** Learning experiences from Joint Logistic and Training endeavours would be prudent[66]. **The self-interpreted and immutable service centric "roles" need to be reviewed and promulgated with despatch, ensuring role clarity and complementarity. "Service Centric"** ***interpretation of multi-domain operations be nipped in the bud and Joint test bedding of concepts be commenced right away.*** The **cost of new structures** for space, cyber, Special Forces, Joint C4ISR, Joint Air Defence, Joint logistics and joint training, *especially equipment/software and specialised manpower* **be ascertained through cost modelling.** *Capabilities to buttress* ***maritime interests be evaluated in terms of urgency and importance, vis-à-vis proximate territorial challenges.*** Trade-off options between manned vs unmanned platforms, **aircrafts vs stand-off weapons** or **air defence systems** will potentially balance the force structure and associated costs.

- **Modernisation.** ICDP/DCAP need to be evolved innovatively and be *approved by the CCS/ Parliament, to* ***ensure commitment and political oversight*** in ***aligning the***

66 Arun Sahni, "Integrated Theatre Commands- Is It the Right Time for Proposed Restructuring?", Defstrat, Vol 15 Issue 3 Jul – Aug 2021, https://www.defstrat.com/magazine_articles/integrated-theatre-commands-is-it-the-right-time-for-proposed-restructuring/

military means and ways for meeting politically decided ends. A premium be placed on Interoperability while prioritising inter-Service and intra-Service capabilities **based on cost modelling.** Forecasting budgetary resources across multi-domain capabilities over a 10 year horizon, based on likely TGR, will enforce pragmatism and discipline. The Takshashila and DPG models discussed above be factored while evolving the ICDP. ***AAP must be subjected to CCS/Parliament oversight prospectively.*** Considering the centrality of precision, lethality and information dominance, the following capabilities areas needs to be prioritised:

- Joint C4ISR, networked sensors and quantum communications.
- Enhanced EW, Space and Cyber capabilities.
- Robust Joint tactical SDR networks with cloud storage.
- Enhancing Agility and mobility, reducing size of platforms and entities.
- Smart & intelligent munitions.
- R&D and innovation in disruptive and niche technologies.
- Interoperability of manned, unmanned and autonomous systems.
- Precise, lethal and long range fires.
- Non-lethal and non-kinetic systems for Grey-zone responses.

- **Readiness.** *Readiness reporting needs to be made institutional with quantified assessment of* the ability to mobilise, deploy, and fight within operationally viable timeframes. Training needs to ***leverage simulators and joint field exercises. Allocations*** on the ***revenue (non-salary)***

head must address the requirements. Progressively relieving defence forces from internal security tasks should be achieved in a time bound manner.

- **Sustenance.** *The number of* ***days of war reserves for equipment and munitions/missiles be assessed pragmatically,*** *considering shelf life.* **Administration, IT and logistics share commonalities across Services, where jointness can deliver** economies of scale. For logistic functions, end to end process redesign, especially for the repairs function, prevents wastage and saves manpower. Tri-Service **inventory must be standardised on priority and managed through a shared ERP** system. Efficient ***Life Cycle Support approaches like "availability contracting",*** in which the *contractor commits to deliver a specific output,* must be adopted.

- **Budgetary Process & Allocations.** ***MFCDIS Fund must be created without further delay and restrictive conditions recommended by the MoF as regards usage be waived.*** Initially, insufficient monetisation of defence land for MFCDIS be compensated and once exhausted, alternative sources be examined. *While promoting indigenisation in new schemes,* ***oversight be maintained on Capital outlay, to cover non-indigenous CL.*** **TGR of 7% for the Revenue head (2021-26) assumed by the MoD be subjected to a reality check,** lest the ***non-salary component shrinks, adversely impacting readiness.*** MoD must conform to the guidelines for the outcome based reporting, for internal audit, to begin with.

There is no easy way out of the universal CD dilemma- balancing indigenisation and modernisation, the proximate and the future threats. There are no silver bullets in defence planning and budgeting. Transforming both these multi-disciplinary processes would be demanding. ***What is important is to stay invested in driving the change from***

"the top", towards a disciplined approach to defence policy-making, set milestones and ensure accountability of stakeholders. Procrastination in ***adopting effective mitigation strategies to address concurrent scenarios and avoiding hard trade-off choices in force structures or budgetary commitments, will only make the problem harder for future planners and stakeholders.***

***Lt Gen Sunil Srivastava,** AVSM, VSM** (Retd) is the Director CENJOWS, New Delhi