Vivekananda International Foundation

Is Indian Airpower Preparing for Tomorrow's War?

Air Vice Marshal Rajesh Isser

VIF Brief - August 2019

Published in August 2019 by
Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415
E-mail: info@vifindia.org
Website: www.vifindia.org
Follow us on
Twitter | @vifindia | Facebook | /vifindia

About the Author

Air Vice Marshal Rajesh Isser is an experienced aviator of the IAF with extensive operational and combat record. He has been IAF's HADR Task Force Commander in many national and international rescue and relief ops, including Nepal, Bhutan, Bangladesh, Sri Lanka, DRC, Rwanda, Burundi and Uganda. He is currently pursuing doctoral studies on leadership challenges in disaster response.

Is Indian Airpower Preparing for Tomorrow's War?

Abstract

Technology is moving ahead in leaps and bounds, and in the years to come, it will be a prime driver of doctrinal changes in how conflicts are started, managed and won. Technologies such as big data analytics, hyper-connectivity, robust and ubiquitous sensors, internet of things, lasers, hypersonic and 3D printing allow endless scope for battle concepts such as swarming, unmanned warfare in high-risk environment, non-contact warfare from stand-off ranges and militarisation of space. Multi-Domain war fighting seeks cross-domain synergy by close synchronisation. And a true whole-of-nation approach. Most evolved armed forces are fully on board the race to develop asymmetric capabilities, such as China's A2AD. These have implications for India.

At the same time, India has to be prepared for conflict handling in the present that is characterised by increasing uncertainty and complexity. A spectrum of counter-insurgency, hybrid and compound wars need adaptive capabilities of a very high order which incorporate multi-agency synergy and fast learning curves, among others. Some pertinent questions are posed that are relevant to Indian airpower capability building.

Introduction: An Uncertain Future

This article essentially poses questions that must be asked, and which never are. Technology is moving ahead in leaps and bounds, more so after the explosive and exponential advances in Information and Communications Technology (ICT) such as Artificial Intelligence (AI). Truly, in the years to come, technology will be a prime driver of doctrinal changes in how conflicts are started, managed and won. The article does not give any definitive answers but the writing on the wall is clear. Old agendas of turf under a cloak of core competencies need to be looked at with a microscope for relevance in the coming decades. It touches on certain core sectors that impinge directly on employment of air power in the future. It takes stock of how current conflicts using multi-domain concepts are acting as test-beds, and how countries like China are bridging the divide in combat capabilities. The proper questions the premise of continuing to do the same in a dogmatic fashion.

The 4th Industrial Revolution: Technology Driving Doctrine?

Trans-disciplinary approaches in research and academia has resulted in convergence of ideas, and brought in a new creativity to science. For example, the marriage of neuroscience and engineering has revolutionised fields such as machine deep learning, human-machine collaboration and teaming, and machine-assisted human performance (exoskeletons). Similarly, a nexus of nano-technology and biology has resulted in ability to produce material with specific properties such as avoiding or causing rusting in large structures. High density energetic properties have increased the potency of explosives by ten times, with great spinoffs in rocket and missile technology. But the downsides include ability to manufacture deadly pathogens even in a garage.

While electromagnetic pulse (EMP), through a calibrated nuclear blast in the atmosphere to burn out integrated circuits and chips, has been around for some time, its employment was debateable. Currently, convergence of natural science, computer-aided design (CAD) etc. have allowed pulsed power generation that can be directed to burn out computer chips which are at the heart of any weapon system. Technologies such as big data analytics, hyper-connectivity, robust and ubiquitous sensors, internet of things, lasers, hypersonic and 3D printing allow endless scope for battle concepts such as swarming, unmanned warfare in high-risk environment, non-contact warfare from stand-off ranges and militarisation of space.[1] This requires huge investment in pure and applied research,

nurturing innovation; and creating ecosystems and a solid manufacturing base. Israel is a good example of such visionary planning. Most nations are heavily investing in AI, additive manufacturing (3D printing) and a range of human-machine partnerships. It promises to not only change the character of war but even its very nature with man out-of-the loop and action.[2] Propensity for risk-taking and effective deniability may change strategic decision-making too in the future.

The age of massed armour, fleets and aircrafts with human beings in them may be going away faster than currently thought possible. Already, surveillance and precision have revised fire and manoeuvre concepts at land, sea, air. These developments necessitate doctrinal rethink especially since it may even lead to less expenditure in capital and revenue. Prime Minister Modi in his address to commanders of all armed forces in 2015 clearly underlined transformation as a preparation for the future and not doing more of the same or preparing perspective plans based on outdated doctrines. He also highlighted the point that the services had good field commanders but now the need was for thought-leaders who can drive change in the national security system.

Leaping Technology

Considering developments in the field of science and technology related to military oriented applications, the future of warfare will be characterised by short duration, high intensity and information centric warfare, with greater emphasis on a light or medium size tactical force capable of rapidly escalating capabilities in its region of influence.[3] Some of these emerging fields are truly disruptive and capable of making existing counter-missile technologies redundant, enable stand-off and no-contact actions, hit targets difficult to hit by subsonic weapon, compress shooter-to-target window, and in effect, change many defence and offence concepts.

Additive Manufacturing

3D printing technology has tremendous potential, with new uses being demonstrated almost continuously. The US Navy printed a carbon fibre submersible as a proof of the concept.[4] With potential positive results such as cost avoidance, reduced inventories, delivery time, acquisition and sustainment programs can be truly responsive.[5] Efforts are on in many countries to actively shorten supply chains by additive and just-in-time manufacturing as part of the overall acquisition strategy. By avoiding conventional

processes that are subtractive, removing excess material and creating waste especially in the aviation sector where expensive materials are used, huge cost savings hold promise.

Another advantage is micron-thin width of successive layers that allow newer geometries, designer strengths and reliability. In conjunction with (CAD) techniques, it is capable of producing prototypes and subsequent scaling up at a faster pace and at lower costs. If spare parts can be produced locally, rather than waiting for non-stocked items to be ordered and delivered, down times can be eliminated. In addition to the ability to deliver parts without warehousing, it can actively support legacy equipment and weapon systems. Diminishing manufacturing sources and obsolescence lead to lack of spares which is a significant force degrader in extending the service life of weapon systems.

Hypersonic Technology

For at least two decades US' the Defence Advanced Research Projects Agency (DARPA) has been engaged in work on the concept of Hypersonic Cruise Vehicle that promises carry a 12,000-pound payload consisting of common aero vehicles, cruise missiles, small diameter bombs or other munitions. The Falcon Hypersonic Technology Vehicle 2 and HyperSoar are designed to fly at Mach 10 (3 kilometres per second) and carry approximately twice the payload of subsonic aircraft of the same take-off weight.[6] The Hypersonic Boost Glide Vehicle is used for extending the range of ballistic missiles. There is a DARPA-USAF Tactical Boost Glide (TBG) programme meant for developing and demonstrating technologies to enable future air-launched tactical-range hypersonic boost glide systems. The hypersonic air-breathing weapon concept is another joint programme to develop and demonstrate critical technologies of advanced air vehicle configurations capable of efficient hypersonic flight, hydrocarbon scramjet-powered propulsion, management of thermal and affordability.

Russia, China and India too are investing in this technology. China's re-designating of the PLA Rocket Force (PLARF) and elevating it to a fourth military service, alongside the PLA, PLAN, and PLAAF, indicates its intent. It has made major investments in hypersonic gliders or Hypersonic Glide Vehicles reaching speeds of Mach 10. These are ideal attack munitions which could be used against a variety of hard targets—like warships, command and control facilities, communications links, hangars, and intelligence facilities. This will be crucial to its Anti Access Area Denial (A2AD) campaign against the US. In

India, Brahmos II, a hypersonic cruise missile, is currently under development. This will have extended ranges of about 600 km and speeds of 7 Mach.

Nano-technology

In general terms, nano-technology manipulates matter at the atomic, molecular or macro-molecular levels. High speed, functionality and weight penalties demand smaller and miniaturised designs. Newer properties such as high density, conductivity, efficiency and focussed strengths are possible to be created, which affect critical components in aviation technologies. Molecular nano-technology (MNT) is one such process in which nano-robots will be used to create objects and will also be capable of assembling themselves, just like the cells in the organic world.[7]

In 2006, Chinese sources listed seven military fields for nano-technology, including potential nano-discs with a million times more storage than current computers, nano-structures, a hundred times stronger than steel, produce generic weapons, super thin radar-absorbing coatings for stealth, micro-weapons, nano-satelites, and soldier equipment including armour and laser-protected headgear.[8] Similar and varied programs are being pursued by many nations including Russia, EU and India. A convergence of 3D printing, nano-tech and other newer disciplines could revolutionise fields in aviation such as radars, communication, weapons, unmanned vehicles, and more importantly, integration of all these game-changers. Many countries have demonstrated these capabilities, and due scaling up will only optimise costs and allow operationalising.

Multi-Domain Operations

This classification is not really a revolutionary concept. Many current weapon and legacy systems possess reach, accuracy and networking to allow a multi-domain (MD) approach. Joint operation concepts and architecture are in place to enable effective synchronisation and deliver winning 'effects'. Multi-domain is actually higher in the evolutionary ladder enabled by technology that is developing and changing at paces defying the Moore's Law. More importantly, it is difficult to radically change mindsets emerging from strict hierarchical organisations to a domain-less or domain-free environment. For example, control or partial control of the air may not be dictated by only air force assets, both manned and unmanned. It may be dictated by capabilities in other domains, i.e. land, sea, cyber, information and space. This is decidedly more potent than joint operations or

'fires'. This synergistic approach, that generates much more than sum of joint capabilities, poses a number of questions and challenges:-

- With profound and fast-paced changes around the world, do we completely revamp our joint structures to cope or is tweaking enough?
- Is it possible to respect core competencies and yet demand a cultural and cognitive shift in military leaders to take up the multi-domain challenge?

Multi-Domain war fighting seeks cross-domain synergy by close synchronisation which is enabled by high degrees of situational awareness and freedom of decision across all sensors and shooters connected to the combat cloud.[9] This allows distributed effects that not only foxes an adversary but also covers up vulnerabilities in any domain. It even enables local and temporal superiority in any domain through cross-domain support.

Since networking and connectivity are the foundations of a multi-domain battle, it obviously becomes a prime target for any adversary. Data linking is underlined by a need for accuracy and addressing vulnerabilities that can lead to degradation.[10] Besides built-in redundancy against soft and hard kill effects, an important point is recognising the degree of degradation which allows reconfiguration or other measures to allow the battle-tempo to continue. With shorter OODA loops enabled by technology and AI, it is imperative that this happens equally fast. Protecting a network's reliability is possibly a more important issue than acquisition of large expensive platforms. Most networks are robust enough to avoid any single-point failure architecture; however, ingenuity of the human mind assisted by machine algorithms will continue to throw up new challenges. There will always be a need for constant human-machine interface for innovation and adaptability to counter this.

So does this combat-cloud enabled warfare remove the usual characteristics of war such as the fog of war? In fact, uncertainty and unpredictability will persist without fail – albeit in newer and quicker forms. Network-centric combat allows larger and mixed forces across the six domains to be dispersed, and allows distributed escalation, attrition, pre-emption or surprise – all aided by degrading the other side's information grid. This targeting of an adversary's grid could be for short or long-term, aimed at different levels of degradation, soft or hard kills, or outmanoeuvring the network's resilience. Therefore, battle -network analysis is more important to optimally get the right effects in the overall target analysis. This would necessarily cover deciphering of capabilities, vulnerabilities and

adaptability of the grid or cloud. It would flow out of specifics such as a network's design, robustness, main functional objectives, nodes, redundancy paths etc.

One character of war that technology has surely changed is the blurring of offence and defence in and around the battle space. This is a result of the hi-tech networking grid of shooters and sensors, deeper reach of ground based weapons, precision and accuracy. The Russians demonstrated it quite effectively by decimating two Ukrainian mechanised battalions in a matter of three minutes. It was an example of convergence of networking, lethality, reach and true multi-domain strategy. A similar effect was put in place in Syria led by Russian air power against Islamic State and Syrian rebels. Information and perception shaping formed the core of both these successes. And quite obviously, cyber and Electronic Warfare domains extended on both sides of actual combat. In Ukraine, the partnership of recce Unmanned Aerial Vehicles (UAV) with long-reach ground weapons in producing quick time response was so effective that just the sound of UAVs would make troops dive for cover. This fear effect was used to the hilt by the Russians. All this is exactly how Gen Gerasimov had conjured up the concept of a 'Hybrid War'.

Robotic Swarms

Scenarios of unmanned, autonomous, high AI-based, cheap and expendable swarms of drones to support fire or manoeuvre have been painted for a long time. With exponential leaps in AI, nanotech, cloud-networked system-of-systems, hypersonic technology and other such advances, this is quickly becoming a reality.[11] Initial forays such as US Navy's airborne LOCUST and the European ADDER ground vehicle have shown great promise that threaten to revolutionise concepts and character of war fighting. Even today, such swarms can easily overload and overwhelm air defence systems. Ground forces now can vision every soldier being a sensor with his mini and micro-UAVs feeding the common information grid or cloud. Future swarms could have individual as well as group (Observe, Orient, Decide, Act) OODA loops that beat human coping capacities. Air launched swarms increase possibilities of redefining air power in terms of risk-taking, cost-effectiveness and innovative ways to paralyse an adversary.[12] DARPA is even experimenting a recoverable systems based on a large fixed wing platform that will open up unlimited possibilities in terms of reach and response (programs such as GREMLIN, CODE and ALIAS). A critical enabler is secure communications with adequate redundancy.

Advances in quantum computation are revolutionising the field of secure data communication.

In light of a 4th Industrial Revolution and a looming 7th Military Revolution,[13] the following questions are posed:-

- Is the Indian Air Force's (IAF) insistence on 42 plus squadron strength of manned fighters relevant or does it close windows to adapt for future change in war's character or do we need to put our money into integrating multi-domain capabilities. Is this even possible without implementation of CDS and theatre commands?

- Will technology outpace doctrines and concepts based on large and expensive platforms, and are our current assessment based on flawed vision and turf bias?

- How far into the future can we plan our capability build-up in light of changing character of war and pace of technological advancements; and, is it possible to plan on some unique and niche capabilities that will be suitable to India in terms of cost, effective deterrence and future adaptability?

5TH Generation Air Warfare

The Royal Australian Air Force (RAAF) views a 'combat cloud' as essentially four grids layered and intermeshed by hi-tech networking. These are information, sense, effects and control. Superimposed over the operation theatre, this cloud offers quick and accurate situational awareness (SA), caters for redundancy and resilience, offers inter-domain complementarity, and allows a commander full-spectrum flexibility that is limited only by imagination. The concept of fusion warfare directly flows out of this grid in terms of command and control of this whole disaggregated potency. This is real centralised command, distributed control and decentralised execution.[14]

The RAAF recognises six domains, i.e. land, air, maritime, space, information (cyber and electromagnetic or EM) and human (physical and cognitive). The last three of them offer the chances of covert belligerence which allows strategic surprise of sorts. This can easily be followed by short-duration high-intensity multi-domain localised conflict. Any reacting force would have to cater for quick adaptability to this surprise and promise effective response as a deterrent. This brings us to some principal questions:-

- Is the Multi-Domain concept a force-design initiative or a force-employment model?

- Should core competencies such as plans for acquisition, manning and training remain a services domain or an integrated approach is more suitable to multi-domain?

The most suitable approach would be to allow core competencies to be developed by single service under an overarching integrated capability build-up plan that looks through a multi-domain lens from the earliest stage. Since all commanders and leaders at the strategic, operational and tactical level would have to deeply understand synergy and multi-domain concepts, it is important to incorporate these in professional training, exercises, simulations and other validation programs. It is critical for a central strategic core to ensure that multiple agencies, services and their programs are aligned. The tension of managing present issues and ensuring that these do not close future adaptations and windows of opportunity must be guided and managed. Capability building should allow strategic leaders to design and rapidly reconfigure a fit-for-purpose multi-domain task force in the shortest time. These task-forces would inevitably face four challenges: first, limited quantum of capability in each domain will demand prioritisation; second, professional mastery and delivery in each domain is taken for granted; third, robust and reliable networks all across; and fourth, encouraging bottom-up innovation that allows quick adaptability.

Defence vs Offence Spiral

Is it cheaper, in terms of overall costs and manning, to have highly effective air defence systems to deny high performance and prohibitively expensive platforms (manned aircraft)? The exponential increase in competency of detection and SSKP (single shot kill probability), and the lowering of costs will finally decide this debate. Long ranges of detection, ubiquity of a variety of sensors, high and improving SSKPs, and newer technology such as AI enabled autonomy, hypersonic flight and directed energy (DE) might just tilt the balance towards defence.

Current Al technology is highly specialised, restricted within a framework of software limited to learning, reasoning and problem-solving within a specific context. What is not currently possible is for these to adapt to new contexts or dynamically changing situations that human cognitive capacities are accustomed to. However, this is now changing at a break-neck speed despite the active debate on how much autonomy to be granted to non-humans. For example, the X-47B program of the US Navy that is working on an Unmanned Combat Aerial Vehicle (UCAV) for ship-based operations. It already is

competent for catapult take-offs, arrested landings and aerial refuelling. The ALPHA program of USAF and its research laboratories has an Al agent that has beaten all experienced combat pilots in simulated combat through fuzzy logic It holds great promise for human-machine teaming. An example is the US Army's program of teaming Apache helicopter pilots with unmanned MQ-1C towards winning in a multi-domain battle.

In the USAF's 'Loyal Wingman' program, an unmanned F-16 formatted with a manned one broke off to do some air-to-ground firing at multiple targets, modified its flight responding to mock dynamic threats, and rejoined the formation. This opens future avenues of large formations doing 'flocking' and 'swarming'. Conceptually, the risky part would be done by these unmanned components of the swarm. In another experiment, a fighter ejected a swarm of nearly a hundred autonomous micro-drones that demonstrated collective decision-making, adaptability in the air and self-healing capacity.

Al in Decision-Support

As every sensor and shooter gets networked into the 'combat cloud', the volume and velocity of data flows become impossible to be effectively handled by human decision makers. However, human ingenuity, creativity and adaptability cannot be yet replaced by anything else. But what Al can do is handle this data in terms of monitoring, triage, scoping etc. at a basic level, and have manageable information for decision makers to handle. Machines could also provide decision-support on suggested actions to be taken. Decision-support tasks would include: data-mining from all forms of inputs and fusion into a standard form; applying big-data analytics and suitable presentation; providing courses of actions and their consequences; and, provide means to validate the reliability of all these functions.

Assessing China's Capabilities

China's A2AD strategy is primarily aimed at keeping far superior US naval and joint capabilities far away from where it can be devastatingly effective. This is tailored to its eastern seaboard where all the maritime claims would inevitably cause friction and conflicts. Rarely has a medium power achieved a super-power status without conflict. China is getting ready for that, albeit planning to fight a war that it can through asymmetric approaches and not the one that the US wants it to fight.

A2AD is essentially multi-domain with an integrated mix of sensors and shooters based on land, air and maritime platforms.[15] Weaponry includes long and medium range

artillery, rocket regiments, surface-to-surface missiles, air launched munitions, a variety of anti-ship and anti-aircraft missiles, long range cruise and ballistic missiles etc. More importantly, these are all networked to align and respond quickly as per a larger strategic intent.[16] Space-based prowess and anti-satellite weapons add by improving own situational awareness while degrading the adversary's. The final picture is completed with capabilities in the cyber and information realms. Primary targets for hard-kill would be large platforms in the carrier – fleet, airborne command and control aircraft, airborne refuellers and such others that would effectively curtail full spectrum freedom in the designated zone. All this would be done along with a core effort to degrade US' superior network – centric setup.

The war in the domains of space and information (cyber and EM) would start in right earnest well before the deployment in other domains. PLA reforms implemented since 2015 show a distinct trend towards 'informationisation'.[17] In addition to theatre commands to allow multi-domain operations, China established a Strategic Support Force (SSF) under the Central Military Commission (CMC), with a mandate to directly integrate and function with theatre commands.[18] Besides joint and integrated operations with theatre commands, the mandate includes: full spectrum Intelligence, Surveillance, Reconnaissance (ISR), management of satellite operations, defence of the electro-magnetic spectrum and cyber space tasks, and providing all these services to users.[19] This architecture clearly recognises the validity of multi-domain operations. The Chinese believe that a potent mix of space, cyber and EW are key to the overall information campaign.[20] The SSF integrates these quite tightly.

China's main focus is on East China Sea and South China Sea. It is clear that Taiwan, Island claims and future geo-economic issues here would define its trajectory to usurping the USA. Indian and related Line of Actual Control (LAC) issues are a subsidiary of this content as the West would want India as countervail to China. By no stretch of imagination can it afford to redeploy most of its capabilities for an all-out war on the LAC. It would leave a crippling void for USA to exploit. As is well known and analysed by many, using Pakistan as proxy and adequate pressures on the LAC would cater for the period till its rise to top. In this analysis, the questions that are forefront are:-

- Is a 2-front war even remotely possible and is a capability build-up towards this needed in light of the huge costs?

- Should India prepare for limited but intense localised spats after assessing some of the A2AD capacities and a likely plan for attrition by multi-domain operations by the PLA to effectively neutralise Indian airpower?

A Complex Present

Preparing for Uncertainty and Complexity

All participants in modern armed conflict will attempt information warfare, cyber -attacks, irregular war, disruptive technology employment, and other unexpected initiatives before a force-on-force engagement. In the book 'Unrestricted Warfare', two PLA colonels strategise that "the new and old terrorists who consistently uphold the principle of resorting to every conceivable means are still the best teachers of each nation's government."[21] They emphasise that the heart of unrestricted warfare is breaking down the traditional ways of looking at war to a newer perspective. It means overcoming of boundaries, restrictions and even taboos that separate the military from the non-military, the weapon from the non-weapon, and combatant from non-combatant.

Yet unrestricted warfare does not mean that unlimited methods are always suitable. While the focus has been on conflicts such as Israel-Hezbollah (2006), and Crimea -Ukraine currently; closer home, Kargil (1999) was a classic hybrid mode adopted by Pakistan against India. It combined regular army troops (Northern Light Infantry) disguised as Mujahidin, occupation and holding of key locations, use of portable missiles, and even support of Pakistan Army artillery and counter-battery units. Compound wars are conceptualised and directed at a strategic level, where regular and irregular forces operating independently are coordinated towards a strategic objective - for example the Vietcong and North Vietnamese Army operations in the debacle faced by the US in the Vietnam War. The Indo-Pak War of 1965 is another example where 'Razakars' in Operation Gibraltar were coordinated with subsequent operations of the Pakistan Army. Hybrid wars differ in terms of more detailed involvement, fusion and integration at the operational level, e.g. the Israeli-Hezbollah Conflict in 2006.

Hybrid warfare is an emerging mix of tactics, techniques, and technology that combines some of insurgency's key advantages with some conventional strategies such as control and hold of territory. It combines highly decentralised Command and Control (C2), loose leadership, light footprint, and population support with tactics to hold areas and cause

attrition using man-portable anti-tank and anti-aircraft missiles, rockets, and mortars. A true hybrid campaign will encompass an entire spectrum of capability that can only be countered by a whole-of-nation approach, including nuances of combined-arms, manoeuvre and counter-insurgency. This 'gray zone' campaign, that nibbles away without a big bite that may invite all-out reactions, will surely surprise forces that are trained only in classic conflict management.

United States Air Force doctrine defines Irregular Warfare (IrW) as a violent struggle among state and non-state actors for legitimacy and influence over a population, with the non-state entity favouring asymmetric approaches. The nature and characteristics of such a conflict are significantly different from traditional war. Conventional and unconventional refer to the weapons and forces conducting operations.[22] IrW includes insurgency, counter-insurgency (COIN), terrorism, and counterterrorism, but is not limited to just these. A hybrid war is a blend of lethality of state conflict with asymmetric characteristics of irregular war, such as the Israeli-Hezbollah conflict of 2006.

The future holds conflicts that would be a battle of narratives and multiple truths, besides the 'real fighting'. By its very attributes of flexibility, adaptability and availability, airpower can play a critical role in shaping such narratives by causing effects on its own or supporting other agencies of the government. Airpower leadership has to be keenly aware of the context, understand the strengths and limitations of partner agencies, and be innovative and adaptive in the joint campaign. At the same time, they need to be aware of costs or affordability of airpower, and its vulnerability on ground and air. Optimum solutions can only follow if the bigger picture is not lost sight of.

Complexity and Adaptability

The term "wicked" for problems is reserved for complex issues that are: not fully understood till solution formulation; have a no-stopping rule or do not go away; there are no right or wrongs, as well as no given alternative solutions; and, the issue is unique and novel. The approach to such issues involves collaborative participation of all stakeholders, and plans on taming the problem and focussing on the unsolved part. An integrated approach to managing such complex problems requires coordination with objectives of acting on learned lessons and not just pre-planned targets.

Adaptability has two facets, as in the two faces of a coin: the ability to sense a change in situation demanding a change in response; and, the ability to commit to that requirement. There can be no better teacher of adaptability than biology and the subject of evolution. Mutations and selections of the fittest are lessons that can be applied when dealing with CAS or wicked problems. The Australian Army replaced the famous OODA loop with an Act, Sense, Decide, Adapt (ASDA) loop that deals better with non-linear, complex and unpredictable states. What does complexity leadership entail? The natural instinct for a managerial leader to a developing complexity is to respond with orders, directives and even more control. However, this effectively reduces diversity of thought, crowd-sourced ideas and bottoms-up innovative solutions. A leader needs to balance administration control and generative impetus for better solutions. The control part regulates the generation of adaptability and newer ideas from going into a chaotic status. The environment thus created will do both, explore and exploit emergence at lower levels.

In the ASDA cycle, action is first because in uncertainty one needs to prod to elicit a requisite response for assessments to be made. Decisions are made based on these assessments followed by deeper reflection and adaptation. An example from 1971 War is illustrative. Dacca was never an objective even in the final operational instruction by Army HQ to Eastern Command.[23] However, the famous prods by special heliborne operations (Mi -4s) ordered by Gen Sagat Singh (Indian IV Corps) caused disequilibrium and a wrong decision by Pakistani Gen Qazi to defend Sylhet by two brigades rather than defending River Meghna crossings towards Dacca. This allowed IV Corps to reach the doorsteps of Dacca almost eight days earlier than possible. Deeper reflection allowed the Indian Army to quickly go for the jugular and reach the doorsteps of Dacca. There, for some inexplicable reason, it was made to wait for II Corps to fetch up from the west and claim the honours.

Avoiding Decision Paralysis

Complexity cannot be countered by paralysis or adopting a fundamentally reactive wait-watch-adapt actions. A faulty premise is that wicked problems do not allow for ‘good enough’ approaches or preclude right or wrong solutions. Overstating complexity may muddle thinking and also delay and degrade imperative actions. Three approaches can help avoiding this state. First is prioritisation by revising key assumptions and allowing for tactical flexibility in unintended consequences. This does account for non-linear phenomena, butterfly effects, self-organising systems - all hallmarks of complexity.

Secondly, effective delegation of power and authority that encourages and enables empowered players at different levels. And finally, by understanding what empowers an adversary in terms of effect of technological advances and speed of changes.

Adopting a COIN Culture

Irregular warfare will force conventional forces to be able to respond across the spectrum of conflict and contingencies. Air warriors will have to learn to be adaptive and responsive to the demands of unconventional and irregular warfare. An aviation-combat unit must be capable of executing both the hard and soft elements of COIN in differing environments. The main focus must be on creation and training of strong capable leaders who can operate in environments of great uncertainty. Next, it must develop low cost and quick result training methodology that allows multiple iterations of basic skills common to all leaders. This is then followed by special skills such as terrain specific flying or maintaining aviation assets under combat and rugged conditions.

Multi-Agency Framework: Making it Work

Inter-Agency Trust

A shared vision and a synchronised plan of action can force relationships to develop that will allow objectives to be achieved in a whole-of-government campaign. The main four obstacles to inter-agency cooperation, collaboration and effective integration are: a lack of personal and institutional trust; absence of networks for information-sharing; stove -piped plans and strategies in silos; and, competition for resources.[24] Institutional trust is dependent on beliefs about institutional behaviour and perceptions of competency.[25] It grows when an agency is perceived to be value-based, and demonstrates integrity, credibility, reliability, openness and consistency. While elements of personal trust will always be present, it must add on to the edifice of inter-agency trust. For example, ministries of home, defence, diplomacy, and other development agencies needed to synergise plans and execution in a COIN campaign at strategic, operational and tactical levels institutionally. However, the Indian Peace Keeping Force (IPKF) experience showed a dominance of personal rapport and inconsistent networking.

Differences in doctrine, guidelines, practices and agency cultures need to be explained and discussed to avoid misunderstandings, especially between civilians and military. Education and integration can be effectively assisted by liaison cells which allow

horizontal integration. Liaison officers and staff, and overall coordinators are necessary when a situation is highly dynamic and constantly in flux. It follows that such personnel must be of quality, perhaps even more competent than those in the field. However, the opposite is the reality, where mediocre or even unmotivated people are cast in such assignments. Liaison officers need to be recognised in their core competencies by 'own and others', as well as possess high skills of negotiation, integration and understanding of other agencies capabilities. Another important issue is the levels of authority and decision-making such officers possess that in turn affects trust and confidence levels in others. Conflict resolution and de-conflicting of agendas can be effectively addressed by empowerment at delegated levels. It is also important to acknowledge that people-skills, that are mostly individualised, are critical to this communication-based endeavour.

Planning Processes

The complexity of operational planning in irregular war or less-than-war situations is further accentuated by dynamism of threats and challenges. The process per se needs to be flexible, adaptive and collaborative. The key to shared goals and understanding is effective communications. It can be disabled by silo-mentalities and bureaucratic approach.[26] The requirement is of a dynamic model where multiple procedures are performed simultaneously at different levels enabled by real-time data through a net-centric environment. Constant iterations of the OODA Loop allow cyclical collaborative exchange to cater for tempo variations. For example, in response to an emergent contingency, leaders can respond rapidly rather than schedule meetings.

Multi–Agency Decision Making

Extensive research in the USA post 9/11 World Trade Centre (WTC) disaster and Hurricane Katrina has pointed fingers at hierarchical command and control setups for major crises, and advocates a more collaboration-based emergent model for effective emergency handling. Main factors that contribute to this thread are: complexity of multiple and diverse organisation converging; uncertainty due to inadequate information and analysis; time constraints and life-and-death criticalities; physical and mental stresses on participants and affected communities; risks involved and high-stakes; and, experiences of actors in previous disaster.[27]

Collaborative Leader

While a complicated environment or problem can be dissected by domain-experts for proposing solutions, a complex one cannot be so addressed because of its inherent adaptability, uncertainty and unpredictability. Subject-matter specialists in silos may be of little help in never-ending complexities. These need creativity, an experimenting approach and fast-learning curves to be addressed adequately. In this context, the OODA Loop's decide and act steps become synonymous with experimenting or testing the waters; with repeated iterations of the loop serving as feedback and learning facilitators. In such settings, collaborative dialogue means individual inputs add to a greater amount than the mathematical sum of all – almost like a building-block of ideas. Senior leaders must, in the first instance, discern in which zone the problem lies i.e., complicated, complex or chaos. Thereafter, they must adopt an appropriate form and style of working, along with the hierarchical structure i.e., flat or conventional. A flat structure promotes creative debate, dialogue, diversity and dissent (loyal). Here a follower is as, if not more, important as the leader in terms of cognitive contributions.

The potential solution, if that is a plausible proposition, to a wicked problem facing a nation will be beyond the domain, scope and capacity of any single organisation, agency or ministry. Collaboration in an inter-ministerial endeavour will require leadership to look at multiple stakes and competition, and nurture the grouping towards shared understanding and goals. Leadership must be focused on making things happen and acting decisively with rectitude. While there will be formal leaders and authority flowing out of task-force structuring and hierarchy, considerable work gets done by champions who are passionate on the task in hand and entirely committed to larger objectives.

Multi-Domain Capabilities

The Clausewitzian theory was focused solely on physical force and attrition. But with great advances in technology and morphing of asymmetric threats, pure physical capabilities of air, land and naval forces are no longer enough to manage conflict. National comprehensive power will include elements of diplomacy, information, military, and economic, and their synergy. At the strategic, operational, and tactical levels, these elements operate on land, in the air, at sea, and through informational, cyber, and electronic means - in other words, a multi-domain endeavour. Synergised national capabilities should look to create zones of dominance to enable successful pursuit of national objectives and end-states.

A corollary is that mental and physical dislocation of an adversary capable of multi-domain operations is an imperative. Armed forces with multiple capabilities working as part of joint, inter-organisational and multi-national teams will provide national leaders multiple options across all domains needed to deter and defeat highly potent adversaries.

Airpower and Special Action

Special Forces have unique and innate adaptive ability, and are employed to respond with agility to uncertainty from unpredictable enemies. They are masters in asymmetric approaches to problem-solving. Achievement of tactical surprise, a key in such campaigns, is enabled by speed, stealth, and agility, along with superior technology. The ability to appear at an unexpected place and time of own choosing, with an offensive mindset, enables retaining initiative and surprise. This is an effective asymmetric counter to the advantages of experienced insurgents i.e., local tacit support, early warning networks and local terrain knowledge. A paradox is that the characteristics that render Special Forces an ideal choice for dispersed and geographically isolated insurgency is premised upon mobility, responsiveness, and firepower provided by air power. In a Special Forces environment of hyper-competence and sense of purpose, operations are characterised by clear mission orders and appropriate technology that allows dispersed command, control, and execution. Employment of air power must reflect complementary response structures of command and control.

Advances in technology and tactics allow acute target discrimination and weapon effectiveness of air-delivered weapons. Precision weapons can achieve unthinkable accurate and overwhelming firepower in support of light and agile Special Forces; additionally, it greatly reduces fratricide and collateral damage. Persistent ISR can provide appropriate flank protection and early warning. Mobility and effective firepower can allow even 'lighter and more lethal' Special Forces. Terrain following radar, varied flight profiles, all-weather abilities, standoff ISR for threat and detection avoidance, and offset landing zones allow stealth in a true sense. This force structure requires deeper reflection in terms of acquisition plans, training and interoperability.

Conclusion

It is clear that technology is moving ahead at a pace that was unbelievable even a few years back. More importantly, convergence of different fields such as AI, additive

manufacturing and autonomous weapons threaten to even change the nature of warfare, at least to some degree. At the same time multi-domain and hybrid warfare concepts, among others, promise to bring further synergy that cannot be countered by theories and force structures based on lessons from the last war.

The first step in looking at future threat scenarios is posing some uncomfortable but right questions. This paper has put forth nine pertinent questions flowing out of a quick look at some issues that are staring at all armed forces. While the title of the paper and thrust is on airpower in general (and the IAF in particular), these affect all agencies that contribute in a whole-of-nation approach to conflict management. The bottom-line is that an over-investment in current doctrines, concepts and platforms today may close the windows to adapt to future revolutionary changes in the coming decades. Complexity and uncertainty are a given in the future. It demands agile, curious, creative and questioning minds to gauze ahead and build adaptive capabilities. Asking difficult questions and posing disruptive thoughts is a good start to face such a future.

References:

1. Jeffrey L. Caton, Autonomous Weapons Systems: A Brief Survey of Development, operational, Legal and Ethical Issues, Letort Papers (Carlisle, PA: Strategic Studies Institute, 2015).
2. Hoffman, F.G. (2017). "Will War's Nature Change in the Seventh Military Revolution?" Parameters 47(4) Winter 2017–18. Pg 27.
3. Development, Concepts and Doctrine Command, Strategic Trends Programme: Global Strategic Trends—Out to 2045, 5th ed. (Shrivenham, UK: Ministry of Defence, 2016), 67.
4. Andrew Liptak, "Navy 3D Printed a Concept Submersible in Four Weeks," *Real Clear Defense*, July 30, 2017, available at <www.realcleardefense.comMeredith Rutland Bauer, "Weaponizing 3-D Printers: Cyber attacks Could Turn Battlefield Tech into Threats," *FifthDomain.com*, November 13, 2017, available at <www. fifthdomain.com/dod.
5. Russell, T. (2014). "Themed Competition: Additive Manufacturing for Future Military Equipment." Centre for Defence Enterprise, Army Technology, 2014. 2(4). Pg. 4. www.technologyreview.com
6. Lele, Ajay. (2017). "Hypersonic Weapons." Institute for Defence Studies and Analyses, IDSA Occasional Paper No. 46. Accessed from www.idsa.in on 27 May 2019.

7. Tomar. S. (2015). 'Nanotechnology: The Emerging Field for Future Military Applications.' Institute For Defence Studies And Analyses, IDSA Monograph Series No. 48, pg 18. https://idsa.in/system/files/jds/ (accessed on 05 Mar 2019).

8. Tomar, Sanjiv. (2015) "Nanotechnology: The Emerging Field for Future Military Applications." IDSA Monograph Series No. 48**.** Institute for Defence Studies and Analyses, New Delhi. ISBN: 978-93-82169-58-1. www.idsa.in

9. Robert O. Work, foreword to DoDArtificial Intelligence, Big Data and Cloud Taxonomy (Washington, DC: Govini, 2017), 2.

10. Nathan P. Freier (2017). "Strategic Insights: Speed Kills, Enter an Age of Unbridled Hyperconnectivity," Strategic Studies Institute http://ssi.armywarcollege.edu. Accessed on 23 May 2019.

11. Ajey Lele (2019). "Debating Lethal Autonomous Weapon Systems." Journal of Defence Studies, Vol. 13, No. 1, January-March 2019, pp. 33-49. URL https://idsa.in/jds/jds-13-1-2019-debating-lethal-autonomous-weapon

12. Layton, Peter (2016). "A New Direction for Australian Air Power: Armed Unmanned Aircraft". Chief of Air Force Occasional Papers, Paper No 5, Air Power Development Centre. www.airforce.gov.au/airpower. Accessed on 20 May 2019.

13. MacGregor Knox and Williamson Murray, eds., The Dynamics of Military Revolution, 1300–2050 (New York: Cambridge University Press, 2001), 6–7.

14. Kainikara, Sanu. (2016). "What Does Multi-Domain Integration Mean for the ADF?" Proceedings of the 2016 RAAF Air Power Conference, Multi-Domain Integration – Enabling Future Joint Success, National Convention Centre, Canberra, 15–16 March 2016. Ed Squadron Leader David Burns. Pg 40-51.

15. Bonds T.M. et al (2017). "Land-Based, Multi-Domain Anti-Access/Area Denial Forces." RAND Corporation, Santa Monica, Calif. ISBN: 978-0-8330-9746-0.

16. Cliff, R (2017). "Shaking the Heavens and Splitting the Earth: Chinese Air Force Employment Concepts in the 21st Century." RAND Corporation, Santa Monica,CalifMG-915-AF.www.rand.org/pubs/monographs'.

17. Elsa B. Kania, "Chinese Advances." "China's Artificial Intelligence Revolution," *Diplomat*, July 27, 2017.

18. Saunders, P.C. and Wuthnow,J. (2016). "China's Goldwater-Nichols? Assessing PLA's Organizational Reforms", Joint Force Quarterly (JFQ*)*, No. 82, pg. 70. www.ndupress.ndu.edu. Accessed on 15 May 2019.

19. Kevin L. Pollpeter et al. (2017). "The Creation of the PLA Strategic Support: Support Force and Its Implications for Chinese Military Space Operations."RAND Corporation, pg.7. www.rand.org. Accessed on 20 May 2019.

20. Jash,Amrita (2018). PLA's Strategic Support Force: A New Art of Modern War. Scholar Warrior, Spring 2018, CLAWS. www.claws.org. Accessed on 10 may 2019.

21. Qiao Liang & Wang Xiangsui, (PLA Colonels). (1999). Unrestricted Warfare: China's Master Plan to Destroy America. PLA Literature and Arts Publishing House.

22. John Nagl, Counterinsurgency Lessons from Malaya and Vietnam: Learning to Eat Soup with a Knife, New York: Praeger, 2002.

23. Lal,P.C. (1986). My years with the IAF. Lancer Publishers, N Delhi, pp 207-216.ISBN 81-7062-008-2.

24. Alexander,N. and Thibodeau,C. (2016). Trust and Networks in the Interagency. InterAgency Journal Vol. 7, Issue 3, Fall 2016. Arthur D. Simons Center for Interagency Cooperation, Fort Leavenworth, Kansas, USA.

25. Mussoni,S., de Vreede,G-J. & Buckles, A. (2016). The Criticality of Collaborative Planning. Joint Force Quarterly(JFQ) 80, 1st Quarter 2016. Available at <http://ndupress.ndu.edu

26. Klein,R.M. (2007). Adaptive Planning: Not Your Great-Grandfather's Schlieffen Plan. Joint Force Quarterly45 (2nd Quarter), pg 84–88. Available at <http://ndupress.ndu.edu

27. Kapucu,N. & Garayev,V.(2011). Collaborative Decision-Making in Emergency and Disaster Management. International Journal of Public Administration, 34, pp. 366-375. DOI: 10.1080/01900692.2011.561477.

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long -term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia