SYNERGY

Journal of the
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS
(Established : 2007)

Centre for Joint Warfare Studies (CENJOWS)
Kashmir House, Rajaji Marg, New Delhi 110011
Telephone Nos : 011-23792446, 23006538/9
Fax : 011-23792444
Website : http://cenjows.in
e-mail : cenjows@yahoo.com

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

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. 200/- INR or US 10$

Contents

Foreword

Higher Defence Organisation in India has been witnessing incremental reforms especially after the Kargil Review Committee Report. Organisations such as Hqs Integrated Defence Staff (IDS), Strategic Forces Command (SFC), Andaman and Nicobar Command (ANC) created in the aftermath are already functioning well. Necessity for creation of Functional Commands for Cyber, Space and Special Operations has been felt since long and already accepted in principle. Presently, it is a work in progress at different stages for each of these Commands/Agencies/ Divisions and Cyber Agency is likely to be the first to be created.

This issue of the Synergy is devoted to the theme **"Enhancement of Joint Capability through Functional Commands (Cyber, Space and Special Operations) in India".** Authors from Army, Navy, Air Force and Think Tanks have written on all possible aspects of the Functional Commands (Necessity, Organisations, and Employment etc). In all, fourteen well researched articles have been included in this issue out of which five deal with all the three types of Functional Commands, one covers Cyber and Space, four are devoted to Cyber Command and four articles deal mainly with Special Operations and related issues.

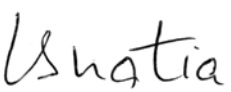
I am sure that the valuable inputs provided by the domain specialists will enlighten the readers and help in fast tracking the decision making process for creation of these vital organisations.

(AS Bhonsle)
Air Marshal
Offg CISC & Chairman CENJOWS

Director's Remarks

India boasts of the fourth largest Armed Forces in the world, the largest voluntary army, the fourth largest air force and a blue water Navy. India also faces multiple and various security threats and challenges across the full spectrum of conflict from proxy war to hybrid to non-contact, conventional and collusive wars to nuclear wars. "India has to be prepared for a two front war and build deterrence that assures conflict is not an option for its adversaries". National Security Advisor (NSA) Ajit Doval said at the Hindustan Times Summit on 23 Nov 2014, "India has two neighbours, both nuclear powers (which) share a strategic relationship and a shared adversarial view of India". It is an imperative that the Indian Armed Forces are operationally ready, optimized and prepared for all contingencies and develop the capabilities and enhance capacities to defend and protect our national interests and assets.

A risen and responsible India is also a net security provider in the region. Future security challenges dictate that the Armed Forces exploit their full potential and capabilities by formalising and refining joint structures and war fighting doctrines. To this end this issue of the SYNERGY aims to address the three joint commands of Space, Cyber and Special Operations. The articles penned by defence strategist and scholars detail the role, mission and architecture of the joint commands. There are various views and debate and deliberations are a must to ensue that the joint organizations are well structured have the requisite wherewithal, are effective and future ready, in keeping with our National Security imperatives and optimize the military potential of the Armed Forces to protect and project our national interests.



(Vinod Bhatia)
Lt Gen (Retd)
Director

Joint Commands under a Chief of Defence Staff: Better Late Than Never

Lt Gen Balraj Nagal, PVSM, AVSM, SM (Retd)*

The nature and direction of war and the geo-political environment for military operations has changed dramatically in the past seven decades ever since India became an independent nation state. During this period, organisations, namely the Defence Ministry, Army, Navy and Air Force have remained more or less the same, as was in 1947. Is the organisation based on strategic considerations, or can it be assumed that the political and military leadership continued to visualise future wars and conduct of operations? Has inertia prevented change for progress to adapt to the changing conflict environment? Today, the spectrum of war that the Defence Organisations and Indian Armed Forces need to address ranges from terrorism to nuclear war, cyber to climate change, internal security challenges to human assistance and disaster relief, compared to the limited, conventional, conflicts of the past. The last combined effort of 1971 war resulting in the liberation of Bangladesh saw synergy where India did achieve commendable results, but it was not a joint command campaign under a single joint commander.

Most developed countries have changed their organisations to adopt modern practices and approaches in organisational structures in order to meet contemporary challenges posed by conflict and war. If change has been accepted elsewhere, we need to examine some important aspects, which led to those changes. Firstly, the new challenges to be addressed had to be carried out in a foreseeable time frame; secondly; the requirements of the respective political leadership for precise, timely and well-analysed inputs, advice, and available policy options for security and defence of the nation, and thirdly; existing systems have proven inadequate to fulfill the needs of emerging and future challenges.

With the expansion of the conflict spectrum from terrorism to nuclear war, and simultaneous increase in the modes to wage violence against the state by non-state actors, proxies and irregular forces the responses that India needs to develop have become complex and complicated, thus requiring specific calibration. In an environment of ambiguity, uncertainty and frequent opacity, the political leadership need to be provided with comprehensive, complete and evaluated options for policy formulation, doctrines and strategy based on broad, full-ranging, and all-inclusive analyses. The advice and inputs are generically called “single point advice.”[1] The policy, doctrinal issues and strategy options will need multiple inputs from political,

military, diplomatic and intelligence agencies besides integral military capabilities.[2] Defence finance management is a critical aspect in modern times, with competing demands from social and development sectors. With shrinking defence budgets, the need for judicious and realistic allocation can best be done by centralised coordination amongst all stakeholders.[3]

The above beliefs and opinions will demand certain actions and structures by the Armed Forces for realisation. The first subject will be pertaining to policy and planning for conduct of war. Future wars may, or may not be fully conventional, hence, planning will have to cater for counter-terror operations, counter-insurgency operations, limited- to full-scale wars, with the possibility of escalation to the stage of a nuclear war. Peace has eluded many parts of India where sub-conventional conflicts have been conducted in the past, and anti-terrorism operations continue till date. Therefore, the joint plan needs a centralised approach and, this can best be prepared by a joint organisation. The Cabinet Committee on Security (CCS) should be presented with options and plans which provide a range of choices to the Prime Minister. In the absence of a joint organisation, the pulls and pressures of individual armed forces, as well as the lack of knowledge and understanding of other related requirements, will surely result in not providing the finest inputs, that would definitely have an impact on the ensuing decision The decision-makers must be provided with policy, doctrines and strategy options based on political directions issued. This task can be done optimally by a body with elements from all forces required to complete the plan. Important subjects which require joint action are policy formulation, planning, coordination and execution in the fields of strategy, capability, operations, readiness, finance, organisation structures, manpower, intelligence and training.

To provide these inputs a dedicated and tailor made organisation is essential. The range and depth of inputs calls for a multiservice approach, besides, domain inputs require experts from other ministries to provide advice and recommendations. In other countries, Joint HQs from all armed forces have been formed to integrate and incorporate the resources to provide jointness necessary for the current environment. Such a body can be created by forming a joint headquarters with staffing from Army, Navy, Air Force and Coast Guard (if required), with the requisite authority to decide and execute plans. The subjects to be addressed by the highest HQ should preferably be exclusive from subordinate HQs, or if concurrent, the level needs to be higher than the charter and responsibility of the armed forces HQs and Commands. Drawing from the above discussion, the case for a prime body for Command and Control should be established – namely the Chief of Defence Staff (CDS), as proposed by the Kargil Review Committee[4] not in the form suggested, but with enhanced powers. The enhanced powers, for functional needs, should not mean reducing the powers of the Services Chiefs of the three armed forces.

The peace and war spectrum will operate in and exploit domains including space, airspace, land, sea and hinterland simultaneously, characterised by deception, confusion, misperception, simultaneity, range, depth, speed, information, firepower, autonomous systems and multiple forms. The challenges centred on situational awareness, prioritization, coordination, strategic targeting and addressing multiple centres of gravity simultaneously.[5] The basic requirements that being of intelligence, surveillance, monitoring, reconnaissance, command and control, coordination, force projection, depth operations and breaking cohesion and will of the adversary. The Revolution in Military Affairs has fielded new weapon systems and operationalised C4ISR systems, which have increased situational awareness, literally making the war environment transparent, but, at the same time, introducing a sense of doubt because of deception, deliberate false feed, friction of war, and ambiguity of intention by design. Protection of C4ISR systems will remain critical for prosecution of actions and conduct of operations.

The universal requirement of intelligence, information and situational awareness in all domains and fields places an enormous burden on the leadership to create appropriate, and suitable structures to collect, collate, synthesise and analyse intelligence. To achieve this, strategic, operational and tactical intelligence-collection organisations must form part of the structures that are created to support the highest HQs. In intelligence analyses, duplication or overlapping of effort may be inevitable at times, but must be with a specific purpose. This condition must prevail where the service HQ needs tactical and operational intelligence. The means of gathering intelligence from human to technical needs highly trained and tech-savvy force, nurtured over decades to remain abreast of events and means. This generally is feasible in tailor-made organisations supported by requisite funding.[6]

The challenge to intelligence challenge has been further aggravated by introduction of the cyber realm[7] , in which, the offensive and defensive needs of the Armed Forces will require a dedicated sub-effort to remain dominant in cyber space. The contours of cyber space will continue to evolve with time, hence, the organisation created to deal with the cyber domain should be dynamic, not only to defeat cyber-attacks, but also conduct offensive operations to prevent and pre-empt threats and challenges. Any offensive cyber policy must have centralised direction and control, whilst execution can be decentralised. The policy and strategy aspects must remain with the highest decision-makers. The scale, size and extent of both aspects discussed demand a highly specialised and technically-proficient organisation at the apex level. To perform this role, the Armed Forces should create an Intelligence and Cyber Command that will be functional under the CDS.

With the militarization of space beginning decades ago, the realm of space has become the fourth dimension of war in a revolutionary way[8] , whilst it has not

yet been weaponised. The revolution in space has created capabilities at land, sea, air and space in the fields of surveillance, monitoring, tracking, protection, interception, communication, targeting, damage assessment, guidance, movement and electronic intelligence (ELINT). These capabilities are required for situational awareness, intelligence collection, remote targeting, operations control, offensive actions in space if necessitated by the adversary's action, operational planning and execution of plans, seamless communication in all types of terrain and maritime control. The means in space now include geo-synchronous communication satellites, military satellites for various purposes at different altitudes, hypersonic missiles and space weapon delivery platforms based on reusable technology.

Doctrines and strategies of space are in the evolutionary stage, given that knowledge from developed nations remains in the confidential sphere, hence, there is a need for creating core specialists in the space doctrine, policy, programmes and technologies. The doctrines and policies should identify a long-term integrated roadmap for developing space-based capabilities as well as capacities that would ideally support their operational doctrines and increase their effectiveness. Specialists in the field are developed in years and technology revolution being constant, demands that they continue to function in the same domain. Hence the organisation to man the systems must be super-specialists in doctrine, strategy and policies, in the fields of imagery, communications, target assessment and damage evaluation, electronic monitoring and all other aspects, which forms part of the space-based systems. The fields are common to the Army, Navy and Air Force, and in so far as the overlaps in requirements go, hence, the organization lends itself to jointness.

The advent of anti-satellite missiles and space vehicles has added a new dimension to the offensive and defensive capabilities; therefore, protection and attack requirements of the military assets have become inherent and incumbent. Development and demonstration of the anti-satellite weapons (ASAT) capability has become an international necessity because of the lessons drawn from the Non-Proliferation regime, where then nuclear powers denied nuclear capability to other nations by bringing in the NPT Treaty. A similar treatment might just be applied to the ASAT technologies of the future. Another argument rests on deterrence – that the ASAT capability must be demonstrated to deter other nations from undertaking an/any offensive action in space. Situational awareness capability in space is required to protect own assets as also for space control.

The real time necessity to launch space-based systems be it nano-satellites, micro- or mini satellites, reusable space vehicles will require an organisation for planning and implementation of designing, fabrication, production and launch on demand. Creation, operational deployment and sustenance of space assets calls for sophisticated high-end technology and expertise. Space users must

possess advanced knowledge, comprehensive understanding of space assets as well as the capabilities that these provide, which, would include operational planning, execution and assessment. The specifics include types of payload, multiple technologies, numbers of each type, commonality and the mandatory redundancies. Signals Intelligence and multispectral and hyper-spectral imaging assets, modular spacecraft structures, Launch on Demand and Mobile Launch capabilities for micro- or nano-satellites with specific payloads into orbit, building infrastructure and training of personnel, build secure ground stations and data links are critical issues to be addressed by any organisation created to shepherd the space effort. The technology and eco-system for the basic essentials will have to be worked on by the same organisation, needing armed forces personnel and technical experts from the DRDO, besides consultants from the industry. There is a need to create a pool of manpower that is capable of using space-based tools equipped with war-fighting functions. This requirement calls for a tiered approach to provide appropriate institutions at the apex, middle- and lower levels of the environment including specialised manpower. What needs to be highlighted is that all this can happen in the military sphere, and not in the civil programme.

The discussions on space leads us to conclude that a joint force HQ would be an essential pre-requisite, and that its charter besides issues stated above should include interface with various agencies for procurement, coordination with R&D agencies such as the ISRO and DRDO and also with the operational agencies such as the NTRO with an aim to look at the requirements of space holistically. The organisation would control and coordinate defence assets including dedicated launch services for military satellites, for which appropriate infrastructure should be developed.

Building the military space capability and implementation of space security policy can be achieved through the establishment of a Joint Space Command that would function with active support from other stakeholders such as the ISRO, DRDO and NTRO etc. Setting up of the space command should not be prejudicial to the responsibilities of each Service towards their current or futuristic concept of operations and service specific space requirements which need to be built and integrated towards each user's effectiveness or its force enhancements. Harmonising national space capability to further military and commercial interests needs to become critical element of current national strategy. A more inclusive institutional structure that would have much more coherent approach towards how to maximise options in the area of military and space security policy. Manned by personnel of the three Services along with domain experts and scientists, it would also enable the Armed Forces to play a more proactive role in ensuring security of the domain. The Armed Forces are the right agencies to shoulder the responsibility of space-based applications that would support both offensive and defensive operations. The Joint Space Command should be the central point of responsibility

and authority in planning and coordination of national assets in ensuring national security.

Special Forces have been used innovatively and successfully in the past and the scope increased exponentially during the period of the Cold War, wherein specialised tasks were given to these elite units ranging from reconnaissance to eliminating nuclear units. The growth of sub-conventional conflict has introduced a new dimension in the use of Special Forces, where insurgency support, counter-terror and many other tasks have become intrinsic to their employment. The employment of Special Forces now extends to the imagination of the strategic planners and handlers in operations. The fundamental principle in employment of Special Forces is that the political decision-maker determines the aims and purpose of the Special Forces, which are based on deep insights into future scenarios, anticipated conflict areas, defence of national interests and timing of the action. Special Forces can be used to achieve political and military objectives by addressing high-value targets, psychological operations, and civil affairs operations in under-developed areas. Special Forces personnel possess unique and unusual skills, are unorthodox and low-cost and potentially high payoff. Special Forces often use covert or clandestine methods that national, sub-national or theatre leaders use independently in peace time or to support warfare across the entire spectrum of war.[9]

The Special Forces are a low-cost option to attack the psyche of the public, political leaders and military leadership with missions of interdiction and destruction, off shore facility damage, psychological operations, special intelligence, escape and assassinations to name a few. Special Forces aid in peace by conducting insurgency support operations, training of counter-insurgency forces, counter-terror operations by targeting origins and supporters, sabotage, subversion, deception, intelligence-gathering, reconnaissance, rescue, or raid/commando attacks to safeguard citizens abroad. During war, the missions may include strategic target destruction including nuclear assets, reconnaissance and surveillance, disruption, elimination of command and control systems, unconventional warfare, psychological and civic actions, power grid failures, contamination of utilities, target designation and maritime targets of many types.[10] The scope, range and nature of missions dictates, that these be planned and controlled at the highest level, to determine the strategic effect and provide appropriate resources. The Special Forces by nature work deep in enemy territory, isolated and under bare subsistence or local resources. Special Forces missions will be on land and sea, whilst they can use land, sea or air for insertion, movement and operation. This necessitates that these are all forces organisation. This scope of employment and method of operation make them of value to the Army, Navy and Air Force so as to enhance the operational reach and improve capability.

Being high risk in nature and generally conducted in hostile territory, Special Forces employment involves centralised planning at the highest level with centralised command and control. However, execution and operational control will be decentralised. Special Forces operations' objectives being at national and strategic level planning must be dynamic and continuous. This is most essential to calibrate the operations, and it is best achieved by control at the highest level. Any high level control must have access to the national political leadership for decisions, changes or amendments. The operation to capture or kill Osama Bin Laden remains a case in point of centralised control of Special Forces operations.

The Special Forces operations beside central planning and control are also characterised by secrecy and fool proof security at all stages including post-successful completion. Hence the need for limited sharing of information, the longer the chain of command, the greater the diffusion of information, therefore, it must remain limited to a select few at the highest level. All Special Forces operations require detailed and real time intelligence and these requirements need a short chain of command for secrecy and speed. Most clandestine and secret operations are performed by an all Forces combine during insertion, conduct and exfiltration, even in training and insurgency support missions, continuous supply of arms, ammunition, equipment and manpower.

The concept of jointness has taken a backseat in India for the past few decades, not by design, but due to lack of political will to modernize India's defence organization, and the armed forces' reluctance to adapt to the future needs of contemporary warfare. In short, it can be summarised that the armed forces saw everything through the prism of their own respective force and, not in the national interest, and did not evolve strategic thought based on modern concepts, strategic environmental requirements and technological advances. The time is opportune to redress the past faults to create a Chief of Defence Staff to cater for a single HQ for centralised policy and doctrinal formulation, joint evaluation of financial needs of the armed forces, coordinated operational planning and control of the joint command of Space, Intelligence and Cyber, and Special Forces. The synergy expected from the new structures will enhance capability, economise expenditure and provide the political leadership harmonised, tri- service evaluated and objective advice.

*Lt Gen Balraj Nagal (Retd) is a former C-in-C of the SFC and Director CLAWS (New Delhi)

[1]For related details see the Summer 2013 edition of the *CLAWS Journal,* based on the specific theme focussing on building capacities given the unremitting continuity in the patterns of threats and power equations in the region, which make long-term defence planning an indispensable prerequisite; and for related reading see, *Journal of Defence Studies,* vol. 1, no. 1, August 2007, based on the theme of Jointmanship.

[2]Vinod Anand, "Integrating the Indian Military: Retrospect and Prospect," *Journal of Defence Studies,* vol. 2, no. 2, Winter 2008.

[3]For more details see, *Report of the Comptroller and Auditor General of India,* for the year ended March 2014, Union Government (Defence Services) Army, Ordnance Factories and Defence Public Sector Undertakings, Report No. 44, published 2015.

[4]*Kargil Review Committee Report,* Government of India, established July 29, 1999.

[5]For details see, Robert Bebber, "A Cyber-Information Operations Offset Strategy for Countering the Surge of Chinese Power," Center for International Maritime Security (CIMSEC), April 20, 2016, available at http://cimsec.org/cyberspace-information-operations-strategy-countering-surge-chinese-power/24383

[6]Cited based on a discussion organised by the Centre for Land Warfare Studies (CLAWS), *C4I2SR in the Indian Context: Challenges and Responses,* September 26, 2008.

[7]See paper on *"Cyber Intelligence," Georgetown Journal of International Affairs,* March 17, 2015.

[8]For details see, Ajay Singh, "The Revolution in Military Affairs: 4-Dimensional Warfare," *Institute for Defence Studies and Analyses;* and related in-depth study see, Nordin Yusof, "Space warfare: High-tech war of the future generation, (Malaysia: Penerbit Universiti Teknologi, 1999).

[9]As quoted in, Walter N. Lang, *The World's Elite Forces,* (Guild Publishers, 1987).

[10]For details see, *Critical Infrastructure Threats and Terrorism,* Handbook no. 1.02, Deputy Chief of Staff for Intelligence, US Army Training and Doctrine Command, Fort Leavenworth, Kansas, August 2006.

The Politics of Military Transformation and the Three C's

Brig Rahul Bhonsle, SM (Retd)*

Conceptual Underpinnings

This Paper attempts to address the creation of the three functional commands – Cyber, Space and Special Forces through the perspective of the politics underlying military transformation. Towards this end two frameworks are used – a historical analysis of successful military transformation in India and abroad and the politics of institutional decision making in India that has contributed to military change. Historiography will cover the changes that have been undertaken by the military so far with spotlight on the Indian and some relevant examples of foreign forces. The unique environment of the Indian military with threats, challenges and organisations are obviously not found elsewhere. More over the sheer size of the organisation implies comparisons can be carried out with only three forces in the World – the American, the Chinese and the Russians. The focus is more on drawing lessons from positive transformation and identifies the triggers as well as processes for these changes.

In the larger perspective any transformation is a political process. The armed forces are one of the multiple institutions of the State in the triumvirate of the executive, legislature and the judiciary. While being the teeth arm of the executive the role, size and unique identity occupied by the military necessitates examination of multi institutional politics in terms of distribution of power in this network or maze. The Weberian bureaucracy designed to achieve maximum efficiency in complex organisations is also resistant to change unless forced upon by internal circumstances – such as collapse or extinction of an organisational silo and not or external stimuli. When applied to the Indian military governance this truism is evident with the persistence with organisations as military farms which are continuing despite being functionally redundant due to lack of an external push.

An examination of these factors should lead to the possible trajectory of creation of what are essential mechanisms for command and control, synergy and economic utilisation of resources the Cyber, Space and Special Forces Command. A debate

on necessity of these has been conducted extensively and in principle these are accepted. The enigma is that despite acceptance the necessary momentum for reaching a final conclusion is lacking, thus working towards the same assumes greater importance.

Successful Military Transformation – A Historical Perspective

There are many instances of successful military transformations in India and abroad which can be drawn from post independence history. While most change which is long lasting is evolutionary in nature, the inflexion point for the so called revolution in military affairs are mainly threefold. The first are lessons drawn from a recent conflict – ironically defeat induces greater impetus for change than victory. The foremost example remains that of the United States post war in Vietnam. The initial setbacks in the Kargil conflict also set the stage for the most sweeping recommendations for reforms in the Indian armed forces. A survey of implementation of these has indicated that while many have been implemented some of the most important such as Chief of Defence Staff remain still born. Other successful transformation of the Indian armed forces mainly the Army are mechanisation undertaken in the 1980's which was derived from lessons of the 1965 and 1971 Wars and the Krishna Rao Committee. The initial failure experienced by India in Sri Lanka in the 1980's led to a review of the country insurgency doctrine, organisation and practice is another instance closer home. This was the matrix which contributed to the success in Punjab in the 1990's and Jammu and Kashmir.

Right lessons can also be drawn from wars fought by other armed forces. The British and the French militaries forces shifted to a joint and interoperable paradigm after the Gulf War 1991 when they found themselves operationally incapable of the joint juggernaut created by the US Armed Forces. The reforms undertaken by the Chinese People's Liberation Army (PLA) are said to be based on the lessons drawn from the Gulf War 1991. There are some reports that the Vietnam campaign in 1979 was launched by Deng Hsiao Ping with the aim of bringing about a realisation in the PLA of inadequacies. If true this could be one of the most unique if somewhat out of the ordinary examples of enforcing transformation.

In the security sphere the counter terrorism establishment in the country was created after the 26/11 Mumbai attacks. These reforms led by then Home Minister Mr P Chidambaram had bipartisan support with the opposition too pitching in to agree to the formation of National Investigation Agency (NIA). However a few years later when Mr Chidambaram proposed the National Counter Terrorism Centre there was huge resistance by the opposition for by then the memories of 26/11 had faded which underlines the point that reforms have to be taken to use a colloquial phrase, "when the iron is hot." As public memories fade, the leadership will also lose the incentive for change.

Should we then wait for a cyber attack crippling our infrastructure to lead to acceptance of the need for a Cyber Command, one would dread to contemplate such a possibility.

In the context of the three Cs lessons from contemporary wars waged in the 21st Century are relevant. In terms of major campaigns United States Operation Enduring Freedom and Iraq Freedom are germane. There is possibly a body of work done by various institutions in India in which the benefits of cyber, space and Special Forces synergy where occurring has to be dusted off and presented to the larger audience to create acceptance as well as a felt need for replicating these in the Indian military.

More relevant lessons can be drawn from employment of Special Forces in the context of countering terrorism and insurgency be it in Afghanistan, Iraq or Syria. The Afghanistan National Defence and Security Forces (ANDSF) provide a salient example of the successful employment of Special Forces as a single cohesive force. Numbering around 10,000 this is the premier counter insurgency force which has demonstrated success such as speedy relief of Kunduz city from the Taliban in September-October 2015. Indian personnel deployed in Afghanistan have been beneficiaries of efficiency of the Afghan Special Forces whose record of neutralising a hostile attack is worth emulating. While it may be argued that Afghanistan does not have a navy or an air force special unit thus a single command is feasible yet here the argument is the efficiency and effectiveness of the organisation which creates peer pressure to perform apart from other benefits such as commonality of training and equipment.

The second intervention leading to military change has been initiative by political leadership. In the Indian context the relative success of reforms post Kargil could be attributed to the political push to reforms apart from the historical factor covered in the previous portion of deliberations. The Kargil Committee report was followed by the Group of Minister's which outlined the trajectory of reforms to be undertaken. After the Naresh Chandra Task Force (NCTF) no Group of Ministers was appointed to undertake holistic appraisal of the recommendations and provide a trajectory for their implementation. There were other reasons as well as from the political point of view the NCTF recommendations came when the Congress led United Progressive Alliance (UPA) government was to borrow an American term used for President's a lame duck one, thus political push was difficult. More over once the Bharatiya Janata Party (BJP) led government came to power apart from the delay in settling down there was some scepticism in accepting the NCTF report's recommendations given that this would have led to acknowledgement of reforms by the predecessor regime which also underlines the central theme of politics of reforms.

A successful intervention of political guidance in bringing about very effective and fruitful reforms is that of jointness in the American Armed Forces. Today the US military is the most integrated force in the World perhaps of all times. This change has come about not because of the military but was forced down upon the military by the Goldwater Nichols Act of 1986. This Act was promulgated despite serious reservations and has brought about the single most important organisational change in militaries in recent time commencing what is now known as the, "age of jointness." In order to overcome the resistance to such a move, Goldwater and Nichols used the age old tactics of asking for extremely radical changes while aiming for those that were finally approved.

The transformation of the Chinese People's Liberation Army undertaken by President Xi Jinping who is also the chair of the Central Military Commission (CMC) is another example of change initiated by the political leadership. The process which has commenced on 1 February 2016 was undertaken after extensive debate within the military and political community. Perhaps President Xi did not face as much resistance as in the United States but the process was far from smooth for it has downgraded the role of the PLA Army, emphasised jointness and placed the Central Military Commission in complete control of the military with direct command over the five operational theatres. This is expected to be completed by 2020 and the outcome is eagerly awaited.

Visionary military leadership has also succeeded in instituting change by building a constituency in political leadership and the civilian staff of the Ministry of Defence for the same. The example of General K Sundarji envisioning and raising mechanised infantry could be sited. Against resistance from within the infantry in particular Sundarji succeeded in creating a mechanised corps leading to singular tactical advantages accruing from combat teams, groups and commands, which revolutionised warfare in the plains and the desert sector. Sundarji was also one of the early architects of India's nuclear doctrine though he could not see the same reach fructification.

The evolution of the air land battle doctrine by the American armed forces is another example of successful transformation by the military leadership. The forward looking concept combining fire power and manoeuvre of forces on land, air and sea revolutionised conventional warfare and is attributed as the single most important factor determining American success in the Gulf War 1991 and the War in Iraq 2003. This is the precursor to network centric or networked enabled warfare of today derived once again by the military.

In the context of contribution to the creation of the three commands – cyber, space and Special Forces, the 3 Cs, these historical examples highlight an important pointer. Unless undertaken in the wake of a military defeat in war, the process of transformation is a slow one whether the same is led by the political or the military

leadership. The course is non linear with multiple layers of resistance which will have to be overcome, many barriers will be within the services and will prevail despite the logic of the proposal. First and foremost thus is creating a constituency of awareness of benefits amongst the decision makers and more particularly the political hierarchy. The debate today is too insular – there is a need for engaging a much larger and wider audience including the political leadership, civilian bureaucracy, Indian Space Research Organisation (ISRO), defence research and development Organisation (DRDO), the academia, media and so on to create a constituency for change. Such a campaign should commence with all the three service chiefs on board. This will require energy and determination to drive reforms in an institutionalised manner. Finally the maze of institutional politics in higher governance in India will have to be overcome which is being discussed in the next part of the paper.

Traversing the Maze of Institutional Politics for Change in India

The approval for the establishment of the 3Cs will be given by the Cabinet Committee on Security (CCS) headed by the prime minister with the defence, finance, home and external affairs ministers as members. Decision making in the CCS is normally by consensus thus the proposal will be thoroughly examined by the ministries concerned amongst others. The final approval will come on a file which will have to be prepared in a comprehensive manner analysing all aspects of the proposal. Frequently such a scheme will have to be discussed informally to obtain the approval of the ministers and the secretaries for which formal and informal contact will have to be established.

Assuming that the Ministry of Defence is on board the Ministry of Finance will have to give the go ahead while other ministries such as Ministry of Communications and IT will also have a say along with the Department of Space. Creation of the 3 Cs at least Space and Cyber will encroach upon the domains of the latter two, while the Ministry of Home will be concerned over jurisdiction of the National Security Guards, Thus there is likely to be resistance on various grounds which have to be pre-determined and concerns addressed by underlining the significant contribution that the commands would provide to the national cyber and communications infrastructure or terrorist and other threats. Once again politics may spurn logic.

Given that government decision making is by consensus the first issue is for the military to accept this constant which is quite different from what the armed forces with their hierarchical decision making are used to. Top down decision making is no doubt necessary for war fighting however the culture frequently seeps down to normal military functioning thus the art of building consensus by seeking cooperation, cajoling or even coercion is somewhat strange to military leadership. Frequently an adversarial position is taken vis a vis the civil bureaucracy, which is like the staff of a general or an admiral processing decision making. Just as in

some military HQs the staff seems to be all powerful, the ministerial staff assumes such a halo preventing establishment of the required degree of rapport by the military leadership.

The administrative services in India have build expertise in government decision making. The military is frequently alien to functioning of government based on Rules of Business published by the Cabinet Secretariat. Where officers are exposed to the decision making in higher echelons of government success in getting the files through is better, than those who come straight from the field. Thus for this purpose creation of a team that can process the maze of bureaucracy within the Ministry of Defence as well as other ministries assumes importance. Obviously HQ Integrated Defence Staff despite the truncated staff is well suited to pursue the case of 3 Cs but has to be supported by the Service HQs.

The model for sponsoring of recommendations to the Pay Commission could be adopted where for obvious reasons there has been a joint approach with services acting in tandem and presentations made by an apex team. A high level team of officers headed by a three star general or equivalent should be constituted with a time bound programme to achieve the desired objective of 3 Cs. This team should have three sub teams one each for Cyber, Space and Special Forces. While senior officers should interact at the appropriate level, director level officers are also important to “push the files in the decision loop of ministries that starts with the section officer at the bottom ending to the secretary at the top and return in the same manner. It is a well established fact that no file gathers momentum on its own and needs an appropriate push.

The campaign plan will have to include selling points of the proposal and the likely resistance. Most of the resistance will come from two factors –fear of the commands space, cyber and Special Forces ability to disrupt normal governance in other words mini coups. Let us begin by hypothetically accepting that these fears are not misplaced and have some grounds. To believe that military loyalty in any country including India is completely subordinate to the civil hierarchy may be not be true as at times individual and institutional interests dominate. These fears are accentuated mainly by the large power at the hands of single service commanders.

In the case of the 3 Cs these commands will report to the Chairman Chiefs of Staff Committee (COSC) or the Permanent incumbent/ Chief of Defence Staff when approved. There is likely to be resistance towards this proposal particularly from the Army in the case of the Special Forces Command. As the Army will be fielding maximum numbers as well as necessity for continued deployment of these in a counter militancy role, the concern is genuine and will have to be suitably addressed.

Economy of Resources - Selling Point and Challenges

Operational efficiency through economy of resources will have to be the unique selling point of the proposal for creation of the 3Cs. In the case of the Special Forces Command duplication has to be avoided by allocating resources in direct support to services that require these for operational deployment. In the case of the other 2Cs there would be an obvious duplication as services cannot necessarily do away with their cyber or space cells completely. As far as there is no accretion of overall manpower there is likely to be less resistance to the proposal. Creation of additional flag ranks may be another dampener. A holistic appraisal of the number of flag ranks should be carried out by the three services and rationalisation undertaken within the current authorisation in the larger interest of reducing the weight at the top which may be overburdening the organisational structure at present.

Conclusion - Communication Strategy

While an attempt has been made to outline how the 3Cs can be reached, to achieve the objectives set out there is a need for a comprehensive communication strategy to raise awareness of the requirement by targeting the stake holders, policy and decision makers in a manner as to ensure their acceptance of the proposal. Each stake holder will have to be addressed by using the message and the medium which is best suited to attain the core objective – getting 3Cs on the ground within an overarching framework.

---

*Brig Rahul K Bhonsle, (Retd) is Director Security Risks Asia a South Asia Risk and Knowledge management company.

Defence Reforms: CDS and Theatre Commands are an Operational Necessity

Brig Gurmeet Kanwal (Retd)*

Those who do not learn from history are condemned to repeat it.
George Santayana

Higher Defence Management: Time for Change

Defence Minister Manohar Parrikar said recently that he will soon be recommending the creation of the post of Chief of Defence Staff (CDS), which he considers "a must", and that the final decision will be taken by the Cabinet Committee on Security (CCS). He also said that the Ministry of Defence (Mod) is engaged in working out a mechanism for the post.

Critics have argued that such a post will be out of tune with India's strategic culture. George Tanham of RAND Corporation had written that India does not have a strategic culture. While that is not true, India's defence planners have been neglecting to learn the lessons of military history. In 1962, the Indian Air Force (IAF) was not given any role to play in China's India war when it could have wreaked havoc on the Chinese hordes that had concentrated on the Tibetan Plateau without air cover. In 1965, the Indian Navy (IN) was not even informed about the plans to launch a three-pronged attack across the international boundary (IB) into Pakistan.

It is repeated quite often that the 1971 war was a well-coordinated tri-Service effort that led to a grand victory. The rather limited coordination that was actually achieved during the wars with Pakistan in 1965 and 1971 was mainly due to the personalities of the Chiefs in position of authority and not due to any institutionalised arrangements. For example, during the 1971 war, Field Marshal Sam Maneckshaw was able to carry his Naval and Air Force colleagues with him due to his affable nature and the personal rapport that he had established with them. Yet, there were several glitches in the planning and conduct of the land and air campaigns. By no stretch of the imagination can it be stated that India fought a coordinated "air-land" war in 1971.

The Indian intervention in Sri Lanka was undoubtedly a disaster from the joint planning point of view. The Kargil conflict of 1999 is the only real example of a coordinated effort. Even here there were initial hiccups and it took the IAF several

weeks to begin bombing the Pakistani intruders' sangars (ad hoc bunkers) on the Indian side of the LoC after the army had made such a request. During the Kargil conflict a joint threat and intelligence assessment of the air defence resources available to the intruders was probably not carried out or else the IAF would not have lost two fighter aircraft and one helicopter to shoulder-fired surface-to-air missiles (SAMs) within the first few days of the beginning of the air campaign.

Taking Defence Reforms Forward Again

The need for the early appointment of a CDS must be seen in the light of the efforts aimed at undertaking defence reforms. Many attempts were made to streamline the national security decision making apparatus after independence, but these were mostly superficial. After the Kargil conflict of 1999, a comprehensive security review was undertaken when the government appointed the Kargil Review Committee (KRC) headed by the late K. Subrahmanyam. The committee was asked to "… review the events leading up to the Pakistani aggression in the Kargil District of Ladakh in Jammu & Kashmir; and, to recommend such measures as are considered necessary to safeguard national security against such armed intrusions." Though it had been given a very narrow and limited charter, the KRC looked holistically at the threats and challenges and examined the loopholes in the management of national security. The committee was of the view that, "The political, bureaucratic, military and intelligence establishments appear to have developed a vested interest in the status quo.'' Consequently, it made far reaching recommendations on the development of India's nuclear deterrence, the management of national security, intelligence reforms, border management, the defence budget, the use of air power, counter-insurgency operations, integrated manpower policy, defence research and development, and media relations.

The Cabinet Committee on Security (CCS) then appointed a Group of Ministers (GoM) to study the Kargil Review Committee report and recommend measures for implementation. In turn, the GoM set up four task forces on intelligence reforms, internal security, border management and defence management to undertake in-depth analysis of various facets of national security management. The task force on higher defence management was headed by Arun Singh, former Union minister who was then an advisor to the Ministry of External Affairs on security matters and who had himself headed the Committee on Defence Expenditure in the early 1990s.

Based on the reports of the four task forces, the GoM recommended sweeping reforms to the existing national security management system. Among the major recommendations of the Arun Singh task force was the creation of the post of the Chief of Defence Staff (CDS) with a tri-Service joint planning staff HQ to provide 'single-point military advice' to the CCS. The CCS accepted all its recommendations, including the one for the establishment of the post of the CDS – a decision that has

still not been implemented. While the tri-Service Headquarters Integrated Defence Staff (HQ IDS) was finally constituted in 2002, it is still headed by a three-star officer who reports to the Chairman Chiefs of Staff Committee (COSC). Approval of the four-star post of CDS was deferred by the Cabinet Committee on Security (CCS) pending further consultations. The two reasons cited for the deferment were the lack of political consensus on the establishment of the post of CDS and opposition within certain sections of the armed forces.

Despite the new measures approved for implementation by the CCS on May 11, 2001, many lacunae still remain in the management of national security. In order to review the progress of implementation of the proposals approved by the CCS in 2001 and to take stock of the new developments over the last 10 years, such as the threats emanating from the sea like the Mumbai terror strikes and the rapid deterioration of the regional security environment due to the growing spread of radical extremism and creeping Talibanisation, the government appointed a Task Force on National Security in mid-June 2011. The task force was led by Mr. Naresh Chandra, former Cabinet Secretary. Simultaneously, the government had appointed another Task Force chaired by Mr. Ravindra Gupta, former Secretary in the government, to analyse the requirements of defence modernisation and self-reliance.

The report of the Naresh Chandra committee on defence reforms in India focused attention on the weaknesses in the national security decision making process and the urgent need for change. The recommendations made by the Naresh Chandra committee, as known in the public domain, appear to be incremental rather than revolutionary. According to reports, the committee has urged the government to ensure adequate military preparedness to deal with a militarily more assertive China. By far the most salient recommendation of the committee is to appoint a permanent Chairman of the present CoSC, that is, another four-star post in addition to the army, navy and air force chiefs of staff. This falls well short of the inescapable operational requirement of appointing a CDS and simultaneously creating integrated theatre commands for joint warfare in future conflicts. While a permanent Chairman of the CoSC will certainly be able to better coordinate the modernisation plans of the three services and improve the management of tri-service institutions than a rotating Chairman, he will have no role to play in integrating operational plans for joint warfare. The solution lies in the establishment of tri-service integrated theatre commands with Cs-in-C who report to the CDS while the Chiefs of Staff of the three Services are primarily planners responsible for recruiting, the raising and equipping of new units, acquisition of weapons and equipment, specialised training and maintenance.

Other recommendations of the committee include the creation of three new tri-service commands to better manage future challenges and vulnerabilities: Special Operations Command, Aerospace Command and Cyber Command. The

establishment of a Bureau of Politico-Military Affairs to deliberate on security issues having foreign policy implications, the setting up of an Advanced Projects Agency on the lines of DARPA under the Scientific Advisor to the Defence Minister to oversee defence research and development (R&D), the posting of additional armed forces officers to the MoD and the MEA and civilian IAS officers to the services HQ for better integration and coordination are also reported to be part of the committee's recommendations. The committee's recommendation to allow for an increase in FDI in defence joint ventures from 26 to 49 per cent has been implemented. The committee's recommendations are unexceptionable and, if implemented, will go a long way towards overcoming present shortcomings. In the interest of transparency and wider debate, its report should be made public.

Need for Single-Point Military Advice

The most urgently needed reform is to ensure that the PM and the CCS get military advice that is not based on individual Service considerations. India's prevailing security environment is marked by regional instability with a nuclear overhang. India has been engaged in an over 50-years old low intensity limited conflict along the LoC with Pakistan, an ongoing Pakistan-sponsored "proxy war" in Jammu and Kashmir and elsewhere in the country and a vitiated internal security environment. Repeated air space violations, burgeoning maritime security challenges and increasing demands for Indian contribution to multinational forces are some of the other factors guiding national security imperatives. Under such circumstances, the early appointment of a CDS is an inescapable operational necessity. More than ever before, and especially in the nuclear era, it is now necessary for the national security decision makers to be given "single-point military advice" that takes into account the inter-dependence of each of the armed forces on the other to meet complex emerging challenges.

Success in modern war hinges on the formulation of a joint military strategy based on the military aim and its joint and integrated execution. At present, under the system bequeathed to India by Lord Ismay in the early-1950s, the three Services draw up their individual operational plans based on the Raksha Mantri's (Defence Minister's) Operational Directive. Only limited coordination is carried out at the operational level and the tactical level. In the present era of strategic uncertainty and rapidly changing threats, no military professional now disputes the unavoidable necessity of a joint planning staff for the planning and conduct of joint operations so that integrated operations can be planned "top down". HQ IDS will undoubtedly meet this requirement in the years to come but if it remains headless, its functioning will remain disjointed and it will never carry the clout necessary to ensure that difficult and sometimes unpalatable decisions are accepted by the three services without questioning.

Many analysts have sought to question the need for single-point military advice for India's civilian political masters. With India's "no first use" nuclear strategy, the CCS would be in a real quandary if at a critical stage during war, when the adversary has unleashed the nuclear genie, the Chiefs of Staff express divergent views on the payoffs of using nuclear weapons in a retaliatory strike and the type and nature of response. The service Chiefs would most certainly be influenced if nuclear weapons were to be employed against forward-deployed fighting troops or bases. They would also need to take the prevailing military situation into account while making their recommendations to the government. It is axiomatic that the differences among the Chiefs of Staff are resolved by the military professionals themselves, with one of them acting as the arbitrator. Only a CDS would be able to take a detached view and present an objective analysis of the situation along with the available options and the advantages and disadvantages of each option.

Theatre Command System

Ideally, the CDS should be an overall commander-in-chief and from him command should flow to individual theatre commanders. Given India's long land borders with a varied terrain configuration and two major seaboards, as also adversaries who are geographically separated, a "theatre" system of tri-service command is best suited for the optimum management of both external and internal security challenges. Contrary to the belief that only the United States needs a theatre system because of its wider geo-political interests and involvement in security issues all over the globe, with its inimical neighbours and peculiar national security threats and challenges, India too needs a theatre system for integrated functioning to achieve synergy of operations with limited resources. The Chinese, with similar needs, have a well-established theatre system.

Each theatre commander should have under him forces from all the three services based on the requirement. The initial allocation of forces need not be permanent and could be varied during war or during the preparatory stage. However, at the inception stage it would be more appropriate to make the CDS "first among equals" and let the three Chiefs of Staff retain operational command and administrative control over their Services as change should be evolutionary and not revolutionary. Once the system matures and theatre commanders are appointed, the Chiefs of Staff of the three Services should have responsibility primarily for force structure and drawing up perspective plans. They should oversee the development and acquisition of weapons and equipment, plan recruitment, guide and coordinate training at specialised training establishments and control administrative matters such as the annual budget, pay and allowances, maintenance support and medical services etc.

Each theatre command should be headed by a four-star General, Admiral or Air Chief Marshal. The state of Jammu and Kashmir (J&K) would naturally form the

'Northern Theatre' for both conventional and low intensity conflict operations (LIC). In view of the ongoing operations and the possibility of continuing conflict, this command should be headed by an army General as the operations are by and large land forces-centric. The 'Western Theatre' comprising the plains of Punjab, Rajasthan and Gujarat could be led alternately by an army General and an Air Chief Marshal both of whom would be adequately schooled in the complexities of the AirLand battle at the operational and strategic levels. The 'Central Theatre' with its area of responsibility lying along the borders of Himachal Pradesh, Uttar Pradesh and Sikkim with Tibet and India's borders with Nepal, Bhutan and Bangladesh, could also be placed under an Air Chief Marshal.

The 'Eastern Theatre' should have its HQ near Guwahati and not at Kolkata. It should be given the responsibility for all national security interests, external and internal, in the seven north-eastern states and should be headed by a General due to the ongoing low intensity conflict (LIC) situation and the fact that the predominant component of the force would continue to be drawn from the army. It will be a long time before the "seven sisters" are well and truly integrated into the national mainstream. Till then, some form of LIC can be expected to continue. The 'Arabian Sea Coastal and Maritime Security Zone', including the Lakshadweep and Minicoy Islands, should naturally be an Admiral's domain. The 'Bay of Bengal Coastal and Maritime Security Zone', including the Andaman and Nicobar Islands, at present called the Andaman and Nicobar Command (ANC), could be headed alternately by a General, an Admiral or an Air Chief Marshal.

Each theatre commander should have under him forces from all the three Services based on the requirement. The initial grouping and allocation of forces would not be permanent and could be varied during the preparatory stage as well as during war on an as required basis. There should be a joint planning staff in each of the Theatre HQ. The staff officers and even the Other Ranks should be drawn from all the three Services. In fact, it should be made compulsory for officers of the rank of Colonel/ Captain (IN)/ Group Captain and above looking for further promotion to have served at least one full tenure (minimum two years) in one of the joint HQ. The officer should have completed the tenure successfully. Only then will it be possible to inculcate a culture of genuine "jointmanship" that is so necessary to fight and win today's wars.

Other Tri-Service Organisations

Several other areas of functioning necessitate overarching military command and control at the national level. While India's nuclear doctrine and policy are guided by the National Security Council and the Cabinet Committee on Security, the execution has to be entrusted to the Services and here a joint approach is mandatory. The newly-constituted Strategic Forces Command (SFC) for the planning, coordination and control of India's nuclear weapons must function directly under the CDS while

the nuclear warheads and the delivery systems comprising the “triad” remain with the respective services and under civilian control. The CDS and through him the C-in-C of the SFC must exercise “command” over the deployment and launching of all nuclear warheads and the delivery systems even though their physical possession vests with the individual Services.

The acquisition and dissemination of strategic military intelligence needs tri-Service planning and should justifiably lie in the domain of the Defence Intelligence Agency (DIA) guided by the CDS. The Director General of the DIA should report directly to the CDS. He must coordinate with the National Security Council Secretariat and the civilian intelligence agencies (R&AW, IB et al) on behalf of the three Services and act as a link between them. The tasking of common assets of the three Services like DIPAC should be controlled by the DIA.

Aerospace, information warfare, cyber-security and issues like the management of the electro-magnetic spectrum, including frequency management, electro-magnetic compatibility (EMC), electro-magnetic interference (EMI), electronic emission policy (EEP) and the offensive employment of non-communications devices such as radars for electronic warfare, should all be the legitimate domain of the CDS and HQ IDS. It is time to set up tri-service Aerospace, Cyber and Special Forces Commands to meet emerging challenges in these fields and to better manage all available resources.

Similarly, for better synergy in training and in the interest of promoting a culture of ‘jointmanship’, including the writing of joint doctrine, it is necessary to merge the training commands of the Services like HQ ARTRAC into a single tri-Service Training and Doctrine Command. Training institutions such as the National Defence College, the College of Defence Management and the National Defence Academy and the proposed National Def University (NDU) that is meant to foster professional military education (PME) should come under the Training and Doctrine Command. A tri-Service Logistics and Maintenance command has also been long overdue. Organisations like the Armed Forces Medical Services, Canteen Stores Department and a host of others must be placed under the direct command of the CDS for better synergy in their functioning and optimum utilisation of their potential.

Concluding Observations

The COSC is an experiment that can only be described as partially successful. It is driven by single-Service requirements and perceptions. It is well known that the Chairman COSC lacks executive authority over Services other than his own Service. The COSC works primarily by consensus and cannot make hard decisions that would be binding on all the services. Perhaps it is not so well known that it took the COSC almost two years to reach a consensus on the revised syllabus of the National Defence Academy. The institution of a national War Memorial was

another contentious issue that dragged on for years with the result that while the police actually began constructing a memorial near Teen Murti in Lutyens' Delhi (later disallowed by the government), the armed forces memorial still exists only on paper. While the end goal is common, there are always disagreements on the route to be followed to get there. During peace time, turf battles and inter-Service rivalries rule the roost and minor, inconsequential issues take up most of the time available for discussion. War time decisions require professional understanding, a bi-partisan approach and, often, hard compromises. As Winston Churchill famously said, "Committees cannot fight wars."

It is time to implement the GoM decision to appoint a CDS. Theatre commands are but one step further in the quest for synergy in operations. It should be a short step, but the way the Indian system works, it will probably be a long one. In the prevailing battlefield milieu of joint operations, combined operations and even coalition operations, modern armed forces cannot be successful without a well-developed and deeply ingrained culture of jointmanship. While the colour of the uniform may be olive green, white or blue, the colour of the heart should be purple. The establishment of the Integrated Defence Staff is a good beginning, but there is a long road ahead. Fortunately, it appears to be paved with good intentions.

Often during war, the fate of an entire campaign can hinge on a single decision. Such a decision can only be made by a specially selected defence chief and not by a committee like the COSC that operates on the principle of the least common denominator. Military history is replete with examples of how such decisions changed the course of a war. Eisenhower's decision to launch the Normandy landings in the face of continuing rough weather and MacArthur's decision to land at Inchon against stiff opposition from virtually his entire staff could not have been made by committees. All other major democracies have opted for the CDS system with integrated tri-Service commands. Even the Chinese have opted for regional theatre commands. India should not ignore these developments any further.

As Victor Hugo said, "No army in the world can stop an idea whose time has come." The appointment of CDS is an idea whose time has come. However, international experience shows that such reform has to be imposed from the top down and can never work if the government keeps waiting for it to come about from the bottom up.

*Brig Gurmeet Kanwal (Retd) is Distinguished Fellow, Institute for Defence Studies and Analyses (IDSA), New Delhi, and former Director, Centre for Land Warfare Studies (CLAWS), New Delhi.

Special Operations Command: Conceptual Framework, Architecture and Force Structure

Brig Deepak Sinha (Retd)*

Introduction

There has been increasing talk in the media about the long awaited Special Operations Command being operationalized in the near future. While this will go a long way in ensuring that our Special Operations Forces (SOF) are organised, equipped and trained jointly to ensure their optimal utilization and maximum bang for our bucks. This will also enable us to put in place tri-service special operations doctrine grounded in the reality of our circumstances and thus enable focused capacity building and establishment of linkages within the security establishment and other ministries towards their employment at the strategic and operational level. In this context while we should examine the manner in which other nations have harnessed their special operations capabilities and learn from their mistakes, we must endeavour not to blindly follow in their footsteps.

As India rapidly develops, Price Waterhouse Cooper considers India to be the third largest economy in PPP terms in their Feb 2015 report "The World in 2050", its sphere of influence is also likely to expand beyond the regional. The growing Indian diaspora and increasing economic interests world-wide make it necessary for the Government to look at enhancing its capabilities to protect its interests abroad. It must have the ability to utilize its vast range of assets in a coordinated manner that would provide the necessary synergy required to ensure that we can successfully meet our foreign policy, security and economic objectives in our areas of interest and influence.

Towards this end the capacity to utilize our soft power assets in an organised manner as well as to ensure that we maintain a robust "Out of Area" (OOA) capability becomes of utmost importance. It is here that SOF, suitably organized, whether utilized to provide the spearhead element of the Rapid Deployment Force (RDF) or used independently for conduct of a vast range of missions, some even in conjunction with other elements of Comprehensive National Power can pay dividends.

Finally a caveat needs to be added here that while military reorganizations tend to be carried out incrementally, given the nature of operational commitments, in the

context of our SOF the necessity for transformative changes is inescapable. History tells us that our political leadership and bureaucracy, both civilian and military, are extremely averse to change as we are inclined to aggressively protect our own turf. Moreover, as SOF will play an increasingly vital role in protecting our national interests in the future it would be logical to reorganize them in the manner that they not only meet our future needs without the need for additional changes, but also show the way forward in enhancing tri-service jointness. This paper therefore approaches the subject with that premise.

Aim

This paper examines the conceptual framework for establishing a Special Operations Command along with the operational and administrative responsibilities that would fall within its remit. It also goes on to suggest force structure and command and control architecture that would be required to be able to meet its operational responsibilities effectively.

Background

There has been much discussion of late with regard to SOF raised over the years within the Country. There is a school of thought that takes an exclusivist view, believing that Special Operations must necessarily be restricted to, what in their view can only be regarded as Special Forces, that is the employment of PARA (SF) units and their counterparts within the Air Force and the Navy. The main argument made in support of this hypothesis is that Special Operations must necessarily be conducted only by small teams and that their employment and tasking must be in the sphere of strategic covert operations, that is primarily operations that are low key and non-attributable. These operations they suggest will "prepare the theatre of operations" for optimal employment of conventional forces subsequently. Further, they believe that given that terrorism and Low Intensity Conflict (LIC) is an extremely difficult challenge that we confront, especially from state sponsored groups inimical to us, they believe that the key to counter terror operations would be the tasking of Special Forces to carry out intelligence based unconventional and politically sensitive operations, such as neutralization of extremist leaders in third countries.

In all of this they hold up the manner in which the United States has employed its SOF, ever since 9/11 as the prime example that we need to replicate. They are correct in assuming that US SOF has a key role in their on-going Global War on Terror. There is ample documentation to suggest that the US SOF has, over the years since 9/11, become the lead agency for Counter Terror operations, having increasingly replaced the Central Intelligence Agency in carrying out covert direct action operations, missions that involve assassination or neutralization of terrorist leaders in the US's Global War on Terror (GWOT)[i].

Clearly the reason for making USSOCOM the nodal agency in the GWOT was that it was not mandated to face oversight by the US Congress as the CIA is constitutionally required to do, thereby making it easier for the President to carry out operations that may not otherwise have been sanctioned keeping ethical and moral considerations in mind. Advocates in this country strongly recommend that we follow on these lines and ensure the Special Operations command that we are likely to establish in the immediate future, must report directly to the Prime Minister through the NSA. A recommendation that superficially appears to have great merit since it seemingly cuts through bureaucratic delay and apathy, as well as greatly enhances response times and feedback while simultaneously ensuring that high levels of secrecy are maintained. Needless to say, such tasks are clearly in the realm of intelligence agencies as operatives inserted into third countries require to be provided deep cover as such operations require complete non-attributability as they may involve assassination, subversion and sabotage.

Clearly there is then a necessity for differentiating operations that the SOF are required to carry out from those that Intelligence Agencies are expected to perform, though there may be circumstances where such clear role or task delineation may not be feasible. Suffice it to suggest that broadly operations may be defined as:-

- Covert, as this conceals its sponsor, i.e., the authorizing agency does not take responsibility whether the operation succeeds or not.
- Clandestine, as this conceals its existence, i.e. mission success hinges on the ability to keep planning and execution secret. The sponsor will, however, normally claim responsibility upon completion.[ii]

Ideally, in our context, Research & Analysis Wing (R&AW), our foreign intelligence establishment that is constitutionally mandated to carry out such operations should have its own para-military establishment for carrying out such operations and, where required, request the assistance of SOF elements if there is a necessity for additional support. Such support should, however, be more an exception than the general practice. It is in this context that the USSOF includes the 75th Ranger Regiment with its four light infantry (Ranger) battalions as well as the Marine Raider Regiment with its three raider battalions within the SOF community as they provide the required support where required.

However we would be making a grave error if we were to adopt such an approach for a number of important reasons that are of relevance to us, but do not necessarily apply to the United States. At the outset we need to remember that the United States is the only global super power with its forces deployed in bases all over the world. The diplomatic, economic and military clout that it wields makes it impossible for the vast majority of countries to resist or oppose its actions, mostly forcing them to operate in conjunction with US Forces. Therefore when USSOF operate

"clandestinely" in Somalia or Yemen or Pakistan, it is more often than not, with the tacit approval of the government of that country. If reports that suggest the Bin Laden raid was conducted with the knowledge of the Pakistani military are correct, as suggested by veteran journalist and prize winning author Seymour Hersh, then it only confirms the argument put forward.

The Raymond Davis case, for example, clearly brought out the adverse consequences of attempting to operate in a country without the host government's permission. In this particular instance Davis was taken captive by Pakistani Police after he killed two people who he suspected were attempting to kidnap him. He faced murder charges but was finally allowed to go after both governments struck a deal which included compensation in millions to the families of those killed[iii]. In our context, we would well to remember the adverse ramifications of the on-going casein Pakistan against Commander Yadav (Retd), who is accused of allegedly being a R&AW agent and involved in fomenting terrorist activities in Baluchistan.

We must also face the fact that we have neither the wherewithal nor the financial capacity to engage in a global effort as USSOCOM has done. This is best illustrated by the fact that the USSOCOM with approximately 66000 personnel has an annual budget of around US$10 Billion (excluding pay and allowances and equipment costs)[iv] while our total defence budget is approximately US$ 48 Billion. In fact, while we consider ourselves to be an aspiring rising power and believe that our areas of interests and influence stretch from the Arabian Sea to the Bay of Bengal and the Indian Ocean and its Littorals the facts at present do not tend to support such ambition.

Our strategic ambitions must be tempered by the fact that we have two nuclear armed neighbours in our region with which we share disputed borders and inimical relationships. In addition, we also have to concentrate on overcoming our adverse military capabilities vis-à-vis China, which to a great extent can be blamed on poor border infrastructure and border management structures. We are thus, locked into a competitive embrace that ensures that the primary focus of our security establishment remains on our immediate neighbourhood. Furthermore, we cannot wish away the fact that we have more than a quarter of the world's poorest and dispossessed. Thus, our internal socio-economic challenges and disparities ensure that our political leadership is completely focused on alleviating these, as it must, and in ensuring that fissiparous tendencies within are tackled and we are able to meet the aspirations of our humungous population.

In this context we must also take into consideration the fact that despite its unbridled powers the United States has been extremely circumspect when operating against countries that would not take kindly to such blatant disregard for their sovereignty and have the wherewithal to respond. For example, in these past decades no attempt has been made by the USSOF to get involved in supporting

those opposed to the Russian established Government in Chechnya or for that matter in supporting dissidents against the North Korean regime. It also failed to respond when Russian Spetsnaz assisted in the Russian take-over of the Crimea or the subsequent troubles in Southern Ukraine. Similarly, attempts at bolstering the Syrian opposition to the Assad Regime have also been a spectacular disaster where US $ 500 Million was wasted on attempting to train a rebel army.[v] Libya too is a case in point as the regime change brought about by USSOF and their partners has resulted in an ongoing civil war which has only further destabilized the region.

Finally, while USSOCOM has been responsible for conducting some extremely well planned and executed operations that include the capture of Saddam Hussein and the neutralization of Osama Bin Laden, its impact on GWOT is questionable. These successes do not take away from the fact that the US has suffered military stalemate/ defeat against irregular forces in its Afghanistan, Iraq and Libyan campaigns undertaken following the 9/11 attacks. Some analysts have concluded that these defeats and the rise of terrorism in other areas like Somalia and the Yemen can be blamed to a great extent on the untrammelled criminal acts of assassination and torture conducted by the US SOF, especially the Predator attacks that have caused large civilian casualties.

It is now commonly acknowledged that the rise of Daesh can be directly attributed to the treatment meted out to Abu Bakr al-Baghdadi, self- proclaimed Caliph of ISIL, and also to some of its other major leaders, who were held prisoner in the infamous SOF run prison of NAMA adjacent to the Baghdad International Airport. In addition there have been credible reports that the US Army leadership has been particularly unhappy with some SOF actions that have adversely impacted counter-insurgency operations in Iraq and Afghanistan due to total lack of coordination between SOF and regular forces. As Turse puts it “Over the years, in that country (Iraq), in Afghanistan, and elsewhere, special operators have regularly been involved in all manner of mishaps, embroiled in various scandals, and implicated in numerous atrocities. Recently, for instance, members of the Special Operations forces have come under scrutiny for an air strike on a *Médecins* Sans *Frontières* hospital in Afghanistan that killed at least 22 patients and staff, for an alliance with “unsavory partners” in the Central African Republic, for the ineffective and abusive Afghan police they trained and supervised, and for a shady deal to provide SEALs with untraceable silencers that turned out to be junk, according to prosecutors”[vi] .

It would not be incorrect to conclude that while USSOF have certainly played a critical role in the GWOT, its actions have not been decisive in rolling back the terror threat. In fact, it can be argued that its aggressive and coercive use of force based on an unquestioned mandate from the President with no independent oversight and absolutely no concern for the impact of their actions on the conventional

forces strategy has actually been detrimental to the over- all US war effort. More importantly, they have been able to perform multifarious tasks primarily because of the clout that the United States enjoys thanks to its overwhelming superiority economically and militarily as the sole Super Power.

Conceptual Framework

At the outset we must clearly define our concept of what constitute SOF and the overarching philosophy that will guide their employment. While special operations are carried out from the tactical to the strategic level, in the context of this paper SOF must constitute only those joint forces that are specially trained, equipped and organized for conduct of special operations at the operational and strategic level. That implies that such operations must impact and be conducted at the theatre level and beyond. The size of the force is immaterial and must be appropriate to their tasking.

It must be mentioned here that in our context there has been a debilitating, and rather unnecessary, battle of attrition over the past two decades, to the detriment of the Parachute Regiment, over whether Parachute units should be also considered as SOF. To suggest they are not so because they act as light infantry after they have been dropped is to be stuck in a time warp. Moreover, even PARA (SF) units have to excel in light infantry tactics if they to close with the enemy to destroy him, which is a necessity. That apart, a study of missions carried out by airborne units of both sides during the Second World War clearly show that they were mainly utilized at the strategic level to carry out coup-de-main missions aimed at destroying/capturing bridges and raiding headquarters, communication hubs and Air Defence /Coastal battery positions deep in enemy territory. Their main impact was on the mind of the commander forcing him to either act in haste or not at all, thereby creating panic along the chain of command. We witnessed this in Bangladesh after the successful airborne assault on Poongli Bridge and subsequently in the Maldives when an intervention was carried out to prevent a coup becoming successful. None of these tasks, by any stretch of imagination, would be given to regular infantry battalions deep behind enemy lines.

Moreover, in the existing scenario in which deep thrusts are unlikely, given the nuclear over-hang, and large scale airborne drops (of two battalions/at brigade level) are impractical under most circumstances because of the air defence environment and conflict duration, employment of Parachute units will be restricted to two companies/ battalion group at best. Existing capabilities within our mechanized forces do not require them to establish bridge-heads across water obstacles till relieved. Their importance in future wars lies in their ability to create panic and disruption in rear areas and delay/hinder move of reserves during active hostilities. In addition there are numerous other missions they could be utilized for in operations other than war. Thus, it appears reasonable to suggest that both

PARA (SF) and PARA units fall within the ambit of SOF. Though they have differing tasks, there will be contingencies that would require both these types of units working together to provide synergy.

Thus, in our context, SOF must include the following elements:

- PARA (SF) and PARA battalions as well as the Parachute Brigade with its organic structure. While PARA (SF) battalions will provide elements for low key, below the horizon operational employment, PARA battalions will provide the "muscle" required for Direct action, Coup-de-Main and OOA contingencies (as a part of the Para Brigade).[vii]
- MARCOS.
- Only the Combat Search and Rescue (CSAR) elements from GARUDs. As they primarily provide quick reaction elements for base security, those elements must be de-linked from CSAR elements.
- Both fixed wing and helicopter aviation units that will need to be specifically trained and equipped for special operations.
- The Special Action Groups (SAG) that are presently a part of the National Security Guards (NSG). This should be reduced to one group with a permanent cadre and no rotation. The remainder NSG should be reorganized to provide, in addition to its existing role, immediate intervention elements in various cities/ states.[viii]
- The Special Frontier Force less the Special Group. The Special Group needs to be replaced by a para-military establishment, preferably manned by retired special operations operatives that would be a part of the R&AW. The size and manning pattern of SFF needs to be reviewed and it should be reduced to three columns with indigenous manpower from regional areas for covert employment. [ix]
- Supporting elements including intelligence, communication and logistics.
- Training establishments focused on selection and advanced skills training.

In terms of employability, SOF must be capable of covering the complete spectrum of conflict from peace at one end to armed conflict at the other extreme. Its tasking should be broadly grouped under three parameters- Special Reconnaissance (SR), Direct Action (DA) and Military Assistance (MA). They would include:-

- SR includes area assessment, advance force operations, target acquisition, early warning on enemy forces concentration, movement, command and control, and intelligence on critical infrastructure in denied territory. This list is

not exhaustive, and the emphasis on intelligence collection of operational or military-strategic value is of special importance. SOF elements embedded in selected Diplomatic Missions abroad will form an extremely critical part of this capability.

- DA involves offensive operations normally limited in scope and duration, and usually incorporates a planned withdrawal from the immediate objective area. Coup-de-Main missions that require holding of objectives for limited durations would also be considered as a part of DA.
- MA encompasses assistance to friendly or allied forces in peace, crisis and conflict by providing immediate technical advice and assistance as required.

Likely Roles and Mission Profile

Given the geo-political, economic and strategic environment facing India and the likelihood of asymmetric and fourth generation warfare being the dominating narrative, the appropriate role of the SOF in responding to threats that seek to undermine India's strategic interests needs to be addressed. These include the following:

- Furthering India's sphere of influence in selected countries which would be in keeping with India's growing stature as an economic powerhouse and a world power on its own standing.
- Identification of future threats in the domain of terrorism, energy, food, finance and economy. Embedding SOF in organizations operating in regions of India's concern and shaping the strategic environment to India's advantage will become a strategic imperative.
- Counter Terrorism intervention including hostage rescue internally and externally.
- Responding to the call for military assistance from a friendly country to support them during a hostile takeover or terrorist strike.
- Setting up of military bases in friendly countries at the request of the host nation, which could also be viewed as a base for intervention to protect India's vital national interests.
- Protecting India's Sea Lines of Communication (SLOC) by proactively projecting the Indian SOF capabilities against likely threats and protecting its assets in regions far away from the homeland.
- Ensuring the safety and security of Indian citizens abroad in the event of a local crisis. This may include their evacuation from conflict zone during times of civil unrest and breakdown of political order.

- In the likelihood of armed conflict, shaping and preparing the future theatre of operations and in providing force multiplier capabilities to our conventional forces at the operational and strategic levels. This could also include raids and Coup-de-Main missions as a part of DA.

The SOC Mandate

There can be little argument about the necessity for consolidating all existing SOF resources. It can be no Services case that if an SOC is established, the units that would be under its purview would need to be raised ab initio. Not only would that require immense capital expenditure, both in terms of finances and manpower, but also result in duplication of effort, making the whole structure a white elephant. Moreover, as and when we do establish tri-services theatre commands, something completely unavoidable, the Service Chiefs will no longer be responsible for operational employment of their forces which would then logically be delegated to the Theatre Commanders. At that stage where would the SOF fit in?

Before examining as to the manner in which we should go about establishing our SOC, it would be worthwhile to follow the torturous course of the establishment of USSOCOM as it exists today. All are aware that the disaster of "Operation Eagle Claw" in 1980, the failed mission to rescue American hostages held in Iran, was attributed to lack of jointmanship and a convoluted command and control set- up, among other things. In order to correct the situation the Army first tried to consolidate all Army SOF under 1st Special Operations Command in 1982. However, the lack of jointness led to concern within the Senate Armed Services Committee which resulted in the Department of Defence creating the Joint Special Operations Agency in January 1984. This Agency was however flawed as it had neither operational nor command authority over any SOF. In 1986 the Goldwater-Nichols Defence Reorganization Act was passed which appointed the Chairman Chiefs of Staff Committee as the single point advisor to the Secretary of Defence and the President. They also forced the establishment of Joint Theatre Commands, the C in C's of which also had direct access to the Defence Secretary and the President.[x] Despite stiff opposition the Nunn-Cohen Bill[xi] was passed in 1987 and amended the Goldwater-Nichols Act to establish the USSOCOM under a four star C in C as a separate command which supported other theatre Commands. In 2014 it was re-designated as a combatant command.

However, given our limitations in terms of resources and employability we must play smart and establish an agile and flexible architecture that ensures we meet all our operational requirements ranging from the irregular to the conventional war scenario and beyond, while at the same time avoiding establish bureaucratic silos and duplication of capabilities, visible elsewhere. This requires that the Special Operations Command (SOC) be a tri-services operational command reporting directly to the Chief of Defence Staff, as and when established, additionally with

direct access to the National Security Advisor. The command and control of all SOF personnel, resources and facilities for operations, training and administration must rest with the GOC-in-C SOC. Coordination and conduct of special operations tasks at the operational level will be carried out by subordinate SOF Headquarters co-located with the Theatre Commands as required. In addition, required institutional linkages with the Ministry of External Affairs, R&AW and with the National Counter Terrorism Center (NCTC), as and when established, must be ensured by posting of appropriate personnel in respective Headquarters.

Organizational Structure

The organizational structure given at Appendix has been arrived at keeping in view the following basic principles:

- The SOC will be responsible for conduct of all operations at the strategic level and for vetting and providing requisite resources for special operations at the operational level. Planning and conduct of missions at the Operational level will be the responsibility of the SF Group for the nominated Theatre in conjunction with the Theatre HQs.
- The SOC and its subordinate HQs will be responsible for all operational, administrative and disciplinary aspects pertaining to SOF units, establishment and personnel.
- SOF training establishments will be responsible for selection of trained personnel provided from regular units as well as for advanced skills training for those selected for SOF. In this context the existing PRTC and SFTS will be merged into a tri-services establishment that will be responsible for all selection and advanced skills training. Similarly, the PTS and AATS will be amalgamated to form a tri-service establishment with instructors being provided from all three Services.
- While the SFF will be under command of the SOC, it will continue to maintain separation to ensure non-attributability and personnel will continue to be provided as hitherto fore. Their training will continue to be under the aegis of the Establishment 22 with its own Academy and PTS. The reorganized Special Group could continue to be trained alongside.

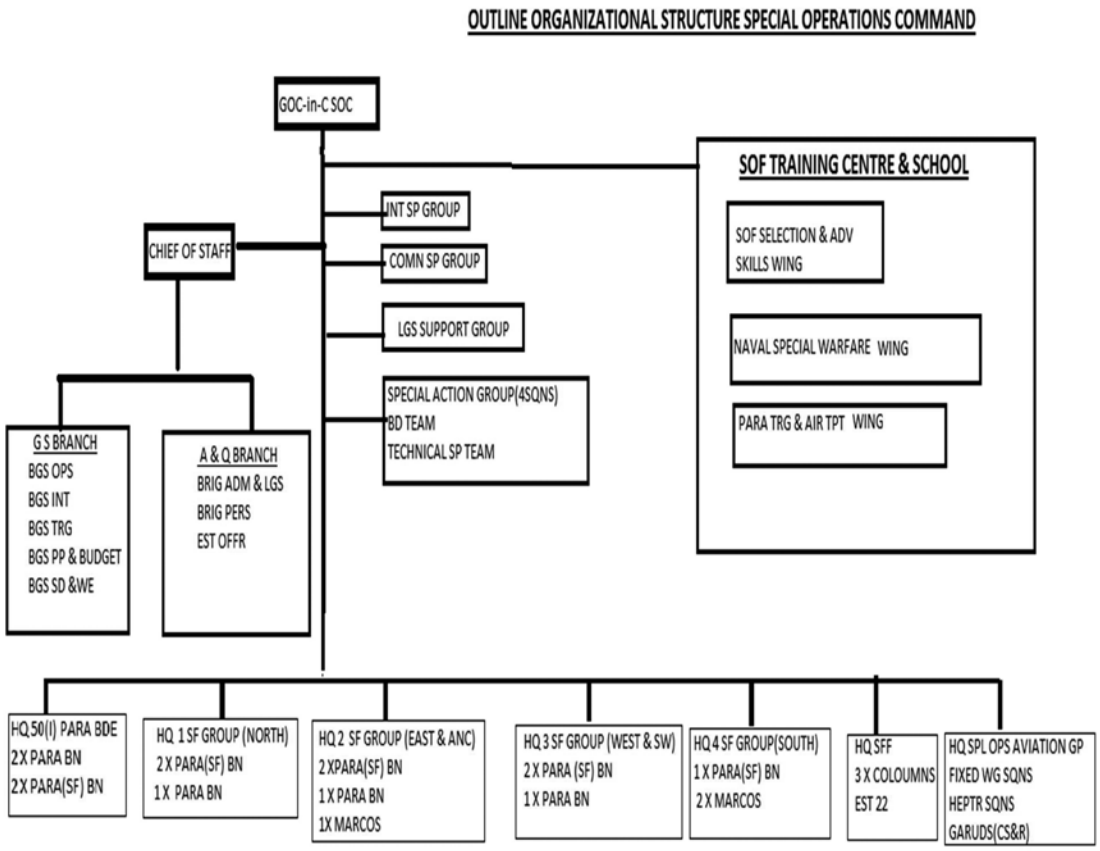
Conclusion

The necessity for establishing tri-services SOC with all SOF elements placed under it is inescapable given the existing security scenario. That this organization will play an even more vital part in the future in proactively ensuring that our security concerns are adequately addressed is also a foregone conclusion, especially given the manner in which fourth generation warfare is progressing and our own regional challenges.

There can also be little doubt that it is better to look at a total transformation of SOF than to progress forward with incremental changes as that would only delay optimum synergy given entrenched views that exist. It will have to be a top driven exercise probably being initiated at the PMO and under direct supervision of the Raksha Mantri. Adequate safe- guards must also be put in place to ensure independent validation of capabilities and performance as also to ensure that equipping norms and personnel policies do not vary greatly from those applicable to the regular units as officers and men will have to revert to regular forces at a later stage or on volunteering out or being found unsuitable subsequently.

We all have choices to make. The military leadership can remain wedded to its age old perceptions and outlook and ignore the need for changing with the times. They can continue to kowtow to bureaucrats and politicians and avoid creating waves in the hope of extracting personal benefits post-retirement for services rendered. The politicians and bureaucrats can continue to spook themselves into believing the worst of the military and work actively at ensuring it remains disempowered or they can take the initiative and turn it into a modern military that we deserve and can be proud of. That we are fated to repeat our follies, till we are willing to learn from history is an old adage that's best not forgotten and a repeat of 1962 is the last thing that our political, military and bureaucratic leadership would wish upon themselves.

*Brig Deepak Sinha (Retd) is a veteran Special Forces Officer


OUTLINE ORGANIZATIONAL STRUCTURE SPECIAL OPERATIONS COMMAND
GOC-in-C SOC
CHIEF OF STAFF
INT SP GROUP
COMN SP GROUP
LGS SUPPORT GROUP
SPECIAL ACTION GROUP(4SQNS)
BD TEAM
TECHNICAL SP TEAM
SOF TRAINING CENTRE & SCHOOL
SOF SELECTION & ADV SKILLS WING
NAVAL SPECIAL WARFARE WING
PARA TRG & AIR TPT WING
G S BRANCH
BGS OPS
BGS INT
BGS TRG
BGS PP & BUDGET
BGS SD &WE
A & Q BRANCH
BRIG ADM & LGS
BRIG PERS
EST OFFR
HQ 50(I) PARA BDE
2 X PARA BN
2 X PARA(SF) BN
HQ 1 SF GROUP (NORTH)
2 X PARA(SF) BN
1 X PARA BN
HQ 2 SF GROUP (EAST & ANC)
2 XPARA(SF) BN
1 X PARA BN
1X MARCOS
HQ 3 SF GROUP (WEST & SW)
2 X PARA (SF) BN
1 X PARA BN
HQ 4 SF GROUP(SOUTH)
1 X PARA(SF) BN
2 X MARCOS
HQ SFF
3 X COLOUMNS
EST 22
HQ SPL OPS AVIATION GP
FIXED WG SQNS
HEPTR SQNS
GARUDS(CS&R)

[i]Jeremy Scahill; Dirty Wars : The World is a Battlefield; Profile Books Ltd; 2013

[ii]Robertson, Tom; Making New Ambitions Work: Transformation of the Norwegian Special Operations Forces; Defence and Security Studies 1/2007; pg 21; https://brage.bibsys.no/xmlui//bitstream/id/12812/DSS0107.pdf

[iii]Scahill; Op Cit; pp 403-429

[iv]Thomas, Jim & Dougherty, Chris; Report of the Center for Strategic and Budgetary Assessments; Beyond the Ramparts: The Future of US Special Operations Forces;2013.

[v]Turse Nick; Tomgram: Success, Failure, and the "Finest Warriors Who Ever Went Into Combat"; http://www.tomdispatch.com/blog/176060/tomgram%3A_nick_turse,_success,_failure,_and_the_%22_finest_warriors_who_ever_went_into_combat%22/; 25Oct 2015

[vi]Ibid

[vii]For Further amplification see Sinha, Deepak; Airborne & Special Forces: Reassessing Role, Tasks & Organizations; Indian Defence Review (Vol 30.3);Jul-Sept 2015; pp

[viii]For further understanding please see "Revamp National Security Guards" in The Pioneer dated 18-Jan-16, "From 26/11 to San Bernadino and Pathankot"; Indian Defence Review website dated 15-Jan-16 and "Beyond the Bayonet: Indian SOF in the 21st Century, Gyan Publishing House, 2006; pp167-176 by the author.

[ix]For further amplification see "Beyond the Bayonet: Indian SOF in the 21st Century" pp 177-182 by the author

[x]Lederman, Gordon Nathaniel; Reorganizing the Chiefs of Staff: The Goldwater- Nichols Act of 1986; Greenwood Press; 1999.

[xi]Cohen, William; "S. 2453"; A Bill to enhance the capabilities of the United States to combat terror and other forms of unconventional warfare; 1986.

Organization Philosophy for the Cyber, Space and Special Operation Commands

Lt Gen GS Katoch, PVSM, AVSM, VSM (Retd)*

Introduction

The argument for Cyber, Space and Special Operation Commands for strengthening India's defence predates their recommended raising by the Naresh Chandra Task Force (NCTF) in 2012.[1] The NCTF only put official approval on what had been articulated by military planners and think tanks for some time. Decline in defence allocations is a subject for much debate in India but in a developing country is a reality which has to be factored in defence perspective planning. Another factor in perspective planning is the changing shape of war including nuclearisation of the subcontinent which makes large scale conventional war improbable if not impossible. Both these factors make it inevitable that manpower intensive armed forces will decline and technology efficient and economic means of defence will gain importance. Lack of resources dictates that clear threats should be the rationale for defence modernization rather than fashion. Our country faces tremendous challenges in combating poverty; hence, decline in defence allocations in the absence of conventional war is not surprising. As Cohen and Dasgupta state "[in India] the balance of resource allocation between defence and development has to favour the latter".[2] In such an environment in order to maintain and strengthen the military we need to optimise and modernise. Optimising means economising and synergising. One way to do this is through joint organizations which synergise power; Hence, the case for having Joint Cyber, Space and Special Operations Commands.

The Cyber, Space and Special Operations – Enablers for Victory in the Changing Operational Environment

Cyber. The word 'cyber' is the short form of the word 'cybernetics' which evolved in the 1940's from the Greek word 'kubernan' which means 'to steer'. Cybernetics is a noun which is the name for the science of communications and automatic control systems in both machines and living things (e.g the Central Nervous System in medical field is in the realm of cybernetics). In the internetted world 'Cyber' refers to the notional environment in which communication over computer networks occurs. Presently the predominance of computer networked communications drives the world. Digitisation has enabled storing mind-boggling amounts

of data in miniscule physical space. Algorithms enable searching for the proverbial needle in a haystack and enabling data to be processed, organized, structured or presented in a given context so as to make it useful. In other words converting data into information. In the military field information provides intelligence and in modern war intelligence enables the optimum utilisation of resources to achieve victory. The dependence on cyberspace by the military also makes it an object of attack. Attacks can be physically on the facilities where the hardware of Command, Control, Communications,Computers, Intelligence, Information, Surveillance and Reconnaisance (C4I2SR) systems is located, or they can be on the software by distorting the programs which operate the C4I2SR. Targeting the hardware and software of C4I2SR systems is Cyberwar. This war takes place in a notional fifth dimension of war- Cyberspace.

Space. From the time Nazi Germany's V2 rocket crossed into the boundary of Space in a vertical launch on 22 Jun 1944,[3] Space became one more dimension in which war can take place. In the medieval world Space was the abode of the Gods. It was unfathomable and hence names of early planets were the names of Gods both in Western and Indian astronomy. So profound was the belief in its religious mysticism that medieval astronomers making revelations which conflicted with religious beliefs were prosecuted. For example, Galileo was imprisoned for life. Mankind has come a long way since then. The utility of Space to benefit humankind is unquestionable. However, so far mankind's direct dependence on space extends only upto 35,786 kilometers above the Earth i.e in geosynchronous orbit. Upto this distance the use of satellites for communication, observation, remote sensing and navigation have exponentially increased the military utilisation of Space assets, which in turn makes Space a true physical fourth dimension for warfare after land, sea and air. One day through revolutions in travel, mankind will be able to open new habitations in Space. But till that happens interfering with the functioning of enemy satellites orbiting the earth and protecting your own satellites are the only offensive/defensive operations that can take place in space.

Special Operations. Special Operations are technologically the least complex of the triad being discussed but the most complex in execution. To a conventional military mind Special Operations are difficult to equate to a battle-winning factor. One definition of Special Operations is that these are "operations conducted by specially organized, trained and equipped military […] forces to achieve military, political, economic, or psychological objectives […]. These operations are conducted during war and in operations other than war independently or in coordination with [...] conventional forces […] Special Operations differ from conventional operations in degree [… of] dependence on detailed operational intelligence [which is much more critical]".[4] Wherever conventional war becomes difficult to wage on account of either nuclearisation, political compulsions or when fighting an irregular opponent, the Special Operation Forces (SOF) provide the most effective option. This is

because of their attributes of economy of scale and deniability. Hence, in a globalised world where conventional wars become impractical, SOF have proliferated. This includes Naval and Air Force special operations capabilities which provide the ability to undertake operations in all three environments. The connect of Special Operations to Cyber and Space lies in the vital utility of these two domains to plan and conduct Special Operations.

Joint Operations

Joint operations are based upon a military doctrine which places priority on the integration of the three Services of a state's armed forces into one unified command. While in the United States 'joint' includes four Services, the Army, Navy, Air Force and Marine Corps, in most other militaries it refers to an integration of the first three. Worldwide 'Jointness' has traditionally been resented by the three main Services in that it dilutes their distinct identity, independence and power. The concept of Unified Combatant Commands which is the present basis of organization of the predominant military power in the world, the USA, was for decades opposed by its respective Services until it was forced upon them by the Goldwater-Nichols Act of 1986. Though there had been a long running debate on the value of jointness, it was the bumbling US involvement in Grenada where the three Services indulged in an ill coordinated operation that the act could be pushed through.[5] While we should not blindly follow the US model yet its framework provides a defined route to follow.

An Organizational Insight in the Raising of Cyber, Space and Special Operations Commands

The word 'Command' associated with a military organisation in the Indian context is a noun which refers to an organisation headed by a three star general who is equivalent in ceremonial precedence to a Chief Secretary of a state.[6] In the Indian Army Context, the head of a 'Command' is referred to as The Army Commander or the 'General Officer Commanding-in-Chief' (abbreviated to GoC-in-C) Northern Command, Central Command etc. The Air Force and Navy also follow the same convention, their equivalent commanders being called 'Air Officer C-in-C (Western Command, SW Command etc) and Flag Officer C-in-C (Eastern Command etc). The C-in-C exercises supreme operational command and control of a nation's military forces (such as the President of India being the C-in-C of the Indian Armed Forces) or significant elements of those forces. The C-in-C appointment carries great single point authority combining operational and administrative functions within the geographical area of that Command. The appointment also carries great prestige. A Command in the US context refers to both its Indian connotation as far as operational/administrative responsibility is concerned, as well as any organisation which has a distinct function. The Indian connotation avatar in the USA is the 'Combatant Command'. The US military organisation peculiar to its

global deployment and responsibilities has six regional (Unified) Combatant Commands (Pacific Command, European Command etc) and three functional commands (Strategic, Special Operations and Transportation Commands). The later are equivalent in power and prestige to the Combatant Commands with a global charter. In India also we have functional Commands such as the 'Joint' Strategic Forces Command (SFC), The Army and Air Force Training Commands and the Air Force Maintenance Command. But other than the SFC the other functional Commands are not 'joint' as they are specific to their Service. In context of this article the Cyber, Space and Special Operations Commands are envisaged as Joint Functional Commands.

'Operational' and 'Line' Functions. The Indian army is organised into an Army HQ and the above explained 'Commands'. Among the constituents of Army HQ are the Line Directorates. They handle line functions of each Arm and Service. Examples of 'Arm' Line Directorates are the Directorate of Mechanized Forces, the Infantry Directorate the Artillery Directorate etc. and of Service directorates, the Supply and Transport Directorate, the Electrical and Mechanical Engineers Directorate, the Ordnance Directorate etc. The Commands are Field Armies which conduct actual operations. Their charter includes training for war, familiarisation in the actual area of employment, making operational plans and ensuring the field forces are quartered, equipped and administered. The Line directorates are responsible to formulate policy and carry out staff functions to organize, train, and equip their arm or service; to prepare specific tactics and drills, to plan and implement modernisation of weapons and equipment peculiar to their arm/service and to formulate management and progression policies peculiar to their own personnel. The Air Force and the Navy also have a distinction between 'Command' and 'Line' functions though not organized in the same manner as in the Army. The 'Command' and 'Line' functions are separated so that those responsible for operations do not get involved in the bureaucratic 'Line' functions.

Suggested Organization Philosophy for Cyber, Space and Special Operations Commands

The initiative seeking approval of the Defence Cyber Agency (DCA), the Defence Space Agency (DSA) and Special Operations Division (SOD) is a welcome first step in setting up the 'Command' organizations recommended by the NCTF. This paper believes that at this nascent stage it is not an efficient option to set up Command organizations. It is better to consolidate and coordinate existing assets and then incrementally build the organization as per requirements. Because of the complex nature of these envisaged Commands and financial constraints it is better to upgrade/expand as the nature of role, charter and duties becomes clearer. It is also advisable not to reinvent the wheel. We need to learn from the experiences of others and adapt those suitable for our conditions.

US Space and Cyber Commands. The United States Space Command was formed before the US Special Operations Command (SOCOM). But whereas the later has gradually become a functional Combatant Command, the former has been made a Subordinate Unified Command under a Functional Command, the US Strategic Forces Command. In other words it does not have a C-in-C. This is inspite of the fact that in 2007 it accounted for 95% of the world's military space expenditure.[7] In 2009 the US Cyber command was also raised as a Subordinate Unified Command under the Strategic Forces Command. This means that the C-in-C Strategic Forces Command wears the hats of C-in-C of two additional smaller 'Commands', the US Space and Cyber Commands. If the USA with greatly more resources does not feel it is justified to set up full fledged Space and Cyber Commands, then we are not incorrect in contemplating the DSA, DCA and the SOD.

Special Operations Command. A school of thought feels that since the US SOCOM is a full fledged Command, so should be our Special Operations Command. The argument against this is that the size of the Indian Special Forces is lesser than the US SOCOM at the time it was formed. SOCOM when formed had 32,000 personnel.[8] While Indian Special Forces presently have a strength of approximately 12000. This includes 8000 Army Special Forces (SF)[9] , 1080 Garuds (they are essentially for asset protection[10] and post the terrorist attack at Pathankot on 02 Jan 2016 are expected to be increased by 700 personnel[11]), and 1200 Marine Commandos (MARCOS)[12] . Lt Gen PC Katoch (retd) a former SF officer and an authority on Indian SF has recommended that we should not have a 'Command' at all for the SF.[13] He also states that Special Operations are "not a game of numbers"[14] and recommends SF based on small teams for carrying out strategic tasks.

Administrative Aspect. Any new organisation requires administrative wherewithal. They require office accommodation, messing, quartering, electricity, water, maintenance support, transport, security and communications among the major tangibles and leadership, HRD, petty finances, troubleshooting, assistance in social events, welfare and legal assistance among intangibles. Any new unified organisation therefore needs a sheet anchor. For small organisations it is not cost effective to be completely self sufficient. They need to ride piggyback on a bigger brother.

Organization Design

Organizations have Geographical, Functional and Divisional design.[15] The existing system of most of our Commands are based on a geographical design model. In a functional structure activities are grouped by common function from the bottom to the top of the organization. The DCA and DSA fit into this design. The advantages this organization offers are economy and in-depth knowledge and skill

development in one core field. The Divisional design is suitable for the SOD. The feature of this structure is that it enables putting together of teams as per the mission/requirement. It also promotes flexibility as task forces can be organised as per the mission and operating environment. In organization design, military organisations traditionally need a vertical linkage, a hierarchy. While this is an unavoidable in modern war there is also a need for horizontal linkages. The DCA, DSA and SOD will be organisations which will also need to interact horizontally with each other. For example, intelligence through cyber and space means would be pivotal to plan Special operations. For horizontal linkages to function seamlessly these organisations need to be joint in their components.

The US SOCOM was formed by closing up an existing Unified Command headed by a C-in-C, the US Readiness Command (USREDCOM). That Command had a function of keeping reserves battle ready and had a "reputation as a desirable 'terminal assignment'".[16] The requirement for a SOCOM outweighed the requirement of REDCOM in view of financial constraints. HQ SOCOM was therefore formed without any additional outlay on manpower or infrastructure. Similarly, the DCA, DSA and SOD are recommended to be built using existing headquarters.

Recommendations

In view of the above the following are recommended:

- The three organizations to be raised not as traditional Commands but as Defence Cyber Agency (DCA), the Defence Space Agency (DSA) and Special Operations Division (SOD). Their detailed organizations should be made keeping in view the workload and technology as existing at present with a 15 year forecast of future threats and security environment. A forecast of the shape of things too far in the future suffers from inaccuracies. This will avoid the pitfall of creating organisations which 'come before their time' and then strive to 'create' work to justify their utility.

- The DCA, DSA and SOD should carry out both 'Line' and 'Command' functions for optimum integrated growth. The very nature of these organisations means that they will not be restricted to defined geographical areas of responsibility. The requirement of development of specialised doctrines, equipment and employment philosophies for them means that if these organisations combine both 'Line' and 'Command' functions their growth will be better planned and coordinated.

- We should follow the US model of the Cyber and Space Commands and raise the three entities i.e the DCA, DSA and SOD subordinate to existing Commands. This will ensure that they are up and running in the shortest time.

- The arguments for having the Navy responsible for the DCA, the Air Force for the DSA and the Army for the SOD are sound and need no change. However, they need to have horizontal linkages because their operations can neither be planned or conducted in a standalone basis.
- Suggested Command & Control options which can be debated are:
  - (i) DCA under Southern Naval Command. DSA under Southern Air Command and SOD under the Central Army Command/Army Training Command or any administrative Area HQ[17] converted to SOD.
  - (ii) Follow the US model of DCA and DSA under the Strategic Forces Command. No change in SOD to above.
  - (iii) All three organisations operationally under the HQ IDS and administratively under their respective Services.
- Cyber, Space and Special Operations 'Commands' as in the Indian connotation of this organizational definition can come into being when the workload, span of control and responsibilities of the organization become too big to be handled by the parent Command.

Conclusion

When planning for the future, forecasting and factoring in the experience of others is a must. In such planning/ forecasting a 100% correct decision is impossible but it does protect one from being 100% wrong. In military perspective planning while we must learn from others, we must modify our actions to evolve organisations for our peculiar threat environment. Planning without any consideration of our financial constraints would be flawed as we would build only castles in the air. One must also make the pragmatic assumption that military threats, technology and our planned responses which drive demand for new organizations and equipment will not continue unaltered. There are political, economic, environmental and technological factors which will always change the nature of security threats that a country faces. The Strategy of annihilation was characteristically the American way of war,[18] it was best exemplified in the US approach to war fighting from the Second World War to the Vietnam war. Following the US lead all large armies of the world had adopted this way of war. From the last 15 years this way of war has been conclusively found to be ineffective. The increasing focus on the Cyber, Space and Special Operations capabilities is the outcome of this lesson.

* Lt Gen GS Katoch is a Special Forces Veteran

[1]PC Katoch, Indian Special Forces: 2030. *CLAWS Journal,* (Winter 2011). p. 36. Katoch states that Admiral Vishnu Bhagwat had recommended the integration of the Special Forces in the nineties.

[2]Stephen P Cohen & Sunil Dasgupta, *Arming Without Aiming-India's Military Modernisation.* (New Delhi: Penguin-Viking, 2010), p xii.

[3]Michael J Neufeld, *The Rocket and the Reich: Peenemünde and the Coming of the Ballistic Missile Era.* (New York: The Free Press, 1995) pp. 158,160–2,190.

[4]Thomas K Adams, , *US Special Operations Forces in Action- The Challenge of Unconventional Warfare.* (London: Frank Cass Publishers, 2001). p.xxv.

[5]Barry. M. Goldwater, with Jack Cassidy, *Goldwater*. (New York : Doubleday, 1988). p. 365.

[6]*Table of Precedence,* President's Secretariat. Available from MHA Website at http://mha.nic.in/hindi/top#. Accessed 01 May 2016.

[7]Helen Caldicott & Craig Eisendrath, *War in the High Heavens-The Arms Race in Outer Space.*(New York: The New Press, 2007) P. 92.

[8]I*nstruments of Statecraft: U.S. Guerilla Warfare, Counterinsurgency, and Counterterrorism, 1940-1990* (New York: Pantheon Books,1992)

[9]The exact strength being classified the numbers are gleaned from sources such as Wikipedia which gives the number of Indian SF and Parachute battalions.

[10]Air Marshal Narayan Menon, " Indian Special Operations capability". *Indian Defence Review.* Vol. 26.3, July – Sept 2011 . Available from http://www.indiandefencereview.com/spotlights/indias-special-operations-capability. Accessed 12 May 2016.

[11]PTI. "IAF to Induct 700 More Garud Commandos". Outlook India 02 Feb 2016. Available from http://www.outlookindia.com/newswire/story/iaf-to-induct-700-more-garud-commandos/929109. Accessed 12 May 2016.

[12]*The Military Balance* 2015. The International Institute for Strategic Studies. (London: Routledge.2015) P. 251.

[13]PC Katoch, op cit . p. 37.

[14]Lt Gen PC Katoch (Retd). Special Operations Command- An Imperative for India. *USI Journal.* Jan-Mar 2016. P. 82

[15]Richard L Draft, *Essentials of Organizational Theory and Design. Mason,* (Ohio: South Western- Thompson Learning, 2003). pp. 38-39.

[16]Susan.L Marquis, *Unconventional Warfare, Rebuilding US Special Operation Forces.* (Washington, Brookings, 1997) P 152.

[17]Area HQs in the Indian Army have a British Army origin. They are akin to a lean Div or Corps HQ. They are responsibly for command of purely administrative units and installations. The author feels that it would be possible to identify area HQs whose area of responsibility can be divided amongst others and which can be spared to be the HQ for the SOD.

[18]Russell F. *Weigley,The American Way of War- A History of United States Military Strategy and Policy.* (Bloomington: Indiana University Press, 1973). p.xxii

Defending Space and Cyberspace

Rear Admiral Vijai S Chaudhari, NM (Retd)[1]

> "The security environment of the future, both in peacetime and during armed conflict, will feature increased threats from offensive cyber and space-based capabilities. . . State and non-state actors now have ready access to highly capable and technologically advanced tools to target others through internet-connected systems and we are seeing greater use of offensive cyber operations. This trend is likely to continue."
>
> Australian Defence White Paper 2016[2]

The Falklands War (1982) was a watershed in modern warfare, bringing together established as well as quintessentially 'modern' concepts and technologies. Joint Operations, nuclear weapons, computer assisted command and control, satellite communications, nuclear and conventional submarines, and Air Early Warning; all played a part. Also involved were: amphibious operations, special operations, aircraft carriers, mid-air refuelling, electronic countermeasures, satellite reconnaissance, electronic surveillance, anti-ship missiles, ship borne helicopters and anti-missile defence. Even a reported cyber-attack, the pioneering use of 'codes' to disable Argentina's Exocet missiles.[3] Thus the war was not only about diverse technologies but also about creating an archetype for late 20th Century warfare. Eventually, a significant outcome of the war had little to do with high-tech. With the Falklands War 'come-as- you-are wars' had come of age.

Even before the Falklands, the Arab-Israeli War of 1973 was a vivid example of the speed and lethality of modern warfare. Sudden onset of war doesn't just impose a steep initial learning curve, it also shortens the transition from peace to war. This was evident during the Falklands War. On April2, 1982, Argentina overwhelmed a small detachment of Royal Marines and captured the Falklands.The next day; British Prime Minister Margaret Thatcher announced the despatch of a Task Force.

---

[1]Vijai S. Chaudhari is a former Rear Admiral of the Indian Navy and currently Additional Director of the Centre for Joint Warfare Studies (CENJOWS), New Delhi. Views are personal.

[2]Australian Government, Department of Defence, *Defence White Paper 2016,* ISBN: 978-0-9941680-5-4, 51 http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf (accessed May 12, 2016)

[3]Jon Henley, "Thatcher used 'Nuclear Blackmail' to get Missile Codes," The Age, Paris, November 23, 2005. http://www.theage.com.au/news/world/thatcher-used-nuclear-blackmail-to-get-missile-codes/2005/11/22/1132421666102.html (accessed May 14, 2016).

On April, 5 1982, just three days after the British surrender,theTask Force actually sailed from Portsmouth. The force had every intention of conducting operations 6,800 nautical miles away. There were reinforcements but the original Task Force stayed the course. Ultimately, 81days after the surrender, Governor Rex Hunt was once again the Commissioner of the Falklandson June 25, 1982.[4] This quick succession of events only underscored a change that had been in the making for some time. After Falklands, military leaders had to be ready for "come-as-you-are" wars. A long and deliberate mobilisationno longer has an assured place in plans for war. Even India made a concession for this change by formulating a 'Cold Start' doctrine. Cyber and space warfare are late 20th Century developments and come-as-you-are war is part of their DNA. Organisational structures must therefore accommodate the changed realities.

Space warfare is actually 'rocket science'.[5] Cyber war too relies more on creativity and innovation than on conventional military power. Nevertheless, these newcomers have to find their places in the larger epistemology of war. At the same time, new threats are emerging and war itself is changing in significant ways. In fact, as Gregory Copley points out, war has become more closely enmeshed with society than ever before. The forces of globalisation, shifting centres of power, changing vulnerabilities and advances in technology have all contributed to this change. Thus the craft of soldiering has moved beyond the strictly military domain and become a "whole of society" affair.[6] Economic security, cyber security, energy security and water security are only a few of the new concerns in national security calculations. Against this backdrop, armed forces continue to structure, equip and train for short, reactive, intense and structured wars. Unfortunately, the wars actually taking place are protracted and unstructured.[7] The undeclared war over Kashmir, for example, has been raging for seven decades; with no end in sight. This proxy war calls for responses to countless pinpricks rather than a general outbreak of hostilities like the set piece wars of earlier centuries. Variants of this type of warfare are unfolding in Afghanistan and Iraq. These are examples that cyber war might well follow.

Another development is the blurring of boundaries between the strategic and tactical levels. An ill-timed but minor incursion on the border with China has the potential to blunt a major diplomatic initiative that may have been years in the

---

[4]The Falklands Conflict - Chronology of Events, http://www.falklandswar.org.uk/chron.htm (accessed May 10, 2015)

[5]Rocket science: something requiring great intelligence, especially mathematical ability. Dictionary.com, http://www.dictionary.com/browse/rocket-science (accessed May 14, 2016)

[6]Gregory R. Copley, "The Last Legions: Farewell to the Past, it is Time to Prepare for the Future of Conflict,"Defense and Foreign Affairs Reports, March 8, 2010.

[7]Ibid.

making. On the other hand, a strategic move in the South China Sea may well evoke a purely tactical response. Space and cyber operations are part of this changing reality. It would be unwise to approach them with only structures and organisations of the past.

Even as we contemplate a brave new[8] military future, experience from the past continues to be relevant. Not so much as a template for action but in terms of the many lessons learnt and relearnt throughout military history. In this regard, insights from Stefan Possony[9] (noted economist and strategist who conceived the Strategic Defence Initiative)are particularly relevant. He wrote about aviation after World War II. Nevertheless, the deductions he makes about the future of military aviation are useful pointers to the future of operations in space and cyberspace:[10]

- The world is currently going through one of its periodic shifts in security architecture, transitioning from one era to another. This calls for a shift in thinking and a move away from obsolescent security structures.
- Even the most rudimentary weapons can be deadly in the absence of effective countermeasures.
- All threats have the potential to evolve. Developing a countermeasure usually triggers a cycle that leads to a more potent threat. Thus the world is moving towards a future of offensive and defensive actions in space as well as cyberspace.
- The balance between offence and defence continues to shift. An effective deterrent is a good way of neutralising an adversary's offensive capabilities.

Space and cyber war may be relatively recent developments but they are also part of the larger continuum of warfare. An analysis of their similarities and differences with the past would throw up clues about their future course. In both areas, technical developments have far outstripped mankind's ability to overtly deploy these offensive capabilities. If these capabilities have not been deployed more extensively, it is only because of the détente created by corresponding vulnerabilities. However, new and established players are ever more willing to adopt risky strategies that push the envelope in these areas. Thus there is a good chance that in time the détente will fail. Already, there are reports that North Korea may be the first nation to break through the cyber security of international banks.[11]

---

[8]The phrase is taken from the title of Huxley's work of science fiction, giving his vision of the future. Aldous Huxley, Brave New World(Vintage Classics, London, 1994).

[9]Stefan T. Possony, "Strategic Air Power for Dynamic Security,"The Infantry Journal Press, Washington, D.C., 1949.

[10]Copley, ibid.

[11]"N. Korea Could be Linked to Cyber-Attacks on Banks, Security Firm Says,"BBC News, May 27, 2016, http://www.bbc.com/news/world-asia-36394986 (accessed May 29, 2016)

States using cyber weapons to seize wealth is quite a different matter from the now commonplace attacks to acquire state and commercial secrets. Moreover, this takes the world a step closer to more damaging attacks that place infrastructure, the economy, defence capabilities and even human life at risk.

During the Cold War, anti-satellite weapons were the preserve of just USA and Russia. However, horizontal proliferation has now commenced with China demonstrating its prowess in this strategic area.[12] There is some comfort in the fact that anti-satellite weapons require advanced technology that is still beyond the reach of all except a small group of nations. However, this does not prevent threats from both space and cyberspace being a 'clear and present danger'.[13]

Space is the latest in a succession of military game changers such as knights in armour, the longbow, the rifle and the machine gun. Its influence, though, extends far beyond the battlefield. Access to space is already critical for Intelligence, Surveillance and Reconnaissance (ISR) besides navigation and communications. Network Centric Operations too are largely dependent on reliable access to satellite links. This is in addition to the huge social and economic dependence on satellites for a host of applications. Common applications include communications, Command and Control, networking, navigation, Geographic Information Systems, Search and Rescue, and weather forecasting. Unfortunately, the vulnerabilities are just as extensive as the uses.14

Today's space systems have evolved in an era when their main role was strategic and war in space was unlikely. This gave rise to a host of vulnerabilities. Most satellites are at least partially hardened against Electro Magnetic Pulse because of high levels of ambient radiation in space. Satellites can also be made difficult to target by raising or changing orbits; use of stealth technologies; radar, laser or IR countermeasures; greater redundancy and by using decoys. However, satellites remain vulnerable to disruption, explosions and direct impact.

At the low end of the threat spectrum, even tiny pieces of space debris have the potential to cripple a satellite. Disruption is another option. Relatively low cost satellite communications jammers are available for sale on the internet. Regardless of the cause, loss of a satellite can be a major setback because of the way satellites are designed. Firstly, putting a payload into space is expensive. Launch weight is

---

[12]"ASAT Weapons Program with Chinese Characteristics," The Council for Strategic Affairs, New Delhi, November 23, 2015,

http://councilforstrategicaffairs.blogspot.com/2015/11/asat-weapons-program-with-chinese_23.html (accessed May 28, 2016)

[13]Title of a 1994 film based on a story by Tom Clancy.

[14]Ellen Pawlikoksi, Doug Loverro and Tom Cristler, "Space- Disruptive Challenges, New Opportunities, and New Strategies,"Strategic Studies Quarterly, Spring 2012, http://www.au.af.mil/au/ssq/2012/spring/pawlikowski.pdf (accessed May 9, 2016).

therefore at a premium. Secondly, satellite capability per kilogram is proportional to the overall weight of the satellite. This economy of scale makes it attractive to build larger satellites crammed with as much capability as possible. With large capabilities concentrated in individual satellites, loss of a single satellite can be catastrophic. Moreover, navigation satellites work as part of a constellation. Loss of a single satellite can therefore seriously degrade the entire system. This makes space a centre of gravity that supports many critical military capabilities. Spreading some capabilities across commercial satellites is at best a partial solution that also spreads the risk to non-military users.

The high-technology threat to space systems takes various forms that include:

- Direct ascent anti-satellite missiles, short-duration co-orbital interceptors and long-duration orbital interceptors
- Stand Off Weapons such as lasers, radio frequency jammers and particle-beam weapons
- Electronic attack on communications, data and command links
- Non-directed nuclear weapons

An effective deterrent could counter anti-satellite weapons but even that would need to be backed by a robust defensive capability. Until technology for satellite defence matures, there are two main options. One is to distribute services across a large number of smaller satellites. The other is an ability to quickly replace destroyed satellites. Currently, satellites tend to be purpose built and launchers require extensive pre-launch preparations. Launch on demand is feasible but far from routine. Besides, launch on demand would be feasible only if there are stocks of satellites available for launching off-the-shelf. Limited satellite-launch infrastructure is another constraint. Besides, the infrastructure that exists is often oriented towards civilian requirements. Worldwide, commercial satellite launches exceed military launches by a wide margin and the gap is widening rapidly.[15]

In space, the assets are tangible but in cyberspace there is a lot that is virtual even if there are real-world effects. In many ways the threat is still evolving. Cyberattacks are “a range of activities conducted through the use of information and communications technology (ICT).”[16] Unlike warfare in space, cyberattacks require relatively modest resources that are available to a wide range of actors. In fact, cyberterrorists, cyber thieves, cyber spies, cyber-activists and cyber-warriors

[15]Ibid.

[16]Catherine A. Theohary and John W. Rollins, “Cyberwarfare and Cyberterrorism: In Brief,”Congressional Research Service Report, March 27, 2015.

are just some of the people who use cyberattacks to achieve their ends. Moreover, the ends that they seek are not mutually exclusive. The lines are further blurred by the fact that there are no clear criteria yet "for determining whether a cyberattack is criminal, an act of cyberhactivism, terrorism, or a nation-state's use of force equivalent to an armed attack."[17]

International Law and the Law of Armed Conflict allow for reprisals against armed attack. However, there are no established criteria for equating a cyberattack with an armed attack even when there is loss of life, injury or significant destruction. This complicates the use of kinetic force in response to a cyberattack. The unsettled legal position tempts many actors to push the envelope of cyberattacks. Consequently, cyberspace is anarchic, where incidents span the spectrum from". . . acts of protest and criminality all the way to invasions of state sovereignty and deliberate acts of destruction."[18] Attackers are emboldened by the fact that it is difficult to prove that a particular state is responsible. Reacting to this mounting threat, the United States has strengthened its Cyber Command. It plans to establish 40 new CYBERCOM teams of which thirteen will focus on offensive operations. The command itself will consist of three groups that will protect critical infrastructure, support regional military commands and conduct offensive operations.[19]

Ultimately, all significant military powers will move towards ensuring unfettered access to space as well as cyberspace. Setting up new Commands to handle these tasks is the default military option. It has the advantage of providing a standard organisational template and the welcome benefit of additional senior positions. However, the new realities have introduced some additional factors:

- Both space and cyber warfare rely on small numbers of highly specialised technical personnel. Military organisations often face challenges in attracting, training, motivating and retaining such people.
- Career management and retention of small cadres of highly specialised personnel poses additional challenges.
- Defending cyberspace requires a continuous stream of people with new skills and fresh ideas. Currency of these skills and ideas can be very short. This requirement is at odds with personal goals of many career military personnel.
- Space warfare will require 'rocket scientists' with higher education and extensive experience. On the other hand, cyber warfare requires advanced skills that

[17]Ibid.

[18]Trefor Moss, "Is Cyber War the new Cold War?,"The Diplomat,April 19, 2013, http://thediplomat.com/2013/04/is-cyber-war-the-new-cold-war/ (accessed May 14, 2016).

[19]Ibid.

may be highly perishable. This could make it difficult to meet military career requirements.

- Both space and cyber warfare can be waged from centralised facilities far removed from the actual military action. This shift could downplay the role of traditional military virtues among these warfare communities.
- Given the increasing reliance on space and cyberspace, each Armed Force will require some integral capabilities in these areas. At the same time, certain capabilities like satellite launch and control facilities will be difficult to replicate.
- Space and cyber warfare will be come-as-you-are wars allowing little time for mobilisation, training or re-equipping. This will require a permanent organisation that is fully integrated with the end-user as well as the civilian and commercial support base.
- Space and cyber warfare have implications far beyond the military domain with critical applications in almost every segment of society. Military defence of space and the cyberspace therefore cannot be conducted in isolation

A proven organisational model for defending space and the cyberspace already exists. Moreover, it does not involve creation of independent operational commands on conventional lines. Medical services for the Armed Forces are provided by a common organisation. Recruitment, training and cadre management are centralised. Personnel rely on highly specialised knowledge that is constantly expanding. Each Service has complete ownership of its medical facilities. These can be scaled up or down to meet actual requirements. The organisation relies on knowledge, facilities and expertise that are spread across the military and civilian spheres. At the same time it remains fully responsive and accountable to local commanders.

While the model for providing medical services has many advantages, it can be improved upon in certain areas. Space and cyber warfare will be heavily dependent on continuous research, highly specialised skills, innovation and a steady supply of fresh ideas. These may not always be available in sufficient quantities within the Armed Forces. Hence there will be a continuous requirement to tap the larger national talent pool existing in academia, research institutes and industry. This requirement could be met by adopting some aspects from the structure of the US Defense Advanced Research Projects Agency (DARPA). A small administrative and project management team could coordinate the efforts of specialists and researchers contracted for specific projects.

To sum up, the need for dedicated organisations responsible for space and cyber warfare is manifest. However, following conventional wisdom and setting up

independent operational commands is not the only option. In view of changing realities it would be prudent to explore additional options for defending space and cyberspace.

Fig. 1.KAL's Cartoon, The Economist, May 7, 2009.

A Comprehensive National Cyber Force Structure for India

Brigadier (Dr.) Rajeev Bhutani (Retd)*

Absract

India has become increasingly vulnerable to cyber attacks. Cyber targets can be found not only within the military sphere but also in the economic, commercial, environmental and social arenas. Inadequate cyber security and loss of valuable data will inflict considerable damage to Indian national security. While the United States and China had established their 'Cyber Commands' way back in 2010 and are vigorously refining their cyber war fighting techniques, India has yet to take a decision for establishing its own cyber command. A comprehensive national cyber force structure with 'Cyber Command' at the apex will not only allow the Indian armed forces to gear up for cyber war fighting and win a network centric war but will also enable synergy with other national agencies / organizations using the cyberspace thereby providing holistic cyber security to the national assets.

Introduction

Cyberspace is being viewed as the 'fifth battle space', alongside the more traditional arenas of land, air, sea and space. Cyberspace and cyber warfare offer unparalleled opportunities to military, because modern societies rely deeply on networks and digital infrastructure, and moving warfare in cyberspace would give rise to new kinds of threats and new kinds of attacks. Just like the tools of conventional warfare, cyber technology can be used to attack the machinery of state, financial institutions, the national energy and transport infrastructure, social media and public morale. While some actions may appear aggressive and warlike, they may not necessarily be classified as acts of war. Therefore, it is pertinent to distinguish between warfare and non-warfare in cyberspace. For example, the cyber actions of terrorist groups and organized criminals can be harmful and appear aggressive but they do not in themselves necessarily constitute acts of warfare.

The most distinctive feature of cyber warfare is the rapidity with which threats can evolve. William J. Lynn III, the U.S. Deputy Director of Defense had rightly stated *"In the cyber world, the speed of attacks will require even swifter and more coordinated responses. Aircraft can cross the oceans in hours, missiles in minutes.*

But cyber attacks strike in milli-seconds. Cyber also disregards traditional notions of sovereignty."1

A military strategy alone is not sufficient to acquire a holistic understanding of cyber concepts. The civil sphere is using cyberspace at least as much as the military; the entire globalized economy relies on cyberspace and every digitalized nation has computerized its vital infrastructure. India has the second-largest Internet user base in the world, behind only China (402 million Vs. 600 million subscribers).2 Continuing with the past trends of cyber attacks, it is expected that the integrity of India's cyber platforms will increasingly be jeopardized and suffer vulnerabilities in the future.

The direct consequence of this strong digital dependence is that the government has to provide cyber security to the whole nation to protect its national and economic interests. The aim of this paper is to explore a Comprehensive National Cyber Force Structure for India with special emphasis on the 'Cyber Command' at the apex and a multi-disciplinary Cyber workforce covering the entire nation to meet its political objectives. To achieve that aim, this paper addresses five objectives:

First, Characterize the cyber security problem in terms of threats and challenges;
Second, Identify Cyber force structure needs;
Third, Study Cyber force structure of other countries;
Fourth, Study current cyber capabilities of the country and key initiatives being pursued;
Fifth, Identify a Comprehensive National Cyber Force Structure for India.

Cyber Security Problem: Threats and Challenges

The character of conflict in cyberspace is as diverse as the actors who exploit it, the actions they take and the targets they attack. Cyber targets can be found not only within the military sphere but also in the economic, commercial, environmental and social arenas. Cyber threats may be categorized into four domains: Cyber espionage, cyber warfare, cyber terrorism and cyber crime. In recent years, India has been the target of cyber intrusions that appeared to have originated in the PRC. In May 2008, Chinese hackers allegedly broke into the Indian Ministry of External Affairs' internal communication network.3 Not long back, Chinese hackers are known to have used social networking sites to break into the computer networks of the Indian defence establishment and among the institutions targeted were the National Security Council Secretariat, 21 Mountain Artillery Brigade based in Northeast Sector and Air Force Station in New Delhi.4 According to 'Norton Cyber Crime Report 2012', India has 42 million cyber crime victims every year and in 2012 estimated financial loss was US $8 billion in case of India whereas the global bill was US $110 billion.5 According to a recent "Cyber crime survey report 2015" by KPMG, nearly 72 percent of Indian companies faced cyber attacks in

2015.6 Fire Eye, a Nasdaq-listed US-based cyber security firm, which had been observing 'spear phishing activities' of advanced persistent threat (APT) group (believed to be based in China) since 2011, revealed that over the past four years, this threat group has targeted over 100 victims, approximately 70 percent of which were in India. Fire Eye Chief technology officer for Asia Pacific Bryce Boland said, "Collecting intelligence on India remains a key strategic goal for China-based APT groups and these attacks on India and its neighbouring countries reflect growing interests in its foreign affairs". The attacks were also detected in April 2015, about a month ahead of Indian Prime Minister Narendra Modi's first state visit to China7.

According to Symantec's Internal Security Threat Report (ISTR), India was ranked second on a list of nations that were most targeted by cyber criminals through social media in 2014, following the United States. Even Indian Computer Emergency Response Team's (ICERT-in) report showed that the total number of security breach incidents including phishing, virus/malicious code, network scanning/ probing, spam, spread of malware through website compromise for the month of January 2015 was 8,311 up from 5987 incidents in November 2014. In addition, a total of 2,224 Indian websites were defaced in January 2015, compared to 1256 in November 20148.

Inadequate cyber security and loss of valuable data will inflict considerable damage to Indian national security. India's strategic challenge in cyberspace emanates not just from external threats but is exacerbated by its rapidly increasing digital ecosystem. A Comprehensive National Cyber Force Structure with 'Cyber Command' at the apex will not only allow the Indian armed forces to gear up for cyber war fighting and win a network centric war but will also enable synergy with other national agencies / organizations using the cyberspace thereby providing holistic cyber security to the national assets.

Cyber Force Structure Needs

For evolving the cyber force structure, it is essential to identify the key needs that drive the cyber force. Four key areas are identified which constitute the cyber domain: Cyberspace, Cyber power, Cyber strategy and the institutional factors that affect the cyber domain e.g. legal, governance, organization (See Figure 1).9 Numerous definitions of cyberspace exist. For the US Department of Defence, "Cyberspace is a domain characterized by the use of computers and other electronic devices to store, modify and exchange data via networked systems and associated physical infrastructures".10 According to one widely used definition, "Cyber power" is "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power".11 In this context, the instruments of power include the elements of the Political / Diplomatic, Informational, Military and Economic. Its strategic purpose revolves around the ability in peace and war to manipulate perceptions of the strategic environment to

one's advantage, while at the same time degrading the ability of an adversary to comprehend that same environment. Transforming the effects of cyber power into policy objectives is the art and science of strategy.12 The term "Cyber strategy" is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power".13 These key areas or needs are linked by the institutional factors such as governance, legal, organizational and public-private relationships.

Further intellectual capital will be required for each of these areas:

- In the area of cyberspace, intellectual capital is required to deal with components of cyberspace through the independent networks of information technology. To meet that need, there is a requirement for highly capable computer scientists, system engineers, system administrators and system-of-system engineers. These positions cannot be filled with recent graduates or novices but require security cleared, highly trained, and competent cadre of cyber security professionals.
- In the area of cyber power, there is a requirement of disciplinary subject matter experts, who are able to assess the impact of the rapid changes in cyberspace on the factors of diplomacy, information, military and economics.
- In the area of cyber strategy, requirement is of subject matter experts, who are conversant with the empowerment of key entities e.g. terrorists, criminals, near-peers. For example, terrorists are being empowered by cyberspace in their ability to perform a variety of key, inter-related functions like recruitment, training, education, raising of resources, planning, command and control of operations as also conduct and influence operations. Advantages of this empowerment include low cost of entry, world-wide reach, sanctuary and the potential to link with transnational criminals.

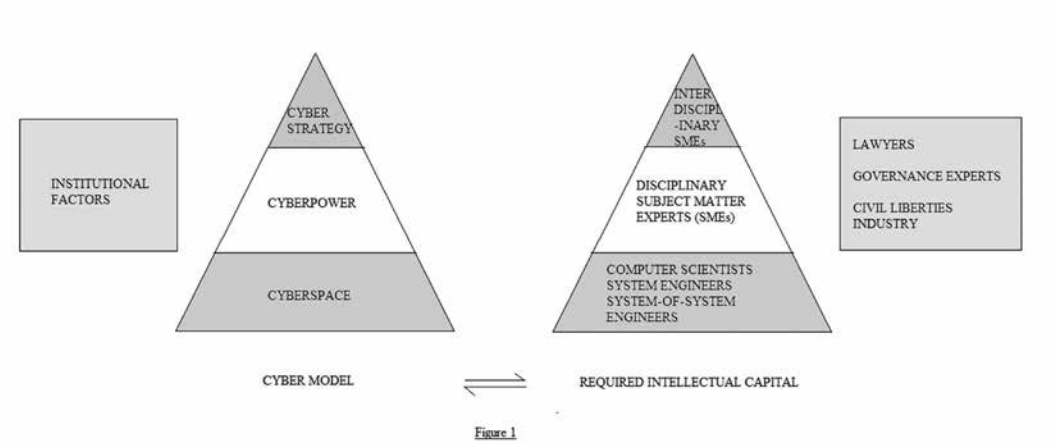


Figure 1

- In the area of institutional factors, legal, governance and private sector experts are required, who are masters in their own fields: lawyers, who are conversant with cyber war and proportional responses, differences in international versus sovereign law; governance experts, who can assess the impact of the new contract with Internet Corporation for Assigned Names and Numbers (ICANN) and the private sector, which controls the majority of the elements of critical infrastructure.14

Cyber Force Structure: Various Countries

Every state in the world now has at least some form of cyber-defence programme, and over 120 states are working on cyber-attack programmes too.15 The rapid creation of cyber units within major militaries of the world is an important indicator of the future use of cyber warfare. The United States had made the biggest public commitment to its cyber war-fighting organization and not to be left behind is the gigantic cyber structure of PRC. Other states which have begun this process are United Kingdom, The Netherlands, Germany, Estonia and Israel. Study of cyber structure of these countries will enable us to draw useful lessons while evolving our own organization.

- The United States. The US Cyber Command (USCYBERCOM), based at Fort Meade, Maryland, about 25 miles North of Washington, was established as a sub unified command of U.S. Strategic Command (STRATCOM) and after several gyrations, it achieved its "full operational capability" in the first week of November 2010.16 It has approximately 1,100 people (military, civilians and contractors). Its key service cyber components are: Army Cyber Command / Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command / Tenth Fleet, and Air Forces Cyber / 24th Air Force. USCYBERCOM operates with several key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The Commander of USCYBERCOM is a four-star General, who also serves as the Director of NSA/Chief CSS, in what is referred to as a "dual-hat" arrangement. Other key mission partners are: Defense Information Systems Agency (DISA), vital to the communications and the efficiency of the entire department; Department of Homeland Security (DHS) and the Department of Justice and Federal Bureau of Investigation (FBI). Further regular interaction is carried out with private industry and key allied nations.[17]

    - In concert with other agencies, the United States' Department of Defense (DoD) is responsible for defending the U.S. homeland and U.S. interests from attack, including attacks that may occur in cyberspace. To this end, the DoD has developed capabilities for cyber operations and is integrating those capabilities into the full array of tools that the United States government uses to defend U.S. national interests, including diplomatic,

informational, military, economic, financial, and law enforcement tools. In April 2015, The Department of Defense Cyber Strategy was released, which has set prioritized strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cyber security and cyber operations.18

- Three Primary Missions in Cyberspace. The Defense Department has three primary cyber missions:
- First, Defend DoD networks, systems and information.
- Second, Defend the U.S. homeland and U.S. national interests against cyber attacks of significant consequence.
- Third, Provide cyber support to military operations and contingency plans.19
- A New Cyber Mission Force (CMF). In 2012, DoD began to build a CMF to carry out DoD's cyber missions. It will be comprised of 6200 cyber operators organized into 133 cyber mission teams, to be fully operational by 2018. These teams will be organized into:
  - ✓ **National Mission Teams (13 Teams).** Defend the United States and its interests against cyber attacks of significant consequence.
  - ✓ **Cyber Protection Teams (68 Teams).** Defend priority DoD networks and systems against priority threats.
  - ✓ **Combat Mission Teams (27 Teams).** Provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations.
  - ✓ **Support Teams (25 Teams).** Provide analytic and planning support to the National Mission and Combat Mission teams.20

The importance being imparted by the U.S. to Cyber Command can be gauged from the fact that in the President Barack Obama's proposed 2014 defense budget, cyber spending grew by $800 million to $4.7 billion while overall Pentagon spending was cut by $3.9 billion.[21]

- **China.** The PRC developed an Information Warfare (IW) strategy a decade ago to leapfrog the technological-military delay they had vis-à-vis the United States. Even though the Chinese do not use the word cyber in their lexicon to qualify the new technologies and rather talk about informatization, one must not be misled here; they are talking about cyber capabilities and cyberspace to wage information warfare.22 On July 19, 2010, the PLA General Staff Department

(GSD) unveiled the country's first ***"Information Support (Assurance) Base"***. Unverified Chinese bulletin board site analyses concluded the base is China's "Cyber Command", tasked to deal with cyber threats and safeguard China's national security.23

It is believed that the PLA's strategic cyber command is situated in the PLA's General Staff Department, specifically its 3rd Department. It is estimated to have 130,000 personnel divided between 12 bureaus, three research institutes, and 16 regional and functional bureaus. Cyber security firm Mandiant, which continues to track dozens of "Advanced Persistent Threat" (APT) groups around the world, has found that the 2nd Bureau of the GSD's 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 is the APT1. APT1 or Unit 61398, located in Pudong New Area of Shanghai, is tasked with computer network operations (CNO) but its nature of work is considered by China to be a state secret. It has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.24 According to Project 2049 Institute (reported in 2011) the Unit 61398 appeared to target the United States and Canada, most likely focusing on political, economic and military-related intelligence.25 This view is not only supported by Mandiant but further reinforced by bringing out that Unit 61398's CNO activities are not limited to the U.S. and Canada, but likely extend to any organization where English is the primary language.26 In June 2014, Crowdstrike, a US cyber security vendor, published a report providing attribution of cyber-attacks to another unit: Chinese PLA, 3rd Department, 12th Bureau, Unit 61486.27

Further, China has a pool of at least 25 million people that have enough education to participate in cyber warfare. Having these many users launch a denial of service (DOS) attack on an adversary could be potentially devastating.28 The size of China's potential force of "cyber warriors" grows even larger when considering China's and the PLA's ongoing cooperation with "cyber criminal" networks. The traditional Chinese criminal organizations or Triads cooperate and compete around the world and are strong in Taiwan and the United States. The criminal networks and apparently the government are allegedly using "Zero Day Exploits" (ZDEs) or software flaws to steal great quantities of valuable information. As ZDEs are often temporary, a large workforce is required to constantly search for more and China is proving to be an ample source of low-cost hackers and software technicians.29 Further China could also carry out cyber attacks or CNO from allied nations.

- **United Kingdom.** The United Kingdom has not moved as quickly towards cyber war fighting as has the United States. At the apex is the UK Defence

Cyber Operations Group (DCOG) which would have become fully operational by March 2015. It will mainstream cyber security throughout the Ministry of Defence and ensure the coherent integration of cyber activities across the spectrum of defence operations. Parallel to this is the Global Operations and Security Control Centre (GOSCC), which is tasked to deliver and assure information and communication services for UK Armed Forces around the clock. Around 200 people work in the GOSCC. Two Joint Cyber units have been established with distinct roles:

- The Joint Cyber Unit (at Corsham) is aimed to proactively and reactively defend MoD networks 24/7 against cyber attacks to enable agile exploitation of MoD information capabilities.
- The Joint Cyber Unit (at Cheltenham) hosted by Government Communications Headquarters (GCHQ), likely to have reached full operational capability by 2015, will have the role of developing new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace.[30]

The DCOG is under the UK's Joint Forces Command and will most likely be more focused on cyber war fighting.[31]

- **Germany.** In Germany, a 60-person CNO group of software experts has been practising for cyber war for years from Tomburg Joint Services Barracks in Rheinbach, near Bonn. The Unit's purpose is to allow the German armed forces, or Bundeswehr, to tackle an enemy via the internet. Operating from German soil, it could penetrate foreign networks using hacker software that is freely available over the internet.32 This unit has been operating since 2006 entirely covertly until the German Government first acknowledged its existence in 2012. The unit reports to the joint forces strategic intelligence command. Germany has also confirmed that it maintains an operational cyber warfare unit with offensive capabilities.33
- T**he Netherlands.** The Dutch Ministry of Defence is establishing a cyber command, which will be responsible for defence, intelligence and attack.34 Its National Cyber security strategy with National Cyber Security Centre (NCSC) at the apex has laid down six priorities:
    1. The establishment of an integral approach.
    2. The strengthening of digital defensibility of the MoD ("defensive").
    3. The development of the military capability to perform cyber operations ("offensive").
    4. The strengthening of the intelligence position in the digital domain ("intelligence").

5. The strengthening of the knowledge position and the innovative power of MoD in the digital domain, including the recruitment and retaining of qualified personnel ("adaptive and innovative").

6. The intensification of the cooperation at the national and international level ("cooperation").35

- **Estonia.** Consequent to the 2007 cyber attacks against Estonia's infrastructure, there had been considerable focus to build up its cyber warfare capabilities. Estonia has established the Estonian Defence League's Cyber Unit, which is a voluntary organization aimed at protecting Estonian cyberspace. The Cyber Unit includes specialists in key cyber security positions, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc.).[36]

India's Current Cyber Capabilities

India's response to cyber threats so far has been reactive and fragmented. India's Department of Electronics and Information Technology (DEITy), under the Ministry of Communication and Information Technology (MCIT) released the country's first ever National Cyber Security Policy (NCSP) on 02 July 2013.37 As regards cyber infrastructure, there are as many as six agencies at the apex level, which are dealing with cyber security management: National Information Board (NIB), National Security Council Secretariat (NSCS), National Crisis Management Committee (NCMC), National Disaster Management Authority (NDMA), National Cyber Response Centre (NCRC), and National Technical Research Organization (NTRO).

Further some more organizations have been planned / formed:

- National Cyber Coordination Centre (NCCC), a multi-agency body is being set up under DEITy at a cost of around Rs 1000 crore, which will carry out real-time assessment of cyber security threats in the country and generate actionable reports / alerts for proactive actions by the concerned agencies.38
- Indian Computer Emergency Response Team (CERT-IN) was formed in January 2004 under MCIT and it was mandated to ensure cyber security of critical infrastructure,39 which was later limited to only non-critical structures. In 2008, the National Critical Information Infrastructure Protection Centre (NCIIPC) was formed under the NTRO and it was mandated to protect critical information infrastructure in the country.40 At the same time, the NDMA which is under Ministry of Home Affairs (MHA) was also assigned responsibility for protection of cyber critical infrastructure.

- Ministry of External Affairs (MEA) also entered into the cyberspace as another coordinating agency. It had coordinated bilateral agreements on cyber security with other countries, for instance the United States.41

- Indian Armed Forces are in the process of establishing a 'Cyber Command' which was confirmed by Shri A K Antony, former defence minister in May 2013.42 Further the Ministry of Defence has mandated the Defence Information Assurance and Research Agency (DIARA) and the DRDO as the nodal cyber security agency for the armed forces.

- **Present Shortcomings.** A detailed analysis of the NCSP and the cyber infrastructure evolved at various levels reveals several shortcomings in addressing our nation's cyber vulnerabilities:-

  - The NCSP essentially laid down a framework for the protection of information in cyberspace by eliminating vulnerabilities but it overlooked several cyber issues as they exist today and failed to incorporate lessons learnt by cyber mature nations. Further, the NCSP-13 was largely the output of deliberations within a single ministry, rather than as part of overall National Security policy.

  - Rather than achieving 'Unity of Command' by having a single authority / organization at the apex to control the nation-wide cyber security, the responsibility of cyberspace security has been split among several ministries, agencies and departments.

  - Agencies have been assigned overlapping responsibilities, for example CERT-In under MCIT, NCIIPC under NTRO, and NDMA under MHA are operating towards the singular objective of securing critical / non-critical infrastructure.

  - Though the lead was taken by DIETy / MCIT in formulating national cyber security policy, this ministry does not have jurisdiction over influential ministries / departments like MoD , MHA and NSCS / NTRO.

  - NIB has become too unwieldy with 21 Secretary level members drawn from the entire spectrum of Indian ministry and bureaucracy.43 It would be an enormous effort to assemble all NIB members together and moreover it would create protracted delay in arriving at decisions.

  - Cyber Command', the essential apex body of a cyber power to win a network centric war has not got its due recognition as the government does not seem to give it a priority.

  - India lags far behind when it comes to official cyber security work force, which comprises a mere 556 experts deployed in various government

agencies. If we compare the figures with China, the US and Russia; China has 1.25 lakh experts, the US 91,080 and Russia 7,300. To strengthen the sector, the government has decided to recruit 4,446 experts to be deployed in six organizations that would take care of India's cyber security infrastructure.44 Incidentally, one of the objectives of NCSP-2013 is to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.45

- As regards funds, the Indian government budgeted just $7.76 million for cyber security in 2013, compared with at least $ 751 million spent by the US government on its cyberspace programmes.46

Comprehensive National Cyber Force Structure for India

If a nation wants to be a great cyber power so as to emerge victorious in future cyberspace conflicts, it must have: a comprehensive national cyber strategy; a 'Cyber Command' at the apex to achieve 'unity of command' of cyber operations and conduct network centric warfare; a professional cyber workforce; develop a cyber culture to have national volunteers in every nook and corner of the country; Coordination and partnership with other organizations – government, public and private sectors; and finally create "international alliances & partnerships".

- **Comprehensive National Cyber Strategy.** There is a need to evolve a comprehensive national cyber strategy, which would define the political objectives, be integrated in the overall national defence strategy and it should focus on: building capabilities for effective cyber security and cyber operations to defend Indian Armed Forces networks, systems and information; defend the nation against cyber attacks; and support operational and contingency plans. To succeed in its missions, the armed forces must operate in partnership with other government departments and organizations, international allies and partners, state governments and most importantly, the private sector.

- **'Cyber Command'.** Just as defending the territorial integrity of India and guarding its overseas national interests whether on land, sea, air, or in space are the sole responsibility of Indian Armed Forces, same way they should be responsible for defending national interests against attacks that may occur in cyberspace, the so-called 'Fifth Domain' of warfare. The United States and China had established their 'cyber commands' way back in 2010 and their cyber workforces are gaining experience to forge ahead for cyber war fighting. Other Western countries like the UK, Germany and the Netherlands have also entrusted this responsibility to their defence forces. There is an urgent need to establish a tri-service 'Cyber Command', which should function directly under the upcoming Chief of Defence Staff / Permanent Chairman, Chiefs of Staff Committee who in turn will be answerable to Cabinet Committee on Security (CCS)/ National Security Council (NSC). It will be headed by a three-star general

from Army/AF/Navy. HQ Cyber Command will have a real-time coordination with NCCC and CERT-In (both under DEITy/MCIT); NCIIPC (under NTRO); NDMA and DRDO; and the private sector. It will have dedicated cyber mission teams distributed under respective service i.e. Army/AF/Navy down to division / AF station / Naval fleet or station level. The mission teams will be categorized according to their dedicated tasks such as cyber defence, cyber attack, support etc. A suggested organization tree is given in the Appendix attached.

- **Cyber Workforce.** To convert the national cyber strategy and plans into operational outcomes, a professional cyber workforce (composed of mission-oriented teams) will have to be created. It needs to be emphasized that normal 'run-of-the-mill' computer graduates will not be able to meet this requirement but a highly trained and competent cadre of cyber security professionals, with a clean security background is the necessity. After selection, these individuals will have to be trained and organized into mission-oriented teams based on their calibre, potential, innovative skill and future employability. A 'cyber warrior' got to have an 'innovative mind' who can transform his techniques to meet the rapidly changing cyber challenges.

- **Cyber Culture.** The cyber workforce alone will not be able to meet the complete requirement of national cyber security as the cyberspace is all encompassing, covering not only military but every sector of modern societies. Rightly so, China's former director of Science & Technology, Beijing Institute of Technology, Huang Chunping claimed that everyone in China is a potential cyber warrior.47 Their cyber war strategy entails recruiting millions of computer users to launch an attack. Though, India is considered as an 'Information Technology' Superpower but it does not seem to have a cyber war fighting culture. Despite having suffered from repeated cyber attacks in the recent past, there does not appear to be an operational urgency to institutionalize a cyber war fighting mechanism. Before, officially declaring establishment of their 'cyber commands' both the United States and China had reportedly practised the cyber war fighting techniques and evaluated their utility values for future employment. The government will take its own time for formally sanctioning the cyber command but it is high time that emergent steps should be taken to evolve a cyber culture at various levels such as colleges/universities; military academies and training institutes; and units / formations:

  - Building up cyber security curriculum in the computer science courses being taught at class XII and college level, will provide the foundation for long-term cyber security. National Cadet Corps (NCC) should have NCC Cyber wings in engineering colleges/ universities on the lines of Army/AF/ Navy wings, where cadets are to be imparted cyber training.

- To create a talent pool of cyber security specialists, competitions should be conducted at national level in the form of 'Cyber Olympiads'/'Ethical Hacking'48, which can be sponsored by Army/AF/Navy. Deserving candidates should be given scholarships and a roster of specialists maintained with their level of achievements; some of them to be absorbed in Services while the remainder to be employed as 'cyber warriors' on voluntary basis in case of national emergency.

- Raising of Territorial Army Battalion (Cyber) should be considered as it will pay great dividends.

- At Indian Military Academy (IMA), Air Force Academy and Naval Academy, cyber security should form part of the academic curriculum taken by all cadets. Every passing out course should have an award for the 'Best Cyber Cadet'. Cadets with excellent cyber aptitude should be posted to technical arms and services.

- The training establishments like Military College of Telecommunication Engineering (MCTE) and their equivalents in Navy/AF should conduct short and long courses in 'Cyber defence' and 'Cyber attack' and qualified officers should be posted to various formation headquarters as per their grades/levels attained.

- All formation headquarters down to divisional level should create 'cyber cells' to be headed by cyber qualified officers and supported by a team of cyber specialists. Once 'Cyber Command' is sanctioned by the government, these trained cyber specialists will be available as a nucleus to form various cyber mission teams.

- **Lateral Partnership with Other Organizations.** Lateral coordination and partnership with other user agencies / organizations of cyberspace should be achieved through real-time networking between the 'Cyber Command' and those agencies and through positioning of liaison officers (LOs), an age-old and proven war-time practice followed by armed forces.

- **International Alliances and Partnerships.** Establishing alliances and partnerships with friendly foreign countries will not only assist in defending against cyber threats but will also contribute towards international security and stability. Bilateral agreements signed with the United States, the UK and Republic of Korea are steps in the right direction.

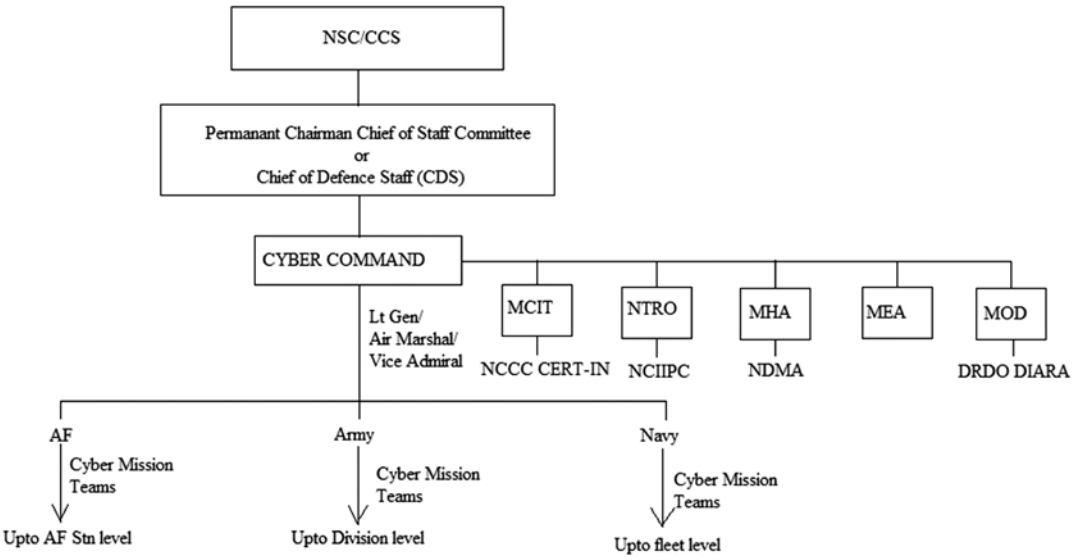
Conclusion

"War is not a mere act of policy but a true political instrument, a continuation of political activity by other means" – Carl von Clausewitz49

With the cyber power being increasingly used as a potent weapon both by state and non-state actors, cyber war fighting has now become a reality. Evolving a cyber security policy and intention to establish a few cyber coordination centres are bureaucratic measures , which cannot conduct and win a network centric war. A fully equipped 'Cyber Command' with its organizational linkages will be the true political instrument enabling the government to achieve its laid down political and strategic objectives in the cyberspace. The US Cyber Command, announced in 2009, achieved its 'full operational capability' as a Headquarters by November 2010 but down to planned cyber mission teams, it will be fully operational by 2018. Any further delay in establishment of 'Cyber Command' in the Indian context, will be at the cost of jeopardizing its national security. It must be remembered that even if a decision is taken now, it may take anywhere between 7 to 10 years for it to become fully operational i.e. somewhere around 2025. However, without awaiting for a formal official declaration to establish 'Cyber Command', necessary steps should be taken to develop cyber culture in the country so that we have a pool of 'cyber warriors' similar to those of China. Realistic nation-wide exercises should also be conducted from time to time to test how cyber security functions in the time of crisis.

*Brigadier (Dr) Rajeev Bhutani is a writer and Defence Analyst.

ORGANISATION: CYBER COMMAND



---

1. Clive Addy, "An Urgency for Cyber Security Leadership – An Interview with the U.S. Deputy Director of Defense, William J. Lynn III", Front Line Security, Vol.5,No.2 (Summer 2010), available at frontline-security.org/index_archives.php?page=384 (accessed on 24 Apr 2016).
2. Neha Alawadhi, "India's internet user base to touch 402 million by December, second largest after China: Report", available at articles.economictimes.indiatimes.com/2015-11-18/news/…user-base/… (accessed on 24 April 2014).
3. Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites", The Times of India, 05 May 2008.
4. Radhakrishna Rao, Visiting Fellow, VIF, 08 December 2012, "Need to Expedite the Creation of an Indian Cyber Command", available at www.vifindia.org/...to-expedite-the-creation-of-an-indian-cyber-command
5. " 2012 Norton Cyber Crime Report" (August 2012) , available at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf (accessed on 7 May 2016) and George Joseph, "India has 42 mn cyber crime victims every year", Business Standard, 24 June 2013, available at , http://www.business-standard.com/article/current-affairs/india-has-42-mn-cyber-crime-victims-every-year-113062400097_1.html (accessed on 7 May 2016)
6. Rica Bhattacharyya, "72% Indian companies faced cyber attack in 2015: KPMG survey", ET Telecom, 30 November 2015, available at, http://telecom.economictimes.indiatimes.com/news/72-indian-companies-faced-cyber-attack-in-2015-kpmg-survey/49984813 (accessed on 7 May 2016)
7. Shivani Shinde Nadhe, "Chinese hackers eye Indian govt, education institutes", Business Standard, 21 August 2015, available at http://www.business-standard.com/article/current-affairs/chinese-hackers-eye-indian-govt-education-institutes-115082100223_1.html (accessed on 14 May 2016)
8. Shivani Shinde Nadhe, "India, a soft target for cyber criminals: Study", Business Standard, 9 May 2015, available at http://www.business-standard.com/article/current-affairs/india-a-soft-target-for-cyber-criminals-symantec-115050900513_1.html (accessed on 14 May 2016)

9. Stuart Starr, Daniel Kuehl, Terry Pudas, "Perspectives on Building a Cyber Force Structure", in Christian Czosseck and Karlis Podins (eds.), "Conference on Cyber Conflict Proceedings 2010", pp.165-166, available at https://ccdcoe.org/sites/default/files/multimedia/pdf/Proceedings2010(FullBook).pdf

10. Joint Chiefs of Staff, "Joint Publication 1-02", Washington D.C., U S Department of Defense, 12 April 2001.

11. Daniel T. Kuehl, "From Cyberspace to Cyber power: Defining the Problem", in Franklin D. Kramer, Stuart Starr and Larry K. Wentz, eds., "Cyber power and National Security", Washington D.C., National Defense University Press, Potomac Books, 2009, p.38.

12. Everett C. Dolman, "Pure Strategy: Power and Principle in the Space and Information Age", London, Frank Cass, 2005, p.6.

13. Stuart Starr et.al, op.cit. p.167.

14. Ibid. pp 167-168.

15. James A. Green (ed.), "Cyber Warfare – A multidisciplinary analysis", Routledge, New York, 2016, p.3.

16. Mike Lennon, "Cyber Command (CYBERCOM) Reaches Full Operational Capability", Security Week. Com, 04 November 2010, available at http://www.securityweek.com/cyber-command-cybercom-reaches-full-operational-capability (accessed on 01 May 2016)

17. Admiral Michael S. Rogers, Commander USCYBERCOM, "Statement Before the House Committee on Armed Services", 4 March 2015, pp1-2. available at http://armedservices.house.gov/index.cfm/2015/3/cyber-operations-improving-the-military-cyber-security-posture-in-an-uncertain-threat-environment (accessed on 30 April 2016)

18. The Department of Defense Cyber Strategy April 2015, pp.2-3. available at http://www.defense.gov/Portals/1/features/2015/0415_cyber_strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed on 30 April 2016)

19. The Department of Defense Cyber Strategy, available at http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy (accessed on 01 May 2016)

20. Ibid.

21. Warren Strobel and Deborah Charles, "With troops and techies, U.S. prepares for cyber warfare", Reuters, 7 June 2013 available at http://www.reuters.com/article/us-usa-cyberwar-idUSBRE95608D20130607

22. Vincent Joubert, "Getting the Essence of Cyberspace; A Theoretical Framework to face Cyber Issues", p.119 in Christian Czosseck and Karlis Podins (eds.), "Conference on Cyber Conflict Proceedings 2010", 15-18 June 2010, Tallinn, Estonia available at https://ccdcoe.org/sites/default/files/multimedia/pdf/Proceedings2010(FullBook).pdf

23. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure", Project 2049 Institute, 11 November 2011, p.2. available at http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

24. Mandiant, "APT1: Exposing one of China's cyber espionage units", Mandiant Publication [online], pp. 3-9, available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

25. Mark A. Stokes, et.al., (Project 2049 Institute), op.cit. p.8.

26. Mandiant, op.cit., p.9.

27. N. Hartley, "Hat-tribution to PLA Unit 61486", 9 June, Crowd Strike Blog [online], available at www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/

28. Steve Elwart, "China's 'Cyber Army' could number half billion", 01/08/2012 in www.wnd.com/2012/01/chinas-cyberarmy-could-number-half-billion/

29. James Dunnigan, "China Attacks, No One Notices", StrategyPage.com, 23 January 2006, available at http://www.strategypage.com/htmw/htecm/articles/20060123.aspx and James Dunnigan, "Chinese Cyber War Munitions Factories", Strategy Page.com, 31 July 2006 available at http://www.strategypage.com/htmw/htiw/articles/20060731.aspx

30. Parliamentary Session (2012-13), "hc 106 Defence and Cyber-Security" Supplementary written evidence from the Ministry of Defence following the private evidence session on 18 April 2012, available at http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm

31. Richard Stiennon, "A short history of cyber warfare", pp 25-26.in James A. Green (ed.), "Cyber Warfare – A multidisciplinary analysis", Routledge, New York, 2016.

32. Michael Fischer, "German armed forces equipping for cyber war", Stars and Stripes, 22 May 2013, available at http://www.stripes.com/news/europe/german-armed-forces- equipping-for-cyber-war-1.222156 (accessed on 5 May 2016)

33. John Leyden, "Germany reveals secret techie soldier unit, new cyber weapons", The Register, 08 June 2012, available at http://www.Theregister.co.uk/2012/06/08/ germany_cyber_offensive_capability/

34. Richard Stiennon, op.cit., p.26.

35. Matthijs.R. Koot, "The Dutch Defense Cyber Strategy of 2012", translation, 18 July 2012, blog available at https://blog.cyberwar.nl/2012/07/nl-uk- translation-of- the-dutch-defense- cyber-strategy/

36. Kaitseliit, 2014, "Estonian Defense League's Cyber Unit", available at http://www.kaitseliit.ee/en/cyber-unit

37. Notification on National Cyber Security Policy – 2013 (NCSP-2013) available at http://deity.gov.in/content/national-cyber-security-policy-2013-1 (accessed on 10 May 2016)

38. Sandeep Joshi, "India gets ready to roll out cyber snooping agency", The Hindu 10 June 2013 available at http://www.thehindu.com/news/national/india-gets-ready-to-roll-out- cyber-snooping-agency/article4798049.ece?homepage=true

39. "Indian Computer Emergency Response Team", http://cert-in.org.in/ (accessed on 10 May 2016)

40. NCSP-2013, op.cit., p.7.

41. "India-US Cyber Security Forum – Fact Sheet", 02 March 2006 available at http://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet

42. "Cyber command will be formed soon: Antony", The Hindu 25 May 2013, available at http://www.thehindu.com/news/national/kerala/cyber-command-will-be-formed-soon- antony/article4750061.ece,

43. V.Singh, 26 August 2013, "Point out the function of National Information Board in Cyber Security", http://www.preservearticles.com/2012032027854/point-out-the-function-of-national-information-board-in-cyber-security.html

44. "Fact Box: India far behind in cyber security compared to US and China", 23June 2013 available at http://currentaffairs.gktoday.in/india-cyber-security-compared-china-0620137136.html

45. NCSP-2013, op.cit., p.4.

46. Amit R. Saksena, "India Scrambles on Cyber Security", The Diplomat, 18 June 2014, available at http://thediplomat.com/2014/06/india-scrambles-on- cyber-security/

47. Steve Elwart, op.cit.

48. Stuart Starr et.al, op.cit., p.177.

49. Michael Howard / Peter Paret translation of Carl von Clausewitz, "On War", pp75-89. Available at http://www.clausewitz.com/readings/Cquotations.htm

Joint Capability – In India it is a Mere Thought Process

Air Marshal Dhiraj Kukreja, PVSM, AVSM, VSM (Retd)*

Introduction

The established concept of national security has undergone a change. No longer is national security restricted to protecting one's own borders from external aggression. Globalisation has 'globalised' the security imperatives of almost all nations beyond their geographical boundaries. The challenges faced by any country today are complex and disquieting, and are increasing with the passage of time. The emerging paradigms can at best be categorised under the following broad heads: traditional, asymmetric, disruptive, weapons of mass destruction, and natural disasters.

In the wars of the future that are likely to be 'short and swift', high intensity conflict may be short-lived but low intensity conflict can continue for a very long time, sapping the energy and resources of any military force. Insurgency and infiltration tactics swing wildly between intense force and tempo, to moderate force and tempo, providing asymmetrical and unpredictable warfare. In order to be successful under such demanding conditions, inputs from all intelligence agencies and the armed forces need to have a textbook coordination to have a holistic appreciation of the threat scenario. Such coordination will assist the commanders to continuously assess the progress of operations and eliminate the threat, even as it evolves. Given the dynamic nature of the threat, the employment of all available assets, irrespective of the ownership - army, air force or the navy, or any other agency - would need a regular review to ensure their effectiveness in repeated usage.

For India, a developing country, resources will always be limited. The available resources, as also the new assets, yet under procurement, would have to be balanced between force projection, force protection, and enabling capabilities. For a successful change in the thinking of utilisation of assets, the overall war-fighting machinery would also have to undergo a doctrinal change. This would have to start at the highest level and perforce filter down to the lowest tactical level. These changes need careful tracking for a meaningful interpretation and for a general benefit of all.

During the introduction of his proposal for the Defence Re-organisation Act of 1958, President Dwight Eisenhower of the United States had said, “Separate ground, sea, and air warfare is gone forever. If ever again we should be involved in war, we will fight it in all elements, with all services, as one single concentrated effort. Peacetime preparatory and organisational activity must conform to this fact.” Other dimensions need to be added today, to ‘all elements’, as quoted above, namely that of space, cyber and special operations. Each of these new dimensions can be interlinked to be a part of conventional operations, but can become a separate entity by itself; therefore the need for individual formations to control valuable assets, and yet share them.

Indian Story

For far too long, the debate of wanting, or not wanting a CDS, to promote joint capability in the Indian armed forces, has been going on; hence, repetition of the arguments is not warranted. Suffice it to mention that it all began with the country gaining independence, then went into a lull with brief resurrections, but gathered a momentum after the Kargil War in 1999. The experience in Kargil warned us that future conflicts would undoubtedly necessitate joint operations, besides highlighting the urgent review and re-organisation of the security set up of the country. Post 1999, a comprehensive study by four task forces constituted by the GoI resulted in a report by a Group of Ministers (GOM), which approved the appointment of a Chief of Defence Staff (CDS), among other radical changes. The office of the CDS is yet to be formed, though his deputy, in the HQ Integrated Defence Staff (HQ IDS) has been functional since 2001!

CENJOWS, in its Concept Note for the theme of enhancing joint capability, has rightly highlighted the review of the Kargil operations and the report by the GOM, which spoke of the then existing deficiencies and measures to be taken to rectify them. The creation of the post of a CDS and joint commands - operational, and functional - were the main issues recommended. It is indeed sad to mention that the situation has not much improved since then.

Post the Kargil War, and after the establishment of HQ IDS, further studies have been initiated, at the behest of the GoI. As recently as 2012, a study group consisting of eminent officers from the armed forces and civil services, under the leadership of Shri Naresh Chandra, himself a distinguished and well-respected civil servant, submitted its report to the GoI. Among other suggestions, it recommended the immediate formation of Cyber, Space, and Special Operation Commands and the appointment of a CDS, for these were considered crucial to national security. The in-principle approval was accorded in 2012-13, but the decision has lain in cold storage since then. Circa August 2015, the Raksha Mantri (RM) announced the formation of the commands, instructing HQ IDS to plan the practical details of the basic structure required; there were hopes on the appointment of a CDS too, but these seem to be ‘planted’ stories in the media, with no concrete action seemingly initiated.

Why Joint Capability?

The long experience of the Indian armed forces has been that the three services have more often than not, been working at cross-purposes in matters of integration and unity of command. This is so deeply ingrained into the existing system that it cannot really be removed without a major surgery. For a complete switchover to the system of CDS, under which various components of the each service will be integrated in a joint command to function under a single Commander, the GoI will have to enact a replica of the Goldwater-Nichols Act of USA.

Over the years, there has been opposition to the idea of joint commands and the appointment of a CDS from various sources, both within the armed forces and the bureaucracy of the MoD; the latter often paints a frightening picture of a military take-over, scaring the political executive to place the proposals repeatedly into cold storage! Many a former PM has mentioned that India's areas of interest now extend from the Suez to the Malacca or even beyond to the South China Sea. A learned former defence secretary, is, however, reported to have countered the statements of the political leadership by mentioning that India does not have any global interests and with the military's role being primarily to defend the country's territorial integrity, thus questioning the necessity of a CDS. He knows best, since the defence secretary is responsible for the defence of the nation as per the government's 'Rules of Business'!

The need for joint command and organisational structures cannot be over-emphasised to meet the challenges of the future battlefield, which is likely to be more complex than ever. Modern day wars, as has been seen in the recent past, would involve all the three services, which, in other words, would necessitate the application of integrated military power. In India, the aspect of integration is often confused with cooperation; the difference being subtle, but fundamental. Cooperation means each of the services planning individually, and providing help to the other when asked for. Integration, on the other hand, entails drawing battle plans together, gathering assets from the Services, and then placing them at the disposal of a single Commander for fighting the battle jointly. The effectiveness of such a battle-plan can be possible only if there is integration at the apex level, for only then can it percolate to the lowest level.

The present system of the COSC and individual service commands is not considered suitable for the future wars that the country may have to face. The Chairman of the COSC works only on consensus and has no executive powers to enforce a decision on other Services. To enable the COSC, either a CDS or a permanent Chairman of the COSC needs to be appointed, with the raising of joint operational commands in tandem. The permanent incumbent would then have resources from the three Services, and be the 'single-window' advisor to the political executive. Needless to mention, yet important, such an arrangement has to be combined with

a corresponding reshuffle within the MoD and policies at government levels too, for one without the other is a meaningless exercise.

There are definite benefits that would accrue from the suggested organization, which would go a long way in ensuring practise of best options for national security. Some benefits are listed.

- The CDS would be a provision of a single point comprehensive military advice. This would be available with continuity, as against the present system. Such an arrangement would also ensure pragmatic assessment of threats and planned actions to ward off the threats.

- An integrated planning process would ensure prioritisation and induction in a phased manner, with optimal utilisation of the defence budget. This, in turn, would ensure a cost-effective, systematic development of military capability.

- Decision-making would be a more streamlined process, more so in times of a crisis. The implementation of the decision would be a natural follow through.

- Theatre commands would reduce the number of individual Service Commands, thus cutting out unnecessary flab. In military parlance, with the joint assets, a well-equipped Theatre Command would provide the desired defence posturing with deterrence, so essential in the initial stages of a brewing crisis.

Implementation Complexities

As can be expected, there are apprehensions in the minds of many as to how would this process be implemented. Some of the fears may be real, but many are lackadaisical, just so to bias the entire exercise, make it counter-productive, to eventually lead to a status-quo. There are many models available in the world; India cannot just pick one and follow it blindly. The models have to be adapted to suit our culture and requirements. The US and the British models have been studied in detail and points adopted from them to formulate our own system, with the sensitivity aspect considered.

The actors are the Armed Forces, the bureaucracy, and the political leadership. What are their stakes? The political leadership has to be given due credit of taking the bold step of initiating the reorganisation of the defence and security set up in the country, though not in totality; the GoI stopped short of appointing the CDS for reasons unknown, under the pretext of further discussions. Those discussions are yet continuing! The political leadership, barring for a few, the number can be counted on fingertips, have a sketchy knowledge of military matters. It, hence,

depends heavily on the inputs from the bureaucracy. There seems to be a misplaced anxiety existing in the minds of the politicos that the military could pose a threat to democracy, should it become all-powerful. This mistrust of the military in not new, continuing since independence, and the civil service has placed itself as the self-appointed arbiter in most military matters. The political leadership should appreciate the nuances of national security in today's global, dynamic geo-politics, and take their own decisions.

For 70 years after independence, the bureaucrats and the Armed Forces have viewed each other with disdain and suspicion. In the recent past, the mistrust has only grown. The change of the Armed Forces HQs, as integral departments rather than attached offices in MoD, was a start that unfortunately has remained cosmetic. The initial acceptance for the need of the establishment of a CDS, with delegation of administrative and financial powers could have benefitted the Services, if properly implemented. The process of necessity will have to be one of 'give and take', if it is not to degenerate into a denying 'one for the other', for the military or the bureaucracy. The fear of the bureaucracy of being rendered redundant, should the Armed Forces be involved in decision making in national security at the macro level, is totally unfounded and misplaced. Thus, they are keen to maintain status quo, and keep the military 'in its place'.

The man in uniform has also added to the complexities of the implementation of the recommendation. The perennial turf battles between the services are historical. The fear of the individual Service in losing out to the "Big Brother" can be detrimental to the very beginning of the implementation progression. It is, perhaps, these persistent territorial battles between the Services, all related to the fear of losing the traditional roles and missions that would have prompted the Prime Minister to thus address the Commanders during the Combined Conference in 2011: *"The Government will never fight shy of finding the funds for the modernization of our forces. At the same time, we have to recognize that resources are not unlimited. I would urge upon you to optimize the use of scarce resources. You are the best judge of how this can be done, but advance and long term planning and the creation of common institutions, communication networks, and infrastructure are some examples of how this could be achieved. We should keep this in mind particularly when we build new capacities for meeting emerging threats."*

In the implementation process there are many opportunities and safeguards for each player to protect own interests. The fear of losing out while implementing something new and untried, is natural. These fears have to be overcome to progress with the process, with the decided path to be additive and developmental rather than radical. Moving a step at a time, learning from mistakes and experiences of others and own, the process of implementation should be such that each Force, the civil service, and the nation derives the maximum from it.

The Way Ahead

What is then the way ahead to establish true integration amongst the three Services and with the MoD? The solution lies in the establishment of a proper command and control structure, a joint approach towards prioritisation in acquisitions, understanding the domain expertise of the other Services, a refurbishment of joint training, followed by a relook of the human resource development. It has to be understood by all parties that the suggested revamping of the various departments has to be with full authority and accountability.

The recommendation of the appointment of a CDS, or whatever name, is a step forward. The incumbent, with a fixed tenure, should have overriding powers to decide on prioritisation in budgeting of plans and procurements for all the three Services. A natural follow-through would then be the setting up of Joint Service Commands, or Theatre Commands, and domain Commands, to cater for cyber, space, and special operations.

The main stakeholders being the three Services, may not find the suggestions palatable; the Service HQ would then be tasked to formulate individual service training, maintenance infrastructure, and procurement plans, but not plan for any operations. Not just the three Services, the Government, and the bureaucracy in MoD too, may not want to hand over such wide-ranging powers to a single entity. As a beginning, along with the CDS, it may be more acceptable to have function-specific commanders, namely cyber, space, and special operations, as templates already exist.

There is also an immediate step to be taken by the three Services. For too long each Service has been making plans in isolation of the others. HQ IDS has now replaced the arbiters in the MoD, who had little or no domain knowledge of military matters, roles and missions, and weapon systems. The bedrock of planning, however, continues to be subjective and the turf wars are not likely to end soon. The three Services need to resolve, once and for all, the differences between themselves; this would be a prudent and a constructive way forward. Appreciation of the benefits of joint functional commands, Theatre Commands, and reorganizational concepts such as the CDS and Joint Forces Commander, will then dawn on the Services if the ghost of ‘roles and missions’ is exorcised.

Concluding Thoughts

Formation of functional commands and Theatre Commands, an understanding of the importance of domain expertise and an impetus to joint training and other HR aspects, will promote closer interaction and an understanding of the distinctive characteristics amongst the three Services. The essence of true integration lies not in merely creating new organisations, but more importantly, in breaking mind-

sets. This is, in fact, the very first step, and like for a child, the most difficult. While the colour of the uniform may vary, as per one's expertise, the colour of the heart must be purple.

In India, the concept of a CDS has had an irksome and a meandering record of accomplishment, a prime reason that we find ourselves in this discordant situation. Services need to look beyond inter-service rivalries that result in the political executive to make disparaging remarks in public forums in India, projecting a very poor image of the Armed Forces leadership.

No nation that seeks greatness can afford to neglect long-term defence planning. Consistently lumbering our way through crises, dents a nation's deterrence and compromises its ability to join other great powers as an equal. India - the military, bureaucracy, and the politicos - needs to understand this and move ahead to optimise its strategic potential to shape the asymmetric battlefield in its favour.

The Defence Minister in August 2015 has recommended the formation of the CDS and three functional commands. This is a God-sent opportunity for the re-organisation of the higher defence management process. It is a small step forward, but knowing the tardy working of the Indian system, the wait is likely to be long.

*Air Marshal Dhiraj Kukreja is a former AOC-in-C of IAF Training Command

Proposed Role and Organizational Structure of Cyber Command and Cyber Operations Units

Brig Navjot Singh*
Prof (Dr) Sanjeev Bansal**

Introduction

Pursuant to the recommendation of the Naresh Chandra Task Force **(NCTF**) in 2002, the raising of the Cyber command is a national security imperative to counter future threats and challenges and to safeguard our national interest and assets. It is understood that due to the strategic importance, reach and impact of this potent force, the Cyber Command would be required to report to the Chairman COSC and would rightly be part of the Tri-Services Headquarters, ie Headquarters Integrated Defence **(HQ IDS)**. Accordingly it will draw assets and manpower from the three services, as well as from other relevant government departments/ organisatons dealing with Cyber Security.

Though the process for the approval for creation of the Cyber Command or Defence Cyber Agency **(DCA)**, would be under deliberation, but if the latter is being considered then it is at best an interim arrangement till the full-fledged Cyber Command is raised and becomes operational. The ideal route to follow would be to upgrade and expand the existing Defence Information Assurance and Research Agency **(DIARA)** into the DCA. The mandarins/ wise men in South Block would have deliberated at length on the organisational structure and manning norms of the agency. However it is more pertinent to appreciate and understand as what is to be expected from the Cyber Command and from the various Cyber Operations units planned to be raised. This paper attempts to provide a broad overview in this direction.

Requirement for a Cyber Command

The need to raise a Cyber Command capability must be understood. Since time immemorial, the saying that *'Necessity is the mother of invention'*, has stood true and stands validated. Most of the developments that have taken place in the world have been on account of realisation and appreciation of the requirement for a particular technological innovation/ development. Practically speaking, a large number of old aged parents, who had never touched computers, quickly

learnt how to chat, send e-mails, and do video call, in order to stay connected with their children who had gone abroad. Likewise it is imperative to appreciate the proposed role and potential of a Cyber Force, which will enable us to comprehend its significance, which in turn will pave the way for willingness in creation of a Cyber Command.

A Cyber weapon is equal to and is comparable to a potent conventional weapon. It however needs to be understood that its potential and employability is very vast and transcends national/ international boundaries. The cost involved in developing and nurturing a cyber weapon and cyber task force is much less, than would be required for developing and maintaining a nuclear arsenal. In the present day context of a world sans digital boundaries and where bulk of the transactions are being done in the digital domain, it is imperative that we have a credible Cyber force to safeguard our national interests.

Known Cyber Warfare Capabilities of Few Prominent Nations

Discussed below are the known Cyber capabilities of few prominent nations. The proposed cyber capability for our nation has been modelled on what is being followed in the other developed nations. As such, the significance/ relevance with reference to the Indian context, where applicable has been brought out.

China. It has an established PLA Cyber Command & Strategic support Force. 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 Philosphy, Electronic Warfare **(EW)** and Cyber Network Attack **(CNN)** 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. There are seven military provinces of China and 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)** have been rumoured to have been developed (e.g. Titan rain, Aurora etc.)

Russia. The Russian Cyber Command and Cyber Warrior Programme exploiting GONGO (Government Organisation NGO i.e. Nasli & the Russian Business Network) should make available a potent Cyber force of at least 5000 persons.

Israel. It has a Separate Cyber Arm called ‘Unit 8200’, with a known strength of approximately 300 persons, with diverse and highly specialised skill sets.

Pakistan. It was the first nation to invent Malwares in 1986 and it’s skills in that field have only increased since then.

USA. USA follows a system of Cyber Mission Teams, totaling 133 in No's which are discussed at length subsequently.

India. It is in comparison to all these that India needs to put in place a credible Cyber Force. As on date the force available with India needs to be considerably augmented.

Cyber Warfare Capability of USA with Relevance to the Indian Context

A typical coherent Cyber Operations Command will not be a classical Theatre Force Command. Instead it will entail the availability of various diverse types of Cyber Mission Teams **(CMT's)**. As per literature available in the 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 which is roughly equal to Six Infantry Batallions. 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 are relevant even in the Indian context and the role and tasking, as listed against each is equally applicable in the Indian subcontinent and the parallels with the existing Cyber organizations in the nation have been drawn. None of these teams can however work in isolation and the same needs to be understood. These five types of teams have been deliberated upon in subsequent paragraphs.

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

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 the strategic level, in India.

Combatant Support Team (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.

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.

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.

The number of such cyber Ops teams, being maintained by the USA and divided amongst the three Armed Forces is as given below :-

		Army	Air Force	Navy
National Mission Team (NMT)	-	4	4	4
National Support Team (NST)	-	2	2	2
Combatant Support Team (CMT)	-	8	8	8
Combatant Support Team (CST)	-	5	5	5
Cyber Protection Team (CPT)	-	20	20	20
Total	-	**39**	**39**	**39**

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 will be dealt with subsequently.

Limitations and Suggested Remedial Measures

Limitations at Existing Level

In order to move ahead we must first take stock of the limitations/ perceived limitations in this field at various levels. These have been deliberated upon at length. At the Armed Forces Level, there exists no doctrine especially for Cyber Warfare. There is however only an Information Warfare Doctrine. At the national level there is no formal training infrastructure available to impart training in this filed. However of late 'Cert-in, DIARA' and other Cyber security organizations have started conducting a series of short term courses, which equip individuals with the knowledge and skill sets required to comprehend the task at hand. There is no formal sharing of information in this niche field at either the govt or public/ private level. 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 Services 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 Operating System.

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.

Measures to Overcome Limitations

Firstly there is a pressing need to restructure the IW Doctrine in a manner that it recognizes the need for capability development. Secondly, we need to have an organisation in place, not only at the staff level but at the level of functional Cyber units, with well laid out role and tasks. Thirdly, jointness is of paramount importance in this field. There are as it is very few persons who have core competency in this field, so we need to pool in resources, synergise and move ahead. Fourthly, there must be synergy in this field between the Academia, Industry and the Government. It should be a healthy self sustaining eco system to nurture development.

Proposed Models for Command and Control of Cyber Command

Having deliberated upon the requirement of Cyber Command, its capabilities and roles, there is a need to analyse various models for command and control of this force and arrive at one model which is suited for our needs. The same has been deliberated upon in this section.

Option 1 : Centralised Control. The control should ideally be centralised at the Cyber Command with operational control being exercised by the Theatre Commands/ Operational Fields Commanders. This has been suggested to enable efficient execution of Cyber Operations at Strategic, Operational & Tactical level. There will be a requirement to have a centralised control at the level of Cyber Command for all Cyber Operations units, because if control is decentralised then there is a possibility that tactical level Ops may trigger off an adverse effect at the strategic level. There will however be a Cyber Coordination Cell at each Command HQ of Army/ AF/ Navy (akin to the model being followed for providing Immediate Air Support by the Air Force to the Army). The Operational field Commander will project their requirement to the Cyber Command through the Cyber Coordination Cell. The Cyber Operation Unit **(COU)** would accordingly be allocated and their requirement would be met. The only **disadvantage** in such a situation is that

the pace of Operations may not be as responsive, as would have been the case if dedicated Cyber Operations Units are placed under command and control of respective field formation headquarters **(HQ's)**.

Option 2 : Allotment on as Reqd Basis. In this scenario the Cyber Command only exercises control over training and recruitment of various Cyber Units. However as regards their employment, various Cyber units are treated as the resource of the Cyber Command and on an as required basis, they are placed temporarily under Command of respective Operational Commands of the three services. Once the cyber units are allocated, the Operational Commander can exert control over their employment. This model provides requisite flexibility for rapid employment and deployment of this critical resource.

Option 3 : Completely Decentralized Model. In this model, the different types of Cyber units are orbatted to various Operational Commands ab-initio. The operational Cyber units are totally amalgamated with Operational forces of various theatre commands. This option is however fraught with the inherent risk of inadvertently triggering off a strategic level impact, by employment of the Cyber Operations units at the tactical/ operational level. A classic example of this misadventure was the identification of a 'Stux Net' type of vulnerability (which happens once in century) and its uncontrolled use. In such a model the inability to the overcome the temptation to use such a weapon for limited tactical gains is the main drawback. It needs to be understood that once a Cyber weapon is fired, there is a capability loss because then the adversary is aware that we are in a position to exploit a known vulnerability and he will develop safeguards against it. A theatre commander is (and should be) worried about the threats in his theatre and might launch a cyber weapon to counter these threats. So in such a scenario, the theatre commander must know the categorisation/ classification of various weapons and when (in which situations) to use them.

Option 4 : Balanced Approach. This is the ideal approach to be followed in such a situation i.e. retain some Cyber Operations Units under Centralised Command, while some could be Orbatted for Operations specific Role (akin to employment of Special Forces). In such a manner, the Army Commander/ Force Commander can dovetail these forces while carrying out his planning. This is required as else the commanders will never factor in this force multiplier in his Operational plan as he would not be aware of its potential and for him it would remain an imaginary/ notional force on paper. In order to ensure total transparency and to avoid an inadvertent use of a strategic Cyber Weapon for limited tactical level gains, there is a need to have in place an over-ride (or Veto) with Cyber Command, to monitor each weapon platform. This will ensure that we do not waste a Strategic level weapon for limited gains.

Suggested Model. Considering all the above factors, the balanced approach model listed above is a model ideally suited in the Indian context. Additional aspects to be kept in mind are that Coordination cells could be created at lower levels i.e. at Corps and Division HQ in the Army and at equivalent HQ's in the Air Force (AF) and Navy. These could be manned by a Principal Staff Officer **(PSO)** of the rank of Colonel and equivalent, who could put in a request for Cyber Capability in support of Operations at the Tactical level at the formation HQ's. Though the size of each Cyber Operations unit will vary between 80 to 100 persons, yet at the level of Corps and below, the activities would be coordinated by the Cyber Coordination Cell comprising of three and four persons. The Cyber Operations could be launched from Command Cyber Operations Room itself. The Cyber Support units will function under the special wing of Cyber Command. Regular interaction with field units through Joint Operation Command (JOC), will be ensured.

Cyber Ops : Factors to be Considered

Certain factors which need to be considered while launching Cyber Operations and employing Cyber Weapons are as discussed in the subsequent paragraphs.

Geographical Independence. Operations can be launched from any part of the world to any remote location as long as network connectivity exists. This considerably eases out the logistics associated with infiltration and extraction of a Special Forces team, for a kinetic kill.

Collatoral Damage. A Cyber weapon is likely to have unintended effect and may end up affecting targets it was not intended to do so. For example the Stux Net virus spread to China and India (which eventually led to it being examined at length and its consequent exposure). These nations were however not the intended prime targets. Thus, this aspect needs to be factored in while employing the cyber weapon.

Degradation of Effect After Use. As explained earlier, once a Cyber Weapon is used, the adversary starts taking measures to mitigate the risk to the known vulnerabilities and will have adequate safeguards in place to deter a re-ocurrance of the same type of exploit.

Strategic effect of Cyber Operations at Tactical Level. The cyber weapon, if intelligently used has the potential to send a message at the strategic level. For eg if a Nuclear reactor detonation of an adversary at a tactical location is effected at controlled speed by use of Cyber Weapons, then the message that is sent out, is at the strategic level and is akin to the message sent out during a controlled nuclear explosion.

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. The bare minimum figure arrived at to man and equip 133 functional Cyber Operations units of the USA, works out to approx 6000 i.e. roughly the strength of two Infantry Brigades. This figure may seem miniscule compared to the 1.2 million strong standing Army that India possesses and it may come as a surprise to many that it is extremely difficult to identify, recruit and train this limited pool of manpower. However the more challenging task is retaining & holding on to the pool of manpower trained in such a niche field. The same is deliberated upon in the succeeding paragraph.

Identification & Recruitment of HR Talent and Few Implications. The people gifted in this field (yes I say 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. Age, experience & seniority may be required to make way for talent – Are we ready for that?

Organisational Structure of Cyber Command

Like all operational commands, the Cyber Command too would be headed by Commander-in-Chief **(C in C)** who would be an Army Cdr equivalent, HAG + serving Armed Forces officer. He would be assisted by a Chief of Staff, again a three star General rank officer from the Armed Forces. Under them there would be five wings, (each headed by a two star General rank serving officers). These are as listed below and are explained in detail in subsequent paragraphs:-

- Joint Operations Centre or **JOC**.
- Offensive Wing.
- Defensive Wing.

- Research & Development (R & D) Wing.
- Administrative (Adm) Wing.

Joint Operations Centre (JOC).

As the name suggests, it is akin to a classical Operations Room. It is from this wing that the Cyber command can exercise strict control over decentralized units. The target Data Base is required to be populated and may be shared between various Cyber Operations units. The Cyber Space to be targeted needs to recced, digitised, mapped and documented for each country/ region intented to be targeted. It is in the Joint Operations centre, that it will be decided as to who will do these tasks. The data base and Cyber Space mapping needs constant updation and responsibility for the same needs to be assigned. The JOC wing will act as an interface with the outside organisation.

Its work of mapping the Cyber Space will be akin to the work being done by CAMS in field of map digitization. There will be a need to have common Data Standards. The JOC wing will ensure that Cyber Operations are more than merely hacking / defacing of websites and entails assured delivery of credible cyber exploits launched through a Cyber Weapons platform.

Role and Capability of JOC. It will be primarily to plan, coordinate & conduct both offensive and defensive Cyber Operations to further the overall objective of the Force Commander. JOC will be heavily committed in planning the conduct of various operations and analysis of the same subsequently. It also needs to ensure preparation, updation and effective utilisation of a comprehensive Data Base, which would be required for launching Cyber operations. The analysis of this wealth of information available in the Data Base can only be carried out by an expert ie a Hacker or a person having domain expertise.

Data Base. This is the heart of the JOC. The Data Base may have been accurately mapped to identify where, which type of server is located, but its only a cyber expert who will be able to comprehend whether this server pertains to vehicular traffic management or Railways or Banking and appreciate the impact of a particular server crashing at different times. It is only the cyber expert who can quantify the effect of a type a server being put out of service, at a given time frame, hence the need for an expert Cyber analyst. These domain experts will not be housed merely in the Cyber Command but will be allocated to different theatres for supporting Operations. Moreover the real challenge is that so many Subject Matter Experts are not readily available. In addition, there is a need to identify language specialists and make them undergo specialist cyber training to enable us to be in a position to effectively target our adversary. All these activities need to be coordinated and the same would be done by the JOC Wing. Periodic updation of

Data Base is a must. While fuzzing is a Brute force method to identify a vulnerability but a more scientific method is re-engineering or reverse engineering Operations. This is done when patches are issued after the vulnerability is found. There is also a requirement to find out what all vulnerabilities have been patched, but not disclosed as this information could be useful in developing a cyber weapon. To do all these one needs an updated Data Base & credible R&D labs. One can then build exploits to specifically target a vulnerabity but these should be packaged in such a manner that a normal cyber warrior can also use it. It is akin to the analogy that a soldier need not know the ballistics of bullet but should only have an idea of the characteristic of bullet and the damage it can cause, besides of course being able to fire the weapon.

Offensive Wing and Cyber Op Units (COU).

These would be specialized units comprising of 50 to 100 highly skilled personnel. They would be in possession of graded cyber weapons and would be in a position to use/ fire them when told to do so. These offensive cyber Operations units would be geographically dispersed and would part of various theatre Commands of the three services and of the Andman and Nicobar command. They will have interfaces at requisite level with the support teams of the R&D support wing and with the field Army/ IAF/ Navy. However, as explained earlier, their employment would be monitored at JOC level in the Cyber Command.

Defensive Wing.

It will perform the tasks presently being performed in the Army by the Army Cyber Group and in the Navy and Air Force by their respective Cyber Wings. At the various command HQ's in Army, the tasks being performed by the Brigadier General Staff (Information Warfare) and his team of officers and at the Corps level, the role and charter of Colonel General Staff (Information Warfare) would accordingly be taken on by elements of this wing. Similar would be the transition of responsibility in the Navy and Air Force at the Command level and at the Fleet/ Wing level respectively. IW per-se comprises of Electronic Warfare (EW), Cyber Warfare and Psychological Warfare (Phy W) (ie EW, Cyber & Psy W). The core competency in the first two fields lies primarily with the Corps of Signal in the Indian Army (and with the corresponding technical arms in the other two services). The domain responsibilities in these two fields are also thus well laid out, but there is considerable ambiguity in the same as regards Psy W (The same is more or less the case in the other two sister services also and needs to be addressed). Training in Psy W and in Cyber Warfare is again a major issue.

Research & Development (R & D) Support Wing.

Offensive Cyber Ops Unit 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 Command 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, Metaspirit 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.

It is rumored that the 'Core Impact' tool was developed by a team of 65 persons and thousands of dollars were possibly funded by US govt to support this venture. If credible Cyber capability is to be developed, it is the norm world over those requisite incentives must be given. The R & D support units should maintain close links with Operations units, during both planning and execution phase. Solution to the problems in the field in the Cyber arena will be provided by the Support Team only. Hence real time association between the two is a pre-requisite. A Theatre Commander can't use his weapon in isolation, hence the need for synergy between the two. The Cyber Support Teams can't be distributed and flittered away in penny pockets as they would at best be 300-400 highly skilled persons looking after vulnerabilities in various technologies ie mobile communication, HF, VHF, UHF links, WiFi, Windows and other Operating System platforms etc.

Capability of R&D Wing. Each weapon platform should permit authentication, identification and control. Each weapon should be able to be upgraded periodically. At present only products that are commercially available are seen (for eg Gailelio). However it needs to be understood that weapons keep on getting degraded with time, (if timely payment for upgrades is not given). Moreover if someone launches a cyber weapon against a known vulnerability, the R&D Wing should be able to ensure that our systems are patched to guard against this vulnerability, resulting in capability loss for the adversary, for using the same exploit. The R&D Wing would need to have No of laboratories (labs) for developing various information security products. The same will be discussed with reference to one such lab pertaining to Windows Operating System (OS).

Window Operating System (OS) R&D Lab. It will need to have an updated Data Base (DB) of various versions of Window 3.1 to the versions released till date. Every possible update (released each Tuesday), must be available with the Windows R&D lab within the R&D Wing. There would be a dedicated group of people doing fuzzing ops to identify vulnerability in windows, so that an exploit can

be developed to use that vulnerability. It is quite possible that these vulnerabilities (if not identified would have been passed on from an older version to the newer version of the windows OS once the OS upgrades to the newer version. The job of this group of persons is to find that vulnerability and develop a cyber exploit/ weapon for it. This is the level of complexity of merely one of the sections (windows OS section). Likewise there be a requirement of such a section for each type of Operating System that we intend targeting.

Cyber Range. This is another important component of the R&D Wing. Whatever is there is Cyber Space, will form part of the Cyber Range. For example if a Cisco Router/ Multi Service Platform is there in Cyber Space, then either it is there in physical form or else its image is created through simulation. The GNS software enables simulation of all Cisco Routers. Nuclear controllers generally use Seimens servers, so accordingly the Seimens server or the simulation package to simulate the same could be made available. There is a need to map the Cyber space and identify how far one can go. The Network topology built in the Cyber Range will have both virtual infrastructure as well as physical infrastructure which will resemble the adversaries Cyber space. Each part of the range will be focusing on a particular area in the cyber space of one adversary and is thus unique and dynamic and will keep evolving. There will be a requirement to stay focused and adopt to role change. Periodic software updates of course are a pre-requisite.

Build Up of Overall Picture: Conduct of Cyber Ops

Having seen the various components of a typical cyber command, a possibly way for the build up of the overall picture for conduct of Cyber Operations, which could be carried out in five phases will now be discussed.

Phase 1. It will involve posting and recruitment of manpower with requisite skill sets. Subsequently there would be a requirement to build up a policy for employment of these Cyber Units. The employment models being followed in other nations would be studied with an aim to adopt them to the national requirement. Training to impart specialized Cyber skills training and basic language training (to enable the Cyber Warriors to understand how to target the adversaries platforms and the effects it will have) will then be imparted. The Qualitative Requirements (QR) for a Cyber Weapon and its platform would need to be finalised and firmed up in this phase. The minimum time anticipated for these activities will vary from six months to one year.

Phase 2. The activities involved in this phase would be policy finalization and promulgation, imparting specialised Cyber Skills Training and Advance Language Training. The build up of Infrastructure would be a concurrent activity. It is in this phase that one could commence populating the Data Base (Anti-Virus companies normally share Data Base and could be considered to be tapped into). The

R&D work would also commence in this phase. The building and testing of Cyber weapons would start and basic Cyber Exploit operations would also start (akin to activities carried out during the EW reccee phase where in both passive and active reccee is carried out).

Phase 3. Refinement of Policies and Protocols would be undertaken and Rehashing of manpower to suit the tasks at hand will be carried out. Specialised Training as well as training in Advanced Language Courses would continue. Cyber weapon development would commence and Cyber Exploit Operations s would also continue.

Phase 4. During this phase the roles of High Grade Cyber Weapons will be defined and a mechanism will be formulated as to how to target the adversary. Planning for advanced Cyber Operations will be carried out during this phase and interactions with Subject Matter Experts industry, academia and domain specialists will also be carried out. The architecture of Cyber Weapons distribution will be evolved and demand based intelligence capability (to meet on the spot demands) will be built up.

Phase 5. This will involve working out the mechanics of Operational funding at desired levels and evolve the on ground day to day working methodology, with an impetus being accorded to R&D, to attain self sufficiency. Each phase is likely to overlap and it will take three to four years for development upto Phase 4 and another year ie five years for Phase 5 to mature.

Funding. Funding needs to be guaranteed and assured and the lack of it should not impact the development. There is a need to develop Hybrid models using the existing tools and modify the same to suit our needs (eg Core Impact Tool commercially available could be tweaked to suit our requirements, rather than redesigning the complete wheel from scratch). The approximate amount that would be needed is Rs. 1,000 Crores. There must be a willingness to train Human Resource (HR) and keep it captive, for use in the Cyber Command.

Conclusion

The raising of a Cyber Command is a national security imperative to counter future threats and challenges because the next generation wars are likely to be fought in this dimension. Even if wars are not fought explicitly in the Cyber domain, a cyber attack can cause mayhem in any Network Centric and IT rich environment Thus there is a pressing need to put in place a mechanism to raise this Cyber Command. Creation of the new orgnisation needs to be progressed on top priority as it would result in substantial capability enhancement in sub conventional and conventional warfare domains. In fact it will have a major covert effect in the domain of nuclear warfare also.

It has been truly said that *"Nothing is permanent except change and nobody can stop an idea whose time has come".* The time to establish a Cyber Command has now come, what needs to be seen is whether the government is willing to bite the bullet for the capability enhancement. The resources should be provided on accretion rather than pooling the same from within existing resources. The latter option may be easier but it will adversely affect the capability of the armed forces in other quarters.

In order to give an overall impetus to this project, the government also needs to concurrently appoint a CDS (Chief of Defence Staff) to be able to effectively interface the Cyber Command with HQ IDS and with the three Service HQ's and with the MoD.

*Brig Navjot Singh is DACIDS (JCES), HQ IDS

**Prof (Dr) Sanjeev Bansal is Dean Faculty of Management Studies, Amity University

---

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 and 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".

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_Lnge Lango. "The Academic Debate on Cyber Security". Internasjonal Polikk 71(2).

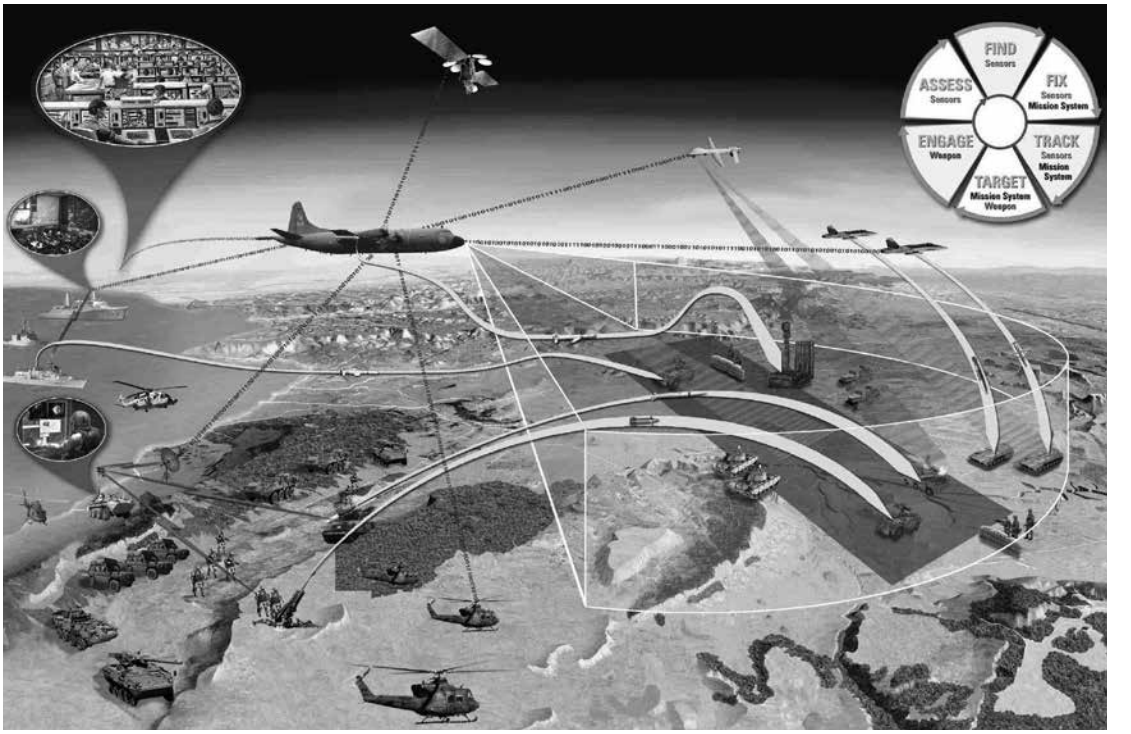
14. M.C. Libicki. "Conquest in Cyberspace National Security and information Warfare". Cambridge University Press.

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.

Preparing Our Armed Forces for the Fifth Generation of War

Group Captain Sanjay Dhankhar, VM*



Introduction

"Just as Alexander's exploits only reached the Middle Ages as a dim, fantastic tale, so in the future people will probably look back upon the twentieth century as a period of mighty empires, vast armies and incredible fighting machines that have crumbled into dust . . . " - Creveld[1]

[1]Creveld Martin Van, Transformation of War, The Free Press Simon and Schuster Inc, 1991.

As the technology changed over the eras the war waging machinery changed & so changed the nature of war fighting. War always changes. The weapons have always been closely linked to science, industrial capability & technological advancements. Our enemies learn and adapt, and we must do the same or lose. But today, war is changing faster and on a larger scale than at any time in the last 350 years. Not only are we facing rapid change in how war is fought, we are also facing radical changes in who fights and what they are fighting for. All over the world, state militaries, including our own, find themselves fighting non-state opponents. This would require the armed forces to be fully integrated in all aspects, whether it is a question of doctrines, equipment procurement, logistics or training. The creation of the Integrated Defence Staff (IDS), the Andaman and Nicobar Command (ANC), the Strategic Forces Command (SFC) and other fractionation is merely a grudging admission of the fact that 'jointness' as a concept and 'jointmanship' as its product are an inescapable reality even in the Indian context. The demands of 5th Generation Warfare (5 GW) also termed as Hybrid warfare will manifest itself not only at the level of the armed forces but also all elements at the national level.

The irony is that India was one of the first countries to realise, at the end of the Second World War that all future military operations would have to be combined operations involving at least two if not all the three Services working conjointly to a common plan. It was this realisation that led to the setting up of the National Defence Academy where cadets for all three Services are initially trained together and also the setting up of a Defence Services Staff College instead of separate services staff colleges, as was the norm in many other countries. While these institutions have certainly helped in improving interpersonal relationships yet these have not translated either in an understanding of each other's operational requirements or of any true integration in thinking and working together.

This lack of integrated thinking was obvious in the 1962 and 1965 conflicts; the former was left purely to the Army to conduct and the latter saw each service fighting very much their own individual wars. The 1971 operations displayed a slight improvement in joint planning, more so due to personality traits of the Leaders rather than institutions. There is a vital necessity for the three Services to integrate their thinking and activities if they are to really influence national policy and to succeed in facing the complex challenges to the Nation's security. There are some areas where this integration and reorganisation is necessary. However, organisation by itself will not succeed in achieving such integration. What is required is a change in mind-set, a change that makes every serviceman feels that he is a member of the Indian Armed Forces, and not just the Indian Army, the Indian Navy, or the Indian Air Force.

Disclaimer. The Indian Space programme was ab-initio declared as an instrument towards peace; geared up for scientific research & development goals. It is an

indigenous program developed under the umbrella of sanctions since inception at various times for one reason or the other. This programme cannot be compromised by creating a military link with this purely civil applications orientation program as declared to the world. Even in the darkest of corners the military links are spoken in hushed tones and there is no official recognition, which is quite understandable till we achieve 100% indigenisation in cutting edge technologies related to instruments, avionics and electronics. Therefore, the article focusses on the modalities of creation of the Cyber-Space Command.

Changed Nature of Warfare

The term Fifth Generation war or Hybrid Warfare came to fore during the Global War on Terrorism (GWOT). In Hybrid Wars we can expect to simultaneously deal with the fall out of a failed state that owned but lost control of some biological agents or missiles, while combating an ethnically motivated paramilitary force, and a set of radical terrorists who have now been displaced. We may face remnants of the fielded army of a rogue state in future wars, and they may employ conventional weapons in very novel or non-traditional ways. We can also expect to face unorthodox attacks or random acts of violence by sympathetic groups of non-state actors against our critical infrastructure or our transportation networks. We may also see other forms of economic war or crippling forms of computer network attacks against military or financial targets.

The kinds of war we will face in the future cannot be won by focusing on technology; they will be won by preparing all forces for the Three Block War. India's approach to Pakistan's continued hybrid warfare offensive has been characterised by the absence of a National Security Policy and a half-hearted response that can at best be termed as 'reactive'. Despite a conventional edge over Pakistan, economic prowess and growing recognition as an emerging global power, India is pursuing a policy of 'deterrence by denial' instead of *'punitive deterrence'*. One should not be misled by the relative lull marked by the absence of any major terrorist attack outside J&K in the period after the bomb blast in the German bakery in Pune in 13 Feb 2010. Even the earlier attack in Mumbai on 26 Nov 2008 had strongly indicated Pakistani involvement.

The Requirements to Wage Such a War

Reality of Proxy War. The simplest definition includes any war in which one of the major participants is not a state but rather a violent non-state actor. 5th Generation Warfare is likely to result from the continued shift of political and social loyalties to causes rather than nations. It will be marked by the increasing power of smaller and smaller entities and the explosion of biotechnology and nanotechnology. The focus of 5 GW would be more on cognitive and moral domains than the physical destruction of forces. Hybrid warfare can be used to describe the flexible and

complex dynamics of the battle space requiring a highly resilient and adaptable response.[2] This response would be possible only with true integrations in all domains.

Modern day operations can only be conducted if they are based on a reliable and effective Information Grid. The grid constitutes the computing and communication backplane through its Command and Control (C2) structures and a communications infrastructure to provide requisite convergence and information assurance. It is into this information grid that the two other entities namely the Surveillance Grid (which enhances situational awareness) and the Engagement Grid (Action) plug in to complete the overall organisation structure necessary for networked operations. All of these exist today in our Armed Forces in varying forms and degrees of sophistication. However, certain issues such as organisation, means of surveillance and their networking and communication infrastructure particularly at lower levels need attention. In addition, there are certain challenges related to integration and interoperability. The Armed Forces are neither fully integrated nor seamlessly interoperable, though stand-alone capabilities do exist. The need therefore is to forge military instrument of NCW based on suitably integrated organisations, new technologies, joint concepts and doctrines and joint training.

Networks are at the heart of the NCW, which would enable the Armed Forces to be more lethal and responsive in the era of Hybrid warfare. They have also led to the expansion of space and compression of time on the battlefield. It will thus impact the manner in which operations may be conducted which may range from change in concepts of application of force to adopting new tactics. The major challenge that stares all armed forces in this era is the translation from fourth to fifth generation warfare. Experts on the subject unanimously agree that this translation may be equally if not more challenging from the third to the fourth generation of war & the armed forces would need to adapt to this change at the earliest, especially ours considering the security issues that are challenging our nation.

Integration with Cyber Warfare

The word Cyber Space was coined by William Gibson in the science fiction Neuromancer in 1984. It denoted the apparent or virtual location within which electronic activities take place. Cyber Space therefore is a place where people meet not physically but virtually and communicate with each other electronically. Cyber Space is the aggregate of Intranets, Internet and World Wide Web. Cyberspace technology is emerging as an “instrument of power” and digital infrastructures have been designated as “national strategic assets”. Adversaries are increasingly exploiting this power to attack, degrade, and disrupt communications and the flow

[2]http://en.wikipedia.org/wiki/generation_warfare

of information. With low barriers to entry, very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Thus has emerged the concept of Cyber War.

Security expert Richard A. Clarke, in his book Cyber War (May 2010), has defined Cyber War as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. The Economist describes Cyber warfare as "the fifth domain of warfare, after land, sea, air and space". Ilias Chantzos, director of government relations EMEA and APJ at Symantec defines cyber warfare as "An act by a state/ government that has a political motivation to destabilise, interfere with, or disable online national security assets or entities of another state/government for the purpose of gaining the upper hand in pursuit of a militaristic objective. Those assets could come in the form of technological, economic or military value". Alvin and Heidi Toffler in their book War and Anti-War[3] have described development in the warfare in three waves:-

(a) **First Wave.** Dominant influence on warfare was by a summation of weapon and numbers.

(b) **Second Wave.** Influenced by mobility and fire power.

(c) **Third Wave.** Influenced by cyber space, an esoteric synonym of information.

Cyber warfare recognises no boundaries, least of all those that make distinction between the traditional levels of geographical delineation of the battlefield and decision matrix viz strategic, operational and tactical. It spills over and encompasses the entire gamut of command from the squad leader to the executive head of the state, and the agenda overlaps. Further, it defies distinction between war and peace, between warlike and criminal behaviour; between "rogue" and civilised"; even friend and foe. Combat info-realm may have many fronts or none. Cyber War is not only a matter of exploiting IT to defeat the enemy on the battlefield, but also of protecting systems and infrastructure critical to the functioning of the society. Potential battle fields are everywhere.

---

[3]Toffler Alvin Heidi, War and Anti-war, Little Brown and Company, USA, 1993, pp 33-38

The terms Cyber War and Net war are interchangeably being used by different countries. However, as per RAND[4] report the difference between these two terms is as follows:-

(a) **Cyber War.** A concept that refers to information-oriented military warfare. It is becoming an important entry at the military end of the spectrum, where the language has normally been about high intensity conflicts (HICs). Cyber Warfare can therefore be defined as 'Any action to deny, exploit, corrupt or destroy the enemy's information and its function; protecting ourselves against those actions; and exploiting these to our own advantage'.

(b) **Net War.** Net war figures increasingly at the societal end of the spectrum, where the language has normally been about Low-Intensity Conflict (LIC), operations other than war (OOTW), and non-military modes of conflict and crime.

Cyber war is not only a matter of exploiting IT to defeat the enemy on the battlefield, but also of protecting systems and infrastructure critical to the functioning of the society. Further, cyberspace is not constrained by the geographic space and potential military targets. It could involve anything from banking, railways, atomic plants, power generation, industries and so on. New modes of war, terrorism, crimes and even radical activism are all emerging from information age dynamics. Therefore, our Armed Forces have to adopt Cyber Warfare as a war fighting strategy and incorporate all facets of cyber war in operational planning and prosecution of war.

Information Warfare. The term Information warfare (IW) covers the full range of competitive information operations from destroying IT equipment to subtle perception management and from industrial espionage to marketing. It is about domination of the "Info-Sphere". In military terms dominating the information battle space has obvious advantages.[5] The methodology of communicating information about what is expected of lower formations and individuals has evolved over time to be matched to a concept or approach, appropriate to the nature of the conflict and the capabilities of the forces.[6]

Psychological Operations. These may become the dominant operational and strategic weapon in the form of media or for information intervention. Logic bombs and computer viruses, including latent viruses, may be used to disrupt civilian

---

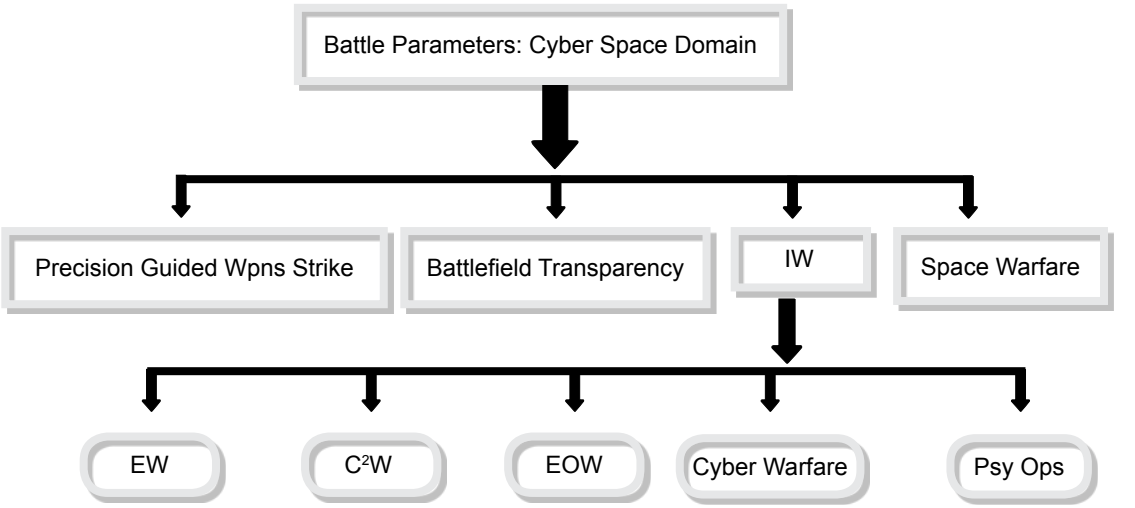
[4]RAND Report submitted to US Congress (http://www.rand.org/pubs/monograph_reports/)

[5]Bill Hutchinson & Matt Warren Butterworth Heinemann, Information Warfare, 2001, Linaerre House Jordan Hill Oxford 2001

[6]Internet Paper by NDU, USA.

as well as military operations. Fourth generation adversaries will be adept at manipulating the media to alter domestic and world opinion to the point where skilful use of psychological operations will sometimes preclude the commitment of combat forces. A major target will be the enemy population's support of its government and the war. Television news may become a more powerful operational weapon than armoured divisions.

Relationship of Information Warfare and Cyber Warfare. Cyber Space domain should be the major parameter with IW as the dominating subset. Other subsets are Electronic Warfare, Command and Control Warfare (C2W), Electro Optical Warfare (EOW), Psychological Warfare and such. The same is diagrammatically shown below:-



The Recommended Organisation

Cyber Space Warfare Command. Keeping in mind the requirements of the 5th GW, there are points that need to be kept in mind while creating the new Cyber Space Warfare Command. **The Cyber warrior will have to be a mix of military and civilian manpower;** the civil component being the IT experts in software, hacking and hardware. This is a paradigm shift from the erstwhile traditional military mind-set and hence needs serious consideration and acceptance. The Cyber Warfare Capability at the National Level needs to be simultaneously integrated. There are many stake holders in IT, ITES and Cyber Security field. At present Ministry of Communication & IT is responsible for infrastructure development of networks. Other organisations are discussed below.

(a) **Computer Emergency Response Team India, (CERT-In).**[7] CERT-In is the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur. CERT-In also assists in implementing proactive measures to reduce the risks of computer security incidents. The role of CERT-In is as follows:-

(i) Provide a single point of contact for reporting local problems.

(ii) Assist the organisational constituency and general computing community in preventing and handling computer security incidents.

(iii) Share information and lessons learnt with other CERTs, response teams, organisations and sites.

(iv) Incident Response, Incident tracing & offer recovery procedures.

(v) Vulnerability & Risk analysis and response

(vi) National Repository and a referral agency for cyber-intrusions.

(b) **National Informatics Centre (NIC).**[8] NIC, which is part of the Department of Information Technology, provides the network backbone and e-Governance support to Central Government, State Governments, UT Administrations, Districts and other Government bodies. NIC assists in implementing Information Technology Projects, in close collaboration with Central and State Governments, in the areas of centrally sponsored schemes including Central or State sector schemes and District Administration sponsored projects.

(c) **National Internet Exchange of India (NIXI).**[9] Nearly eight years after the gates of the Internet were thrown open to subscribers in India, domestic traffic was still being routed via international bandwidth rather than routed through local ISP networks. For instance, if packets have to be routed from Mumbai to Chennai, it is likely that they will first go from Mumbai to Singapore, then to US and then come to Chennai. World over, this routing of domestic traffic is done through 'peering'. NIXI, a non-profit Company was established in 2003 to provide neutral Internet Exchange Point services in the country. It was established with the Internet Service Providers Association of India (ISPAI) to become the operational meeting point of ISPs in India. Its main purpose is to facilitate handing over of

[7]Computer Emergency Response Team (http://www.cert-in.org.in)

[8]National Informatics Centre (http://nic.org.in)

[9]National Internet Exchange of India (http://nixi.org.in)

domestic Internet traffic between the peering ISP members, rather than using servers in the US or elsewhere. This enables more efficient use of international bandwidth and saves foreign exchange. It also improves the Quality of Services by avoiding multiple international hops and thus lowering delays. NIXI currently has seven operational nodes at the centres in Delhi (Noida), Mumbai (Vashi), Chennai, Kolkata, Bangalore, Hyderabad and Ahmedabad. It's role includes the following important tasks: -

(i) Access to the layer-2 switched medium (fast ethernet).

(ii) 24x7 watch service, hardware maintenance and helpdesk services on the NIXI switch.

(d) **National Information Board (NIB).**[10] The Kargil conflict led to a very comprehensive review of our security apparatus and the higher defence org. On recommendations of the Kargil Review Committee, the Prime Minister appointed a Group of Ministers (GoM) to examine the national security system and to make appropriate recommendations. Among the many recommendations made by the GoM, setting up of a 'National Information Board (NIB)' was recommended.

(e) **National Technical Research Organisation.**[11] The National Technical Research Organisation (NTRO) is a premier apex scientific organisation under the National Security Advisor set up in 2004. It includes National Institute of Cryptology Research and Development (NICRD), which is first of its kind in Asia. NTRO is a highly specialized technical intelligence gathering agency. While the agency does not affect the working of technical wings of various intelligence agencies, including those of the Indian Armed Forces, it acts as a 'super-feeder' agency for providing technical intelligence to the govt on internal and external security. The organisation does hi-tech surveillance tasks, including satellite, terrestrial and internet monitoring, considered vital for the national security apparatus. It develops technology capabilities in aviation, remote sensing, data gathering and processing, cyber security, cryptology systems, strategic hardware, software development and strategic monitoring. It is responsible for monitoring and intercepting terrestrial and satellite-based communication. Services of NTRO can also be utilised in investigating cyber-crimes and

---

[10]Lt Gen S.R.R. Aiyengar (Retd) , Exploiting the Electro-Magnetic Spectrum in Jointmanship Journal of Defence Studies • Volume 1 No. 1, Aug 2007

[11]National Technical Research Organisation http://en.wikipedia.org/wiki/national technical research organisation #cite_note-1#cite_note-1

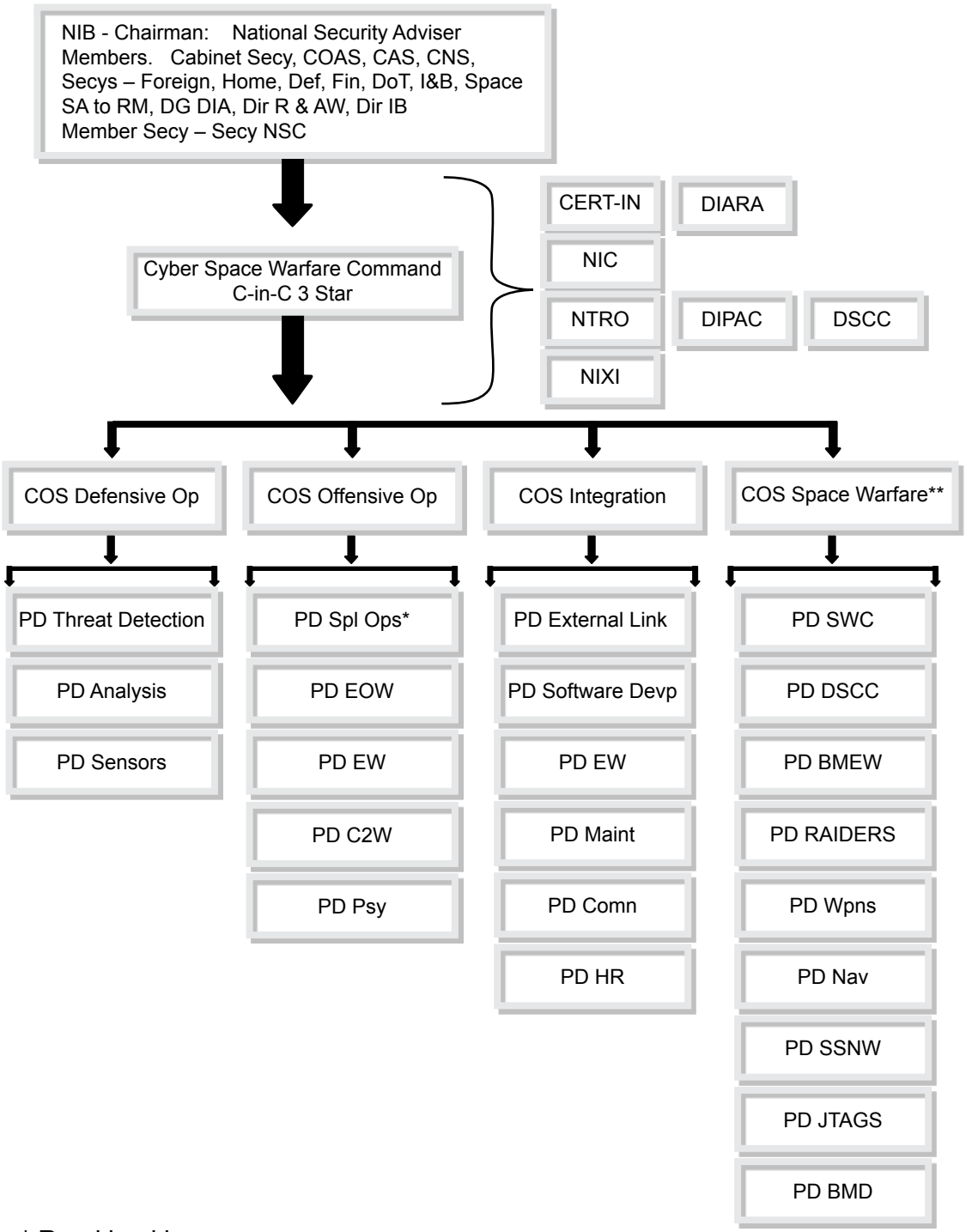
in cyber forensic. NTRO also has the capability for recovering data, monitoring of ISPs as also in securing database management, data mining and data warehousing. The organisation has the necessary talent for providing consultancy on information security policy to various agencies of the government. It is also capable of intrusive or defensive operations. NTRO also has first rate encryption technology and has devised various methods of securing data. Scientists of the organisation are trained to penetrate suspect computers, extract information and map clandestine websites in the cyber world.

(f) **Technical Intelligence.** DIA, Defence Services, Research and Analysis Wing (R&AW), Central Economic Intelligence Bureau, Directorate of Revenue Intelligence, Enforcement Directorate and Narcotics Control Bureau are some of the government agencies which are always in need of technical intelligence to accomplish varieties of tasks entrusted to them. With different government agencies protecting their turf in respect of intelligence gathering, NTRO is understood to have been tasked to assist various financial and economic intelligence agencies in honing their skills. A coordinated sharing and response mechanism can go a long way in playing a significant role in protecting national security.

The Expansion of the acronyms is as follows: -

Acronym	Expansion
AFSCN	AF Space Satl Cont NW
BFT	Battle Field Transparency
BMD	Ballistic Missile Defence
BMEW	Ballistic Missile Early Warning
DIARA	Defence Information Assurance & research Agency
DIPAC	Data & Image Processing & Analysis Centre Defence Imagery & Photo Analysis Centre
DSCC	Defence Satl Control Centre
JTAGS	Joint Tactical Ground Station
OTIC	Optical Tracking & Identification Centre
RAIDERS	Rapid Attack Identification Detection Reporting Sys
RSTA	Reconnaissance Surveillance & Target Acquisition
SSNW	Satl Surveillance & Net Working
SWC	Space Warfare Centre

The Recommended organisation would therefore look something like this: -



* Read hacking

** Interim till creation of Aerospace Command

Conclusion

"Protecting critical information resources will become one of the defining challenges of National Security in the years to come" - John Hamre, Deputy Secretary of Defence, US

The changing natures of threats demand 'flexible force packaging' and 'interoperability' to meet various contingencies[12] and hence the creation of the Cyber Space Warfare Command. With the integration of all national level agencies dealing with this challenge we would have achieved something that hitherto has not even been conceptualised.

NIB at the national level may also be tasked to formulate National level Cyber policy in consonance with the overall national security perspective, direction, control and funding. It needs to be appreciated that the issues involved are of unprecedented complexities and interwoven dependence at the levels of individual functionaries, organisations at the political, economic and social domains, more often with tremendous clash of interests. Periodic monitoring of various institutions and dedicated establishments towards acquisition of requisite IW capabilities would be ensured. In doing so, NIB would ensure that the country develops a holistic approach in developing specific IW capabilities. While the deliberations of NIB would be classified, it is expected that this body meets regularly and monitors the progress on acquisition of the requisite IW capability keeping in mind the threat posed by our adversaries in the near and long terms.

The Cyber Space Warfare Comd would be the central agency addressing the troubling offence-defence asymmetry in the scope of 5th GW. The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of 5th G warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military information functions. There are many information functions critical to our national security that lies outside the military's defensive purview. Land, sea, air, and space are realms within which we may conduct military operations. Each realm imposes its characteristics on operations within it. This is even more significant in this era and there is a need to embrace this reality to create mechanisms for defeating the adage ***'There is no such thing today called fully prepared!'***

---

[12]Hawkins William R, "Is Rumsfeld's Revolution in Military Affairs Finally Over". American Economic Alert, Sep 12, 2006, (http:/www.americaneconomic alert.org)

Books

'Barbarism: A User's Guide', Hobsbawm Eric, New Left Review, (July–August 1994)

Dealing with Global Terrorism: The Way Forward Maj Gen Vinod Saighal 2003 Sterling Publishers

Future Shock Toffler Alvin, 1990 Bantam Books Random House

Information Warfare Hutchinson Bill & Butterworth Heinemann, Warren Matt 2001 Linaerre House Jordan Hill Oxford

Intelligence Security and Asymmetric Warfare Strategies for Solutions Dhirendra Singh & Lt Gen DB Shekatkar, PVSM, AVSM, VSM 2010 Manas Publications

The Sling and the Stone on war in the 21st century Col Thomas X Hammes, USMC, 2006, Manas Publications Zenith Press

Transformation of War Creveld Martin van; 1991 The Free Press Simon & Schuster Inc.

Technology and War Creveld Martin van, Brasseys 1991 UK Press

Journals

Lt Gen S.R.R. Aiyengar (Retd), Exploiting the Electro-Magnetic Spectrum in Jointmanship Journal of Defence Studies • Volume 1 No. 1, Aug 2007

Webliography

http://www.firstworldwar.com/origins/causes.htm

http://en.wikipedia.org/wiki/generation_warfare

http://en.wikipedia.org/wiki/Causes_of_World_War_II

Internet Paper by NDU, USA.

Hawkins William R, "Is Rumsfeld's Revolution in Military Affairs Finally Over". American Economic Alert, Sep 12, 2006, (http:/www.americaneconomic alert.org)

National Technical Research Organisation http://en.wikipedia.org/wiki/national technical research organisation #cite_note-1#cite_note-1

Computer Emergency Response Team (http://www.cert-in.org.in)

National Informatics Centre (http://nic.org.in)

National Internet Exchange of India (http://nixi.org.in)

RAND Report submitted to US Congress (http://www.rand.org/pubs/monograph_reports/)

Raising a Cyber Command for Indian Armed Forces: Requisites and Organisational Considerations

Munish Sharma*

Introduction

Ever since the computers of research institutions in the US began communication with each other for data exchange, the exponential growth of the network has engulfed the computing resources and networks spread across the globe, manifesting in the form of cyberspace. The cyberspace enabled businesses to carry out global operations and provide information to the management in the real time. The governments began expanding their footprint in the cyberspace to deliver governance and services related to transportation, healthcare and education. Cyberspace, deemed to be the fifth domain of warfare, has transformed the way armed forces conduct their day-to-day operations, while bringing in a paradigm shift at the strategic, doctrinal and tactical levels of warfare. In essence, cyberspace is an enabler for business and governments, a facilitator for the wider populace, and a force multiplier for the armed forces. The armed forces conduct and execute a host of operations, which includes transportation and logistics, training and exercises, human resource management, inventory and supply chain management, and above all, the conduct of war. In the entire ecosystem of all the three wings of armed forces, the dependency of operations on cyberspace is of the highest order. The armed forces themselves operate vast communication and data networks spread across the geographical length and breadth of the country, even spanning to its maritime, air and space domains. It is vital for the armed forces to secure their own networks from any kind of intrusion or espionage attempt or a cyber attack which could deny them the access to their own networks, computer resources or command and control infrastructure. In the wake of growing number of attacks from adversaries, both adversarial nation-states and non-state actors, cyber commands within the auspices of the armed forces are the need of the hour to deny the adversary any access to the computer networks during both peace and war, simultaneously developing a deterrent if the nature of the attack deems use of force to be necessary. A cyber command is critical in developing the desired capability, capacity and the tents of requisite response.

The Naresh Chandra Task Force report in 2012 had laid thrust on the issues of internal security, external threats, politico-military affairs, jointness in the armed

forces, including measures for cybersecurity in the Indian defence establishment. The panel had recommended raising a Special Operations Command, a Space Command and a Cyber Command, drawing synergy from the three wings, all together in a unified command and control structure.[1] In essence, the objective is to reinforce the joint combat capability across the tri-services and prepare them for the futuristic battlefield. The paper will explore the case of cyber command for India and the organizational considerations.

Network Centricity and Cyberspace

Technology has been shaping the conduct of war, although it does not define the outcome of the war. It has thrown open new domains of warfare as well; warfare on the surface extended to the sea with the advent of naval ships in the nineteenth century. As aircrafts were pressed into strategic bombing, air support and air superiority roles, since their induction to the military around mid of the twentieth century, aerial warfare has become an integral part of military strategy. The use of space and cyberspace for military purposes have spawned fourth and fifth dimension of warfare; both have been manifestations of technology in the later part of the twentieth century. Furthermore, all the domains of warfare intersect each other, the space is instrumental to the modern warfare; it enables communication, navigation, cartography, maritime domain awareness, battlefield domain awareness, precision targeting and it is progressively being used for ballistic missile defence.[2]

The evolving nature of warfare in the information age is completely network centric. It is shaping up novel doctrines and the conduct of modern warfare, commonly known as Network Centric Warfare (NCW), encapsulating an array of information systems, computers, their networks, satellites, network of sensors, data links, local and wide area networks, various heterogeneous military platforms etc., all integrated for swift information sharing, thus augmenting the combat capability and efficiency of the armed forces. The operational requisite for real time data gathering, analysis and dissemination of command and control information has led to the deployment of sensors, their vast networks and communication channels. The data generated by these networks or integrated platforms enhances the situational awareness; vital to conduct joint operations and efficacious decision making. In principle, network centricity in defence or military domains is a convolution of information and communication technologies. Therefore, network centricity is primarily integration of network of sensor systems, deployed automated systems,

---

[1]Vinod Anand, Defence Reforms and Naresh Chandra Task Force Review, Vivekananda International Foundation, available at http://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review#sthash.Dq7jDhMn.gXhyNIVM.dpuf, accessed on 02 May 2016.

[2]Alex Roland, War and Technology, Foreign Policy Research Institute, February 2009, available at http://www.fpri.org/articles/2009/02/war-and-technology, accessed on 22 May 2016.

radars, detection and recognition equipments, remote sensing, early warning systems, signal processing and imaging techniques and so on. Modern armed forces are desired to execute joint operations, spread across wide geographical area, cutting across the areas of responsibilities of the army, navy and the air force. Under these conditions, uninterrupted communication (in the form of text, voice, images or video) and security of these communication channels (generally built with redundancy), right from the headquarters to the soldier on the ground, is of utmost importance. Therefore, security and integrity of cyber assets, data at rest or in transit and information infrastructure of the armed forces is vital for the success of standalone as well as joint operations, in the era of interconnectedness. The preparedness for joint operations and network centric warfare begins with clearly defined strategy and doctrine, acting as the guiding force.

Cyber Command and the Doctrine

In military terms, doctrine guides the operational art and tactics; it sets the objectives and guides the means and methods to attain the objectives. Doctrinal changes are flexible and fast, adaptable to changing circumstances and environment, such as changes in technology. Thus, doctrine constantly matures and evolves.[3] Consequently, doctrine influences strategy and the results of strategy become the experiences that are the basis for doctrine.[4] The Gulf War of 1991 brought in the paradigm shift in strategic military thinking and in relation to this, Myriam Dunn Cavelty notes that,

"Military strategists saw the conflict as the first of a new generation of conflicts, in which physical force alone was not sufficient, but was complimented by the ability to win the information war and to secure information dominance."[5]

The doctrines and military strategies there onwards were focused on de-capacitating the adversary by degrading the communication and information systems. The full spectrum of intelligence and business operations of armed forces, including logistics, transportation and the command and control have some degree of dependency on the cyberspace. It is an area of competition and confrontation as the fifth domain of warfare with no clear demarcation of geographical, physical or political boundaries. Nation states have proven capabilities to intrude into unclassified or classified networks of other countries for espionage, either through military means or their intelligence agencies. Information Technology has significantly changed the rules or conduct of war within one generation. Such a change has forced the

[3]Dennis Drew and Don Snow, "Military Doctrine", The Air University (US Air Force), available at http://www.au.af.mil/au/awc/awcgate/readings/drew1.htm, accessed on 30 May 2016.

[4]Ibid.

[5]Myriam Dunn Cavelty, Cybersecurity in Switzerland, Springer London, 2014, p. 20.

planning process and strategic thinking of the defence establishment to adapt and align their long term goals according to these developments.[6] For instance, with network centricity in the modern day warfare, armed forces are moving towards agility in their strategic and tactical operations, which is enabled by the use of ICT to integrate platforms in order to overcome geographical limitations.

Network-centric warfare (NCW), as a doctrine enables the forces to utilize these networks, share large amounts of critical information in real time, thereby improving the combat capability and efficiency. The integration of platforms, spread across land, sea, air and cyberspace, paves the way for an operating model for large, geographically spread organizations to have enhanced situational awareness and a united, coordinated and synchronized decision-making process, which is critical in modern-day warfare.[7]

At conceptual level, constituting a Cyber Command is a manifestation of changes brought in by cyberspace at strategic and doctrinal level for the armed forces. In order to secure the national interest, armed forces need to be combat ready in all the domains of warfare. Fundamentally, a Cyber Command secures the information infrastructure of the armed forces, as an area of responsibility, from any kind of adversarial interference, ensures freedom of action in cyberspace and simultaneously denying the same to the adversary.

Cyber and Military: The US Cyber Command

The US Cyber Command (USCYBERCOM) was established with the vision of fusing the full spectrum of cyberspace operations of the US Department of Defence (DoD), primarily charged with the day-to-day defence and protection of its information networks; providing support to military missions and most importantly prepare to and when directed, conduct full spectrum military cyberspace operations.[8]

The DoD is a key stakeholder in the National Infrastructure Protection Plan of the US government, which engulfs critical infrastructure and key resource protection. US Cyber Command aims to build a workforce of 133 Cyber Mission Teams comprising 6,200 personnel (military, civilian, and contractor) by 2016.[9] Once fully operational, these 133 teams will be organised into three distinct Cyber Mission Forces: Cyber Protection Forces to defend priority DoD networks and systems

---

[6]Klaus Ruhlig and Uwe Wiemken, "Disruptive Technologies: Widening the scope", Fraunhofer INT, April 2006.

[7]Ajey Lele and Munish Sharma (2014): Relevance of Cloud Computing for Defence, Journal of Defence Studies, Vol. 8, No. 2, April–June 2014, p. 71.

[8]"US Cyber Command", US Army Cyber Command, available at http://www.arcyber.army.mil/Organization/USCyberCommand, accessed on 30 May 2016.

[9]Department of Defence Cyber Strategy, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, p. 6.

against priority threats; National Mission Forces to defend the US and its interests against cyberattacks of significant consequence[10] ; and Combat Mission Forces to support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations.[11] At operational level, U.S. Cyber Command synchronizes its activities with other DoD organizations, particularly combatant commands, to respond to emerging challenges and opportunities.

A four-star General heads the US Cyber Command while serving as the Director of the National Security Agency, signifying the synergy US draws from the technical capabilities of the civilian sector. Perhaps, because most of the critical infrastructure, service providers, technology developers, and the much desired skill-set lies out of the military ecosystem.

The mission of US Cyber Command could be summarized as to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of US systems to withstand a potential attack. The US DoD has long-standing proposal to reduce the number of geographical commands by merging North and South America into a single entity; and, similarly, place Europe and Africa under a single command.[12] At the same time, the cyber budget has been increase to$35 billion over five years[13], underpinning the importance US DoD draws on the cyber domain.

Cyber and Military: "Informationization" in People's Liberation Army (PLA)

The top order of Chinese political leadership has been working towards the 'informationization' of its military; integrating the divisions, training the officers and soldiers on cyber warfare; improving the information network and studying the outcomes of wars in Gulf, Kosovo, Afghanistan and Iraq. In February 2014, Chinese President Xi Jinping called for collective efforts to build China as a Cyber Power, aspiring to building the PLA into a force capable of winning "local wars under high-tech conditions or the conditions of informationization".[14]

---

[10]Such as loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact.

[11]N. 7.

[12]Ajai Shukla, "US Defence Secy announces major changes before India visit", Business Standard (Philadelphia), 09 April 2016, available at http://www.business-standard.com/article/economy-policy/us-defence-secy-announces-major-changes-before-india-visit-116040900025_1.html, accessed on 18 May 2016.

[13]Anthony Capaccio, Pentagon Seeks 35 Billion to beef up Cybersecurity Over 5 Years, available at http://www.bloomberg.com/news/articles/2016-02-29/pentagon-seeks-35-billion-to-beef-up-cybersecurity-over-5-years, accessed on 18 May 2016.

[14]Information Office of the State Council of the People's Republic of China, "China's National Defense in 2004", see http://www.china.org.cn/e-white/20041227/index.htm, accessed on 18 May 2016.

The Chinese efforts to augment its capabilities in cyber war fighting and political backing to put it in practice against political, governmental, industrial or military targets clearly establishes the dominance of cyber in the security calculus. The offensive capabilities of China are concentrated in its military establishment. A report from the cybersecurity firm Mandiant identified Military Cyber warfare unit number 61398 to be the 2nd Bureau of 3rd Department of PLA's General Staff Headquarter.[15] The same unit is alleged to be building expertise in covert communications, network security, operating systems design and development.

The burgeoning role of military establishments in securing the civilian components of critical infrastructure of the nation or combat readiness to execute an offensive cyber operation (if the need arises), in addition to securing its own vital networks, is not just imminent but essential. The US Cyber Command and the impetus of PLA towards "informationization" connote the emergence of a militarized cyberspace. India has vital interests in the security of cyberspace, and dilating military presence of other nations jeopardizes these interests. The National Cyber Security Policy 2013 is a prominent step in this direction. However, further delay in setting up a Cyber Command is detrimental to the legitimate interests of the government of India or its armed forces in the cyberspace. However, along with a Cyber Command on the ground, India needs a well articulated military strategy or a doctrine for cyberspace operations.[16]

Raising a Cyber Command: Organisational Considerations

The idea of a Cyber Command for Indian Armed Forces has been in the policy circles since it was first mooted by the NCTF report. Various media reports state that the Ministry of Defence has a draft on the subject ready and it is awaiting nod from the Cabinet Committee on Security.[17] The subject has appeared in many policy statements by the present[18] as well as former[19] defence ministers. The three new commands – Special Operations Command, Aerospace Command and Cyber Command – are planned to be under the tri-services headquarters and draw

---

[15]Dan McWhorter, "Mandiant Exposes Apt1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators", FireEye, 19 February 2013, available at https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html, accessed on 18 May 2016.

[16]Munish Sharma, Military in Cyberspace, Defence and Security Alert (New Delhi, April 2015), Volume 6, Issue 7.

[17]Pradip R Sagar, "India readies cyber command service to combat espionage threats online", DNA India, 15 January 2014, available at http://www.dnaindia.com/india/report-india-readies-cyber-command-service-to-combat-espionage-threats-online-1950997, accessed on 24 May 2016.

[18]"Armed Forces vulnerable to cyber attacks, says Defence Minister", Business Line, 23 November 2015, available at http://www.thehindubusinessline.com/info-tech/armedforces-vulnerable-to-cyber-attacks-says-defence-minister/article7909315.ece, accessed on 24 May 2016.

[19]Cyber command in armed forces soon: Antony, The Hindu, 26 May 2013, available at http://www.thehindu.com/news/national/cyber-command-in-armed-forces-soon-antony/article4750288.ece, accessed on 24 May 2016.

capacity, assets and human resources from all the three services.

The Cyber Command proposal was prepared in consultations with the Chiefs of the Air Force, Army and Navy, in the wake of growing number of incidents of cyberattacks on Indian defence establishment, such as Chinese hackers breaking into sensitive computer systems at the headquarters of the Eastern Naval Command in Visakhapatnam[20], where the indigenous nuclear submarine Arihant had been undergoing sea trials. The emails of several high-level officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP) were hacked into in 2013. An investigation put the total number of hacked accounts at roughly 12,000.[21]

Under the shadow of growing number of breaches, defacements and the expounding strategic imperatives of cyberspace in particular, the forces need to prepare for conventional as well asymmetric warfare in a unified manner. However, the experience with unified theatre command at Andaman and Nicobar islands has not been pleasant, perhaps due to turf between the services or organizational constraints.[22] [23] The Andaman and Nicobar Command (ANC) was raised in 2001, and if the experiment had fared well[24] , more unified commands would have been constituted. Nevertheless, ANC remains to be the only joint service theatre command. Therefore, raising three new unified commands would be organisationally challenging, given the past experiences and the lack of inter-service as well as inter-governmental coordination.

The proposed plan is to upgrade the Defence Information Assurance and Research Agency (DIARA), the nodal nodal agency dealing with all cyber security related issues of Tri Services and Ministry of Defence, into a Defense Cyber Agency as in interim arrangement till the full-fledged commands become operational.[25] The response to networked threats must be networked defence. Figure 1 summarises the

---

[20]P K Vasudeva, "Secure our e-frontiers", Hindustan Times, 12 July 2012, available at http://www.hindustantimes.com/india/secure-our-e-frontiers/story-orh6I0tb5ZUyMbheH5PJDM.html, accessed on 24 May 2016.

[21]Manu Kaushik and Pierre Mario Fitter, "Beware of the bugs", Business Today, 17 February 2013, available at http://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html, accessed on 24 May 2016.

[22]Anit Mukherjee, "India's Joint Andaman and Nicobar Command is a Failed Experiment", Asia Pacific Bulletin (East-West Center), Number 289, 17 November 2014, available at http://www.eastwestcenter.org/sites/default/files/private/apb289.pdf.

[23]P.S. Das, "Jointness in India's Military —What it is and What it Must Be", Journal of Defence Studies, Volume 1, No. 1, available at http://www.idsa.in/jds/1_1_2007_jointnessinindiasmilitary_psdas.

[24]N. 10.

[25]Concept Note

probable placement of Cyber Command in the existing cybersecurity architecture[26] and its interaction with the network of agencies. It would be constituted under the aegis of tri-services headquarters as a unified command, and draw assets, human resources from all the three services. It should acquire operational information, monitor the networks, defend them from any attempt of espionage, intrusion or attack, and draw operation planning and execution in close coordination with the services and the Ministry of Defence.

Conclusion

The Indian Armed Forces have drawn ambitious plans for transformation into a potent network centric force. The integration of C4I2SR (command, control, communication, computers, information, intelligence, surveillance and reconnaissance) components at the operational level for either of the services would be effective in the presence of integrated doctrines and inter-services synergy to conduct joint operations. The three services operate and administer Wide Area Networks, Computer Data Networks, Switched Communication Network and Satellites for communications, weapon control and management systems, and navigation to enable net-centric operations. During both, peace and war, the integrity of communication channels, security of information and information systems, ability to operate with degraded infrastructure, and resilience to overcome an attack are paramount operational objectives. A Cyber Command draws synergy from the war fighting capability of the services, the government resources and the expertise lying with the private sector. It is a hallmark of jointness and the enhancing unified mission effectiveness of the armed forces to meet their objectives in all the domains of warfare.

India is at the vanguard of cyber enabled attacks at its defence establishments – predominantly originating from the neighbourhood – having various geopolitical motivations. Given the growing competence and proficiency of non-state actors and exorbitant investments in cyber war fighting practices of the armed forces across the globe, the threat to cyber and information assets of Indian armed forces is imminent. Gaining wisdom from the experience of unified ANC and conscientious stride on the recommendations of the Naresh Chandra Task Force, India should align its cyber doctrine for the armed forces in tandem with the emerging reality. The Cyber Command should now move beyond the policy circles and start assimilating the assets, experiences, domain expertise and tenacity of the forces into a unified net-centric armed force.

---

[26]Over a dozen organisations are entrusted with Cybersecurity at various levels of governance, and these are: (i) National Information Board (ii) National Security Council Secretariat (NSCS) (iii) National Crisis Management

Committee (iv) National Cyber Response Centre (v) National Technical Research Organisation (NTRO) (includes the National Critical Information Infrastructure Protection Centre) (vi) National Disaster Management Authority (NDMA) (vii) National Cyber Security and Coordination Centre (viii) National Intelligence Grid (NATGRID).

Civilian Operations
NSCS/PMO/NCSC
CERT-IN
NATGRID/Cabinet Secretariat/MHA
NTRO/NCIIPC
Human Resources, Intelligence, Operation Planning and Execution
Responsibilities: Defence/Military Domain
Defend own Networks from espionage/attacks
Support unified operations/missions
Tri-services Headquarters
Cyber Command
Dispense Information, Support Agencies, Execute Operations
Defend or respond to cyber attacks of significant consequence
Responsibilities: Civilian Domain
Defence Operations
Army
Navy
Air Force
Ministry of Defence
Assets, Human Resources, Monitoring, Operational Information, Operation Planning and Execution
Technical Inputs and Human Resources (Training, Contractors, Projects, Technology)
Academia (NDU/ CoE/IITs)
DRDO
Industry
Technology, Research and Training (Capacity Building)

In the civilian domain, the Cyber Command is ought to work in tandem with the agencies dealing with cybersecurity and intelligence to keep a tab on any sort of conventional or asymmetric threat to either the defence networks or critical infrastructure. The agencies should be NTRO/NCIIPC for critical infrastructure, NSCS/PMO/NCSC for cyber related policies or crisis management, CERT-IN for updates on malware and their signatures, NATGRID/Cabinet Secretariat/ MHA for security and intelligence information. These agencies would lend or draw human resources, intelligence inputs, and conduct operations to or from the Cyber Command. Since, the requisite capabilities are spread across armed forces, governments, industry and academia, the Cyber Command has to draw in technology and capacity building in form of trainings and research from DRDO and Industry. Academia, comprising of National Defence University, Centres of Excellence in Cybersecurity and technology institutions have a very constructive role in raising the Cyber Command. Cyber Command should not just avoid interference with any of the existing apparatus, but share resources and expertise with its civilian counterparts as well.

The Cyber Command would need to have clearly defined objectives and responsibilities. These may be spread across both military and civilian domains. The first priority would certainly be to defend own networks from espionage or attacks to ensure information superiority during both war and peace. Subsequently, the Cyber Command would be tasked to support the unified operations of the tri-services or any of the services spread across land, sea, air, space and cyberspace, bringing in the element of jointness in war fighting. Perhaps, Cyber Command would have to respond to cyber attacks significant consequence on the civilian infrastructure as well, particularly the sectors deemed to be critical for the functioning of the state.

* Munish Sharma is an Associate Fellow (Cybersecurity Project), Institute for Defence Studies and Analyses, New Delhi

Strengthening India's Regional Footprint
The Need for a Clear Vision for Special Operations

Cmde Lalit Kapoor (Retd)*

Ever since the Naresh Chandra Task Force recommended, amongst others, creation of a Special Forces Command[1] and the Chiefs of Staff Committee recommended the creation of Space, Cyber and Special Operations Commands[2], a number of writers have explored the command and control issues of an Indian Special Operations Command (SOC), but not much else. That there is need to think through C2 issues is beyond dispute. Also beyond dispute is the need to reform India's security architecture, which a former Home Minister had described as comprising of political, administrative, intelligence and enforcement elements.[3] Reform of each of these elements is perhaps more important than C^2 reform: the political element lacks interest in and rarely has time for national security matters, believing that both conventional and nuclear wars are highly unlikely. A telling indicator of the seriousness with which the government views national security is provided by the statement, "a new NSAB is yet to be appointed" on the official NSAB website.[4] The administrative element, intended to deal with financial and administrative aspects, rather than focussing on building and fielding an effective military force, has concentrated (successfully) on excluding security professionals from security management under the guise of ensuring civilian control over the armed forces[5] . It has effectively usurped authority for policy decisions, without the concomitant accountability, leading to K Subrahmanyam saying, "Politicians hold power without responsibility, bureaucrats wield power without accountability and the army assumes responsibility without direction".[6] Too much has been written

---

[1]Brig Vinod Anand, "Defence Reforms and Naresh Chandra Task Force Review", see http://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review

[2]Col PK Vasudeva (Retd), "Increase in Para Special Forces Without a Unified Structure is an Exercise in Futility", see http://usiofindia.org/Article/?pub=Strategic%20Perspective&pubno=41&ano=2702

[3]P Chidambaram, "A New Architecture for India's Security", published by Outlook, 23 December 2009, see http://www.outlookindia.com/website/story/a-new-architecture-for-indias-security/263495

[4]See http://nsab.gov.in/?1003, accessed on 24 May 2016. The tenure of the last NSAB ended in January 2015.

[5]To paraphrase observation initially made by Stephen Cohen and Sunil Dasgupta in "The Drag on India's Military Growth", see http://www.brookings.edu/research/papers/2010/09/india-cohen-dasgupta

[6]As quoted by Admiral Arun Prakash (Retd) in "Civil Military Dissonance: A Chink in India's Armour", 3rd K Subrahmanyam Memorial Lecture, 20 Jan 2014, see http://www.globalindiafoundation.org/Admiral%20Arun%20Prakash%20Speech[1].pdf

about the failures of the intelligence[7] and defence industry elements (missed by the minister)[8] to bear repetition. A former Chairman COSC says, "One of the most worrisome aspects of India's national security scenario has been the sustained failure of India's vast military industrial complex, consisting of a large pool of DRDO scientists and network of sophisticated laboratories, backed by advanced production facilities of the Defence PSUs (DPSU), to deliver badly-needed capabilities to the armed forces".[9] The enforcement element, comprising the Armed Forces and internal security apparatus, has little voice in national security management.

Given the preponderance of sub-conventional threats to national security coupled with nuclear realities, the global tool of choice to militarily enforce a nation's will in the external environment, when the need arises, is Special Forces (SF). Use of SF for this purpose by numerous nations, particularly in Asia and Africa, has grown exponentially in the last decade or so. British SF are operating in Syria[10], Afghanistan[11] and Iraq[12]. The Russian Spetsnaz is operating in Syria[13] . Australian SF have operated in Afghanistan[14]. American SF have reportedly been involved in 147 countries[15] in 2015, to an extent that there are now calls for revoking Obama's Nobel Peace Prize due to his unprecedented use of illegal force through

---

[7]For an excellent overview of reforms required, see "A Case for Intelligence Reforms in India", IDSA Task Force Report 2012, http://www.idsa.in/system/files/book/book_IntellegenceReform.pdf

[8]Even the Prime Minister has expressed his disappointment at DRDO's performance, see Rajat Pandit, "World Won't Wait for You, PM Narendra Modi Tells Laggard DRDO", published by The Times of India, 21 August 2014, http://timesofindia.indiatimes.com/india/World-wont-wait-for-you-PM-Narendra-Modi-tells-laggard-DRDO/articleshow/40550218.cms.

[9]Admiral Arun Prakash, "Defence Reforms: Contemporary Debates and Issues", IDSA Monograph 'A Call for Change: Higher Defence Management in India', No. 6 July 2012, P 27

[10]Nick Gutteridge, "SAS Heroes Don Burkas for Raid on ISIS Bunker to Take Down Jihadi Chief", The Express, 18 Jan 2016, see http://www.express.co.uk/news/world/635517/Islamic-State-ISIS-SAS-burkas-raid-headquarters-Syria-Raqqa-jihadi-leader.

[11]Jonathan Reilly, "Brit SAS Heroes Kill 20 Taliban fighters During Firefight in Afghanistan" The Sun, 28 December 2015, see http://www.thesun.co.uk/sol/homepage/news/6825644/SAS-are-heroes-of-Sangin.html

[12]Will Worley, "British SAS Troops Injured Fighting ISIS Near Mosul In Iraq", see http://www.independent.co.uk/news/world/middle-east/british-sas-troops-injured-fighting-isis-near-mosul-in-iraq-a6857896.html

[13]Thomas Gibbons-Neff, "How Russian Special Forces are Shaping the Fight in Syria", The Washington Post, 29 March 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/03/29/how-russian-special-forces-are-shaping-the-fight-in-syria/

[14]Dylan Welch, "Inside the World of Australian Special Forces in Action and at Play", ABC News, 05 August 2014, http://www.abc.net.au/7.30/content/2014/s4061544.htm. See also Sam McKeith, "Australian Special Forces to be Investigated in 'Independent' ADF Probe", The Huffington Post, Australia, 17 April 2016, http://www.huffingtonpost.com.au/2016/04/17/sas-army-australia_n_9710610.html

[15]One report, quoting award winning American journalist Nick Turse, indicates that they were involved in 147 countries in 2015. See http://www.democracynow.org/2015/11/13/tomorrows_battlefield_as_us_special_ops

[16]Nat Hentoff and Nick Hentoff, published by ATO Institute, 20 May 16, see http://www.cato.org/publications/commentary/revoke-obamas-nobel-peace-prize

SF.[16] Recent missions they have undertaken include Operation Neptune Spear, the killing of Osama bin Laden in Abbotabad in May 2011[17] , the rescue of Ali Haider Gilani[18], son of the ex-PM of Pakistan and the killing of Mullah Mansour in Pakistan.[19] French SF are reported to be in Libya.[20] Canadian SF are operating in Iraq.[21] Turkish SF are operating in Syria.[23] UAE's SF are reported to be operating in Yemen, Afghanistan and Somalia.[24] India has been a somewhat cautious and reluctant participant in this trend, notwithstanding the retaliatory operation in Myanmar on 09 June 2015. It has yet to internalise the wisdom of the recent words of the British Prime Minister, David Cameron, who said, "You do not protect people by sitting around and wishing for a better world. You have to act in this one. And that means being prepared to use military force where necessary" .

It is, then, no surprise that the call to create a SOC, so far limited to veterans of the Armed Forces and informed sections of the media, has not found resonance at the political level. Though much has been written about the synergy that the SOC will provide as well as changes required in India's Higher Defence Organisation, this may not suffice to persuade the political elite to overcome institutional inertia and create the competence to translate the change it will involve into tangible national security outcomes. Numerous preparatory aspects must be addressed at the national level before the SOC comes into being, including the changing nature of national security threats; identity, role and missions of SF; politico-legal and oversight issues; intelligence reform; equipment and technology requirements; command and control; HR aspects and many more. Each of these aspects merits

---

[17]See "Operation Neptune Spear", http://www.globalsecurity.org/military/ops/neptune-spear.htm

[18]Salman Masood and Mujib Mashal, "Son of Pakistani Ex-Prime Minister, Kidnapped in 2013, is Rescued", The New York Times, 10 May 2016, http://www.nytimes.com/2016/05/11/world/asia/pakistan-ali-haider-gilani.html?_r=0

[19]BBC News report, "Taliban Leader Mullah Akhtar Mansour Killed, Afghans Confirm", 22 May 2016, see http://www.bbc.com/news/world-asia-36352559

[20]Paul taylor and Mark Heinrich, "French Special Forces Waging Secret War in Libya: Report", Reuters, 24 February 2016, http://www.reuters.com/article/us-libya-security-france-idUSKCN0VX1C3

[21]Lee Berthiaume, "Military Defends Letting Media Show Pictures of Canadian Special Forces in Iraq", National Post, 09 May 2016, see http://news.nationalpost.com/news/canada/canadian-politics/military-defends-letting-media-show-pictures-of-canadian-special-forces-in-iraq

[22]"Turkey Confirms Special Forces Operations in Syria", report in The World Weekly, 09 May 2016, see http://www.theworldweekly.com/reader/view/newswire/2016-05-09/turkey-confirms-special-forces-operations-in-syria/7804

[23]William MacLean, Noah Browning and Yara Bayoumy in "Yemen Counter-terrorism Mission Shows UAE Military Ambition", Reuters, 28 Jun 2016, see http://www.reuters.com/article/us-yemen-security-emirates-idUSKCN0ZE1EA

[24]"David Cameron Announces £2 bn extra Funding for Special Forces over next five years, ITV Report, 16 November 2015, see http://www.itv.com/news/2015-11-16/david-cameron-announces-2bn-extra-funding-for-special-forces-over-next-five-years/

a detailed study in itself. This article addresses the identity, role and missions of SF.

The start point must lie in defining who comprises SF and what they can be tasked to do. This is particularly relevant in India, where a number of units described as SF operate under different ministries. The Army has the Para Commandos and the Ghatak Force, the Navy has MARCOs, Air Force has Garuds, the Ministry of Home Affairs has the National Security Guard (NSG) and Indo Tibetan Border Police (ITBP), the Cabinet Secretariat has the Special Protection Group (SPG) and the Special Frontier Force (SFF), CRPF has COBRA battalions and the Parliament Duty Group, the Maharashtra Government has Force One and many states have Anti Terrorism Squads (ATS). Each brings to bear different specialised skill sets, albeit with some commonality. There is need to separate internal security missions, which will inevitably come under the Ministry of Home Affairs and the concerned state in view of India's federal character, from missions outside India, which will usually be conducted by the Indian Armed Forces. But India has successfully duplicated and muddled external security responsibilities: the NSG Act of 1986 (Article 6)[25] , the ITBP Act of 1992 (Article 7)[26] and the CRPF Act of 1949 {Article 7(2)}[27] all permit the utilisation of these internal security forces outside India and the evident contradiction in MHA controlled forces being tasked for extra-territorial operations seems to be lost on our lawmakers. All can also be used for "performing such other duties as may be entrusted to it by the Central Government"[28], leading to "lack of coordination, turf wars, ego problems and wasteful expenditure"[29]. In this context, the comments of an erstwhile Union Home Secretary questioning the limitations of institutional structures following the Pathankot terror attack are relevant[30], as is a former Chairman COSC calling it an addition to India's 'Hall of Shame'[31] .

---

[25]Sourced from http://mha.nic.in/hindi/sites/upload_files/mhahindi/files/pdf/NSGAct1986.pdf

[26]Sourced from http://itbpolice.nic.in/itbpwebsite/Documents/ITBP-Act.pdf

[27]Sourced from http://mha.nic.in/hindi/sites/upload_files/mhahindi/files/pdf/crpf_act1949.pdf

[28]In accordance with relevant acts cited above

[29]Air Marshal Narayan Menon, "India's Special Operations Capability", published by Indian Defence Review, 09 February 2014, see http://www.indiandefencereview.com/spotlights/indias-special-operations-capability/0/

[30]Dhirendra Singh, "Why India Needs an NSA Who is Duly Empowered but Also Knows His Limits", in the Wire, 26 January 2016, http://thewire.in/2016/01/26/why-india-needs-an-nsa-who-is-duly-empowered-but-also-knows-his-limits-19916/ . See also Rajit Ojha, "Force Alarm: The Many Failings of the National Security Guard", published by 'The Caravan', 01 February 2016, http://www.caravanmagazine.in/perspectives/force-alarm-failings-national-security-guard

[31]Admiral Arun Prakash, India's Civil Military Dissonance: Road to Perdition", published by The Sentinel, 24 January 2016, http://www.sentinelassam.com/editorial/story.php?sec=3&subsec=0&id=255093&dtP=2016-01-25&ppr=1

No one grudges highly trained units involved in internal security tasks equivalence in perquisites and allowances, but this need not translate into equating them with SF for operational purposes. Dilution of SF identity to include Central Armed Police Forces further blurs the distinction between the police and military maintained by every other great power, with deleterious consequences[32]. For the purpose of this article, SF are defined as military units trained and equipped to conduct special operations with an emphasis on unconventional warfare. Special operations in turn, as described by the United States Special Operations Doctrine[33], "require unique modes of employment, tactics, techniques, procedures and equipment. They are often conducted in hostile, denied, or politically and/or diplomatically sensitive environments and are characterised by one or more of the following: time sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk".

Linked with the confusion in identity is confusion in role of SF. The Indian Army doctrine states[34], "The SF are specially selected troops who are trained, equipped and organised to operate in hostile territory, isolated from the 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". It goes on to identify missions that could be assigned to SF as follows[35]:-

(a) Conventional War. Strategic and tactical surveillance of vital targets, early warning of enemy activity in depth areas, denying strategic or operational assets and terminal targeting by precision munitions.

(b) Low Intensity Conflicts. Seek and destroy missions including trans-border operations.

(c) During Peace. Hostage rescue, anti-terrorist operations and assistance to friendly foreign governments.

The Indian Maritime Doctrine[36] states, "SF are elite units designed to progress operations in remote areas that are hostile, defended, culturally sensitive and beyond the reach of naval forces, both in time and space. Special Operations

[32]For an overview of the consequences, see Admiral Arun Prakash, ibid.

[33]JP 3-05, US Special Operations Doctrine, 16 July 2014, P ix, https://fas.org/irp/doddir/dod/jp3_05.pdf

[34]Indian Army Doctrine Part 2 – 2004, para 4.13. Sourced from https://file.wikileaks.org/file/india-army-doctrine-part2-2004.pdf

[35]Ibid, Para 4.15

[36]Indian Maritime Doctrine, NSP 1.1, updated online version 2015, P 96, sourced from http://indiannavy.nic.in/sites/default/files/Indian-Maritime-Doctrine-2009-Updated-12Feb16.pdf

entail use of SF to target military-strategic or vital operational assets of the enemy, towards attaining the military objectives. SF operations can be a separate mission and can also comprise a set of tasks in support of a range of other missions. Marine Commandoes (MARCOs) of the IN can undertake SF operations, as part of specific missions. They may also be tasked for combating terrorism in a maritime environment including rescue of hostages. The Indian Maritime Strategy 2015 states, "The Indian Navy is cognisant of the strategic and operational potential of SF Operations. The Indian Navy's MARCOs have significant capabilities for undertaking SF Operations in the maritime domain, as well as on land and by air. They can operate independently and in conjunction with Army and Air Force SF, including against non-state actors. Development of MARCO capabilities will remain a thrust area for the Navy[37]".

The Basic Doctrine of the Indian Air Force states[38], "IAF Special Forces are highly trained and are equipped to carry out specific operations, in offensive and defensive roles. They operate in small numbers but the payoff s from a successful operation are generally much higher given the size of the forces involved. They generally operate independently or in close coordination with other forces at the operational level". It goes on to say, "Though the Special Forces are primarily to be used for offensive operations, the conditions for their employment are flexible. Some of these are Surveillance and reconnaissance, Combat and peace time search and rescue missions, Counter Terrorism, Destruction and degradation of enemy air assets (DEAA), Special missions in the interest of IAF, sister services and the nation, Protection of IAF high value assets, and Emergency response force".

Each service has evidently framed its doctrine in isolation, from its own perspective, keeping in mind what it anticipates it may be called upon to do. This inevitably leads to considerable duplication of effort and wastage of national resources. An example of this wastage is the independent and separate purchase of UAVs by the IAF, the Army, the Navy and later by NTRO from Israel, at different costs, and duplication of repair and maintenance facilities by all except NTRO, whose UAVs are reportedly unusable.[39] There is a Joint Doctrine for Special Force operations, published by HQIDS in 2008.[40] Unlike its American counterpart, this is not available in the public domain. The absence of coherent national vision for SF operations is striking. This gap needs to be filled on priority.

---

[37]"Ensuring Secure Seas: India's Maritime Security Strategy", P 141

[38]Basic Doctrine of the Indian Air Force 2012, P 101, sourced from http://indianairforce.nic.in/pdf/Basic%20Doctrine%20of%20the%20Indian%20Air%20Force.pdf

[39]Air Marshal Narayan Menon, Op Cit

[40]Sandeep Dikshit, "Joint Doctrine For Special Forces Unveiled", The Hindu, 02 October 2008, see http://www.thehindu.com/todays-paper/tp-national/joint-doctrine-for-special-forces-unveiled/article1349699.ece

"Most people—and, indeed, many policymakers—associate the special operations forces with secret night-time raids like the one that targeted Osama bin Laden: tactical operations against a particular individual or group. The abilities of special operations forces, however, extend much further...[41]". Twelve core operations and activities are assigned to the United States Special Operations Command (USSOCOM)[42], including Direct Action, Special Reconnaissance, Countering WMD, Counterterrorism, Unconventional Warfare, Foreign International Defence, Security Force Assistance, Hostage Rescue and Recovery, Counterinsurgency, Foreign Humanitarian Assistance, Military Information Operations and Civil Affairs Operations[43]. India's operating environment is different from that of USA. Absence of internal security challenges permits the American SF to focus on the external environment. India does not have that luxury: India's Armed Forces remain heavily involved in internal security operations and will remain the tool of the last resort, when other forces fail, for the foreseeable future. Nor does India have the overwhelming superiority in military power over all potential adversaries that USA enjoys. Consequently, the priorities and missions for India's SOC will differ, even though many of the core missions will remain the same. There is, at the outset, clear need for identification of the missions that are likely to be assigned to the SOC and determination of the lead agency for each.

This identification could be done by parliament, by way of law, as in the American Goldwater Nichols Act of 1986 and the Nunn-Cohen Amendment to the National Defense Authorisation Act of 1987, which mandated the creation of a new four-star command to be activated to prepare Special Forces to carry out assigned missions and, if so directed, to plan and conduct Special Operations. It also gave the new command specific authorities and responsibilities[44]. It is noteworthy that the American Congress chose to legislate rather than recommend change through a non-binding resolution conveying the sense of the House. This followed the testimony of Maj Gen Richard Scholtes, who had retired as the Commander of the Joint Special Operations Command during Operation Urgent Fury in Grenada. Scholtes spoke extensively about the misuse of SF, the complete failure of conventional commanders to understand and appreciate the capability of these forces and the command and control disasters of the Grenada operation[45] . Similar

---

[41]Richard Haas, foreword to Linda Robinson's "The Future of US Special Operations Forces", published by Council on Foreign Relations, April 2013, http://www.cfr.org/special-operations/future-us-special-operations-forces/p30323?cid=ppc-Google-grant-csr_robinson_special_ops&gclid=CK-Ms7u51MwCFdgmvQodDxwAfw

[42]Joint Publication 3-05, Special Operations, 16 July 2014, pages II-1 – II-17, see https://fas.org/irp/doddir/dod/jp3_05.pdf . The old April 2007 version of this doctrine is available on HQ IDS website, at http://ids.nic.in/doctrine.htm.

[43]An elaboration of these operations and activities can be found at JP 3-05, ibid.

[44]USSOCOM Factbook, P 6, sourced from https://fas.org/irp/agency/dod/socom/factbook-2009.pdf

[45]Susan Marquis, in "Unconventional Warfare: Rebuilding US Special Operations Forces", published by Brookings Institution, 1997, P 144

views about the sub-optimal utilisation of SF for routine tasks by India's military leadership have been expressed by experienced Indian SF officers[46]. Is there evidence to assume that India's conventional commanders are better than their American counterparts in this regard?

Identification could also be done by India's Ministry of Defence, but it lacks domain knowledge and, as experience has shown, is averse to letting any Armed Forces organisation come into direct contact with decision-making levels. It could be done by the Armed Forces, but in India as in USA, it is rare for an SF officer to rise to senior levels and chances are that the decision would be made more based on individual whims than on reasoned evaluation. Finally, it could be left to the circumstances of each case, which will inevitably extract a heavy price from the units tasked to carry out operations by way of casualties and result in the SOC being tasked for missions for which it is neither trained nor equipped. The nation and its leaders have to choose.

To quote an erstwhile Minister who has held the Defence, Finance and External Affairs portfolios, "strategic decision making is the function and responsibility of a small political-military class alone"[47]. In India, however, the political elite has consciously failed to develop the interest, vision or expertise required to evolve policies that can effectively tackle the complex internal or external security challenges facing the country. "Apart from a few individuals, no political party has built a cadre of strategic thinkers, which is in sharp contrast to China – where their one single party has a tradition, starting from Mao, of concentrating on military and strategic issues with a long-term perspective"[48]. The military elite, on the other hand, has been completely marginalised under the guise of retaining civilian control, as brought out earlier in this article. This leaves a bureaucracy without the requisite background or training the effective advisory body for strategic decision-making, without the concomitant accountability. Until this fundamental shortcoming is addressed, there can be no clarity on the missions that the SOC may be tasked with.

A primary requirement, then, is for clear political direction on the identity, role and missions of India's SF. The multiplicity of agencies, each with its own operational experience, budget, equipment, Standard Operating Procedures and training standards, among others, inevitably leads to internecine competition, turf battles, lack of synergy and the need to learn the same operational lessons time and again. Consequently, institutional expertise, vital for the nature of tasks SF perform, has

---

[46]See Lt Gen PC Katoch, "Modernisation of India's Special Forces", United Service Institution of India Strategic Yearbook 2016, published by Vij Books India Pvt Ltd, ISBN 978-93-84464-87-5

[47]Jaswant Singh, in "Defending India", MacMillan India Ltd, 1999, P1

[48]Dhirendra Singh, Op Cit.

not emerged. As said by a veteran, "In a whole set of seminars held over the years, the need, necessity, imperatives, quantum and control of special forces required has actually not been addressed holistically. ... Resultantly, a clear cut policy for employment of Special Forces at the national level has not been evolved, partly because of lack of strategic forethought and partly because the controlling masters of the various SF are cozy in their respective turfs and cocooned environment"[49]. India's leaders would do well to recall the words used by Lord Amery in a telegram to Lord Linlithgow, then the Viceroy of India, regarding British action during the Quit India movement, "Twice armed is he that hath his quarrel just, but three times he who gets his blow in first[50]". A nation that depends only on the creation of consensus or diplomatic effort to resolve contentious regional issues and is otherwise perceived as toothless is unlikely to engender respect even in the immediate neighbourhood, leave alone in the wider world.

There are signs of change. Speaking to Indian Heads of Missions of conflicts in the twenty-first century, the Prime Minister said there were new "actors" and new "threats" to global peace and prosperity, and added that India, which always stood for "Vishva-Bandhutva" and peace – the brotherhood of the world – had a great responsibility in helping the world counter these challenges to peace[51]. Around the same time, Shri Shiv Shankar Menon, the erstwhile National Security Adviser wrote, "I have no doubt that sooner rather than later India will have to make real political and military contributions to stability and security in this region that is so critical to our economy and security. What has inhibited us since the seventies have been limited capabilities and the fact that other states were providers of security in the area. Now that both those limiting factors are changing, our approach and behaviour should change in defence of our interests"[52] . When India's approach and behaviour does begin to change, the understanding will come that Special Forces (SF) are amongst the vital tools required to militarily change the external and internal environment and an effective SOC will finally emerge.

*Cmde Lalit Kapoor is a former DACIDS, HQ IDS

---

[49]Lt Gen PC Katoch (Retd) and Saikat Dutta, "India's Special Forces: History and Future of Special Operations, Vij Books India Pvt Ltd, 2013, P 119.

[50]Narendra Singh Sarila, "The Shadow of the Great Game: The Untold Story of India's Partition", Harper Collins Publishers India, P 134. The original quote is "Thrice armed is he that hath his quarrel just, but four times he that gets his blow in first" from William Shakespeare in "Henry IV, Part II, Act 3, Scene 2".

[51]http://www.mea.gov.in/press-releases.htm?dtl/24765/Prime_Ministers_message_to_Heads_of_Indian_

[52]Outlook India, 23 January 2016, "We Must Now Choose", see http://www.outlookindia.com/website/story/we-must-now-choose/296484 , sourced on 01 May 2016.

Joint Operations Capability: Need for a Special Operation Command

Maj Gen Dhruv C Katoch, SM, VSM (Retd)*

Special Forces (SF), as the words connote, are forces required for Special Operations. As defined by the US military, "Special Forces are forces organised, trained and equipped to conduct special operations with an emphasis on unconventional warfare capabilities. Special Operations encompass the use of small units in direct or indirect military actions focused on strategic or operational objectives. They require units with combinations of trained specialised personnel, equipment, and tactics that exceed the routine capabilities of conventional military forces. They are characterised by certain attributes that cumulatively distinguish them from conventional operations.[1]

Special Operations have been executed across the world in various conflict situations with telling effect. Not much is known about what actually happens in such operations, till the time information on the subject is declassified, which may take many years. Such operations have been used in support of military operations, such as SAS (Special Air Services) operations conducted by Britain in World War II, which entailed parachuting trained soldiers behind enemy lines to gain intelligence, destroy enemy aircraft and attack their supply and reinforcement routes.[2] Britain has used her SAS in various operations thereafter, ranging from the successful rescue of hostages from the Iranian embassy in London on 5 May 1980 (Operation Nimrod), to various interventions across the world, to include the Falklands campaign, the Gulf Wars, interventions in Bosnia and Sierra Leone and the ongoing conflict in Afghanistan and Iraq. The US too has made effective use of its SF in furtherance of their political and military objectives as have Russia, Israel and others.

Some SF operations, by their very spectacular outcome, have captured the imagination of the world. Operation Thunderbolt, launched by Israeli commandos on 4 July 1976, which led to the rescue of over 100 hostages held by pro-Palestinian terrorists at Entebbe airport in Uganda is one such. The killing of Osama bin Laden

---

[1]US Special Operations Forces Reference Manual, Chapter 1, available at http://fas.org/irp/agency/dod/socom/sof-ref-2-1/SOFREF_Ch1.htm

[2]For details, see Shortt and Mcbride, The Special Air Services, Osprey Publishing.

by US SEAL Team Six[3] on 2 May 2011 in Abbottabad, Pakistan, is another. The examples given above simply highlight the myriad nature of SF operations, which cover the entire spectrum of conflict, from hostage rescue to conventional conflict, insurgencies and counter terrorism operations.

The Indian Context

India has been engaged in various forms of conflict post independence till date. Four wars with Pakistan, one with China and a series of insurgencies in Northeast India and later in Jammu and Kashmir has seen the consistent employment of India's military in various types of operations since independence. In India's heartland, the Central Armed Police Forces are deployed to quell Maoist inspired violence. However, Special Forces have rarely been employed for the roles that they should or could perform, largely because of lack of understanding of the nature of SF operations.

A brief distinction must here be made of Special Forces and Airborne/ Parachute regiments. Regular parachute battalions are not SF, as once landed or paradropped, their role is akin to that of regular infantry - to hold ground till a link up is established.[4] As clearly stated by Lt Gen. R.K. Nanavatty, when he was the Northern Army Commander, "a parachute battalion is simply an infantry battalion in airborne role and has nothing in common with a Special Forces battalion".[5] The Indian paradrop of 2 Para Group in Tangail in the 1971 Bangladesh Liberation War, was thus not a SF operations.[6] It is important to understand this role distinction. While SF would of necessity have to be capable of insertion by paradrop, the corollary does not apply.

It would be useful to contextualise the role of SF in the Indian context. From that would emerge the justification of the quantum of force required to be raised and maintained as also its equipping needs and requirement of support structures for mission accomplishment. Some of the missions given to SF may also be politically sensitive, wherein failure may lead to loss of national prestige. Obviously such missions will have to be undertaken with great care, at the behest of the political authority. This further underlines the need for manning the SF with elite personnel

---

[3]A US Navy special forces unit, that officially operates under the cover name Naval Special Warfare Development Group

[4]http://www.indiandefencereview.com/news/equating-airborne-forces-with-special-forces/

[5]As quoted by Lt Gen. PC Katoch in his article "Equating Airborne Forces with Special Forces", available at http://www.indiandefencereview.com/news/equating-airborne-forces-with-special-forces/

[6]For details of the operation, see Lt Gen. Nirbhay Sharma, "The Story of the Indian Army's First Airborne Assault", in Maj. Gen. Dhruv C Katoch and Lt Col Quazi Sajjad Ali Zahir, ed. LIBERATION, Bangladesh 1971, (Bloomsbury, India, 2015), pp133-140.

and the best possible equipment and support structures for task accomplishment.

In conflict situations, SF can be effectively employed in support of conventional operations, to shape the security narrative. Their correct utilisation is however of paramount importance. If utilised correctly, they achieve spectacular results. Used poorly, their capabilities and sometimes their lives are wasted.[7] In the US military, the SF have time and again proved their utility to the ongoing conflict in Afghanistan. They were instrumental in evicting the Taliban from their hides in the Tora Bora cave complex, with support from the Northern Alliance. This, in the words of a former U.S. Army Green Beret, 'sent shockwaves through the conventional military', and brought home to the policy makers the strategic value of SF Operations and encouraged the integration of such forces into broader operational planning.[8] This trend is increasingly being seen in the U.S. and is likely to grow to 'achieve greater impact with lighter footprints'.[9]

The Indian experience in SF operations has been far less demanding than those of the US and other countries despite the fact that India's security challenges could have done with far greater employment of Special Forces. When employed, India's SF have been spectacularly successful, but the fact that India has not made more use of this very potent capability, highlights shortcomings in the understanding of what such operations can achieve. Among the successes notched up by India's SF, Operation Cactus, launched to neutralise the coup attempt by a group of radicals, was successfully executed within 16 hours of getting the first information, at a place 3000 kms away! This undoubted ranks as one of the most professionally executed operations by SF across the globe, but unfortunately, this capability was not built upon and exploited. Lesser known but conducted with equal competence was an operation carried out against Indian insurgents hiding in the jungles of Myanmar in June 2015. Here, after crossing the international border, the SF struck at two groups of Indian insurgents, the NSCN(K)[10] and the KYKL.[11] Many insurgents were eliminated, both the hideouts were destroyed and the Force exfiltrated thereafter without suffering a single casualty. While the SF operation at Maldives suggested Indian capability to be a net security provider in the region, the cross border operation in Myanmar signalled political willingness to pursue hostile targets beyond India's borders.

---

[7]Steven P. Bucci, "The Importance of Special Operations Forces Today and Going Forward:, available at http://index.heritage.org/military/2015/important-essays-analysis/importance-special-operations-forces-today-going-forward/

[8]Whitney Grespin, 'The Quiet Professionals: The Future of U.S. Special Operations Forces' , available at http://www.diplomaticourier.com/the-quiet-professionals-the-future-of-u-s-special-forces/

[9]Ibid.

[10]NSCN (K) - National Socialist Council of Nagaland (Khaplang), is a Nagaland based terrorist organisation.

[11]KYKL - Kanglei Yawol Kunna Lup is a Manipur based terrorist organisation.

The Indian military however continues to use its SF personnel as regular infantry, which belies an understanding of what such forces are meant for. As recently as February 2016, SF personnel were employed to flush out a small group of terrorists who had taken refuge in a building in Pampore after attacking and killing some police personnel. Such operations are best dealt with by regular infantry units. In the Pampore encounter, two SF officers lost their lives while trying to enter the building, which made for good propaganda for the terrorists, in comparing their forces with own SF.

While the role of SF remains imperfectly understood within the military, in the domain of civil policy makers, there is a complete lack of comprehension of their role and functions. SF need to be employed to pursue strategic objectives, for which they must be organised and trained. In war, they could be employed in a variety of ways behind the enemy lines, in furtherance of military objectives. This could include striking at enemy leadership, destruction of enemy strategic assets, supporting elements inimical to the enemy within his depth areas and the like. As part of anti terrorism and anti insurgency operations within the country, they could be employed in black/ grey operations to neutralise leadership elements within hostile groups, in disinformation campaigns, in operations to eliminate financial, moral and material support to such groups, anti hijacking operations and the like. In out of area contingencies, they could be used in response to requests for support by neighbouring countries, anti hijacking operations in the seas, rescue missions and for joint operations with friendly countries for specific missions.

Joint operations with friendly forces in an interconnected world is increasingly becoming the norm. A prime example is the mission carried out by joint forces of Russia, Iran and Syria to rescue a Russian Su-24 fighter pilot who had ejected over insurgent held territory after his aircraft was shot down by turkey for violating Turkish air space. The pilot's location was identified six km deep inside territory held by the FSA (Free Syrian Army), through his Personal Locator Beacon - a handheld radio that contained a beacon transmitter. The ground element of the rescue operation consisted of 24 commandos, six of whom were from Hezbollah's special operation unit and 18 were Syrian commandos. To assist the ground force, the Russians electronically sanitised the area, stretching to several kilometres from the target area, to blind all hostile satellites and communication equipment in the area of operations. The EW effort from the air was provided by a Russian marine EW detachment, which primarily resorted to GPS and communication jamming, to prevent western satellites from picking up details of the rescue mission and leaking it to the FSA/ rebels.[12] The success of this operation, completed within 12 hours, brings out many important lessons for SF. Besides having well trained SF ready for

[12]http://en.farsnews.com/newstext.aspx?nn=13940905000553.

operations at all times, there is also need for quick decision making and exploiting technology to assist the task force.

Role for the SF

Greater role clarity is required if India's SF are to be exploited to the full extent of their capability. The Army's SF consist of nine parachute (SF) battalions. The operations conducted by Para (SF) in Maldives and along the Indo-Myanmar border, as highlighted in this paper were brilliant, but they continue to be employed in less demanding tasks, which are well within the purview of regular infantry units. The Indian Navy has its Marcos (Marine Commandos), created in 1987. The force was employed during the 2008 Mumbai terror attacks, but lack of role clarity led to sub optimal results. The Garud Commando Force, the SF for the Air Force, was primarily created to protect Air Force installations from terrorist attacks. Their performance against terrorists in the Pathankot terror attack was again suboptimal, which again points to lack of role clarity. In addition, we have the National Security Guards (NSG) Commandos, who are trained for anti hijacking operations. These are personnel from the armed forces, led by military officers on secondment to the Ministry of Home Affairs. There is a need to bring all such forces under a common umbrella for optimal functioning and role clarity.

While the military must continue to focus on conventional conflict, present commitments point to greater involvement in operations at the lower end of the conflict continuum. Here too, a shift is taking place from high-visibility, heavy presence interventions to more refined capacity enhancement initiatives and surgical direct action missions. This is where the SF can play an important role. What is required is to synergise the assets of the different Services under one overarching command, as has been done by the U.S., which grouped their SF assets under SOCOM (Special Operations Command), headquartered in Tampa, Florida to unify coordination.

Conceptually, an Indian SFC (Special Forces Command), could plan, coordinate and execute Special Operation missions within India and abroad, as part of an overarching strategy to serve interests that could have a strategic reach/ purpose. Missions could range from hostage rescue and out of area contingencies to intra service joint operations as well as joint operations with friendly forces. They would also encompass special missions targeted at various militant and insurgent outfits within the country. In conventional conflict, they could be employed as part of the larger plan to achieve a strategic purpose. The SFC would need to coordinate its activities with other national agencies whose assets would be required to support SF missions. These could be in the domains of space, cyber, intelligence, media or others, as also with the three services, the para military forces, the central armed police forces, the state police forces and most importantly, with the political authority.

As a concept, the SFC could look into the following:

- Work in close coordination with the political authority and the military in shaping the operational narrative.
- Training and equipping of the force in conjunction with the concerned Service, for operations across the spectrum of conflict.
- Focus on eliminating the nation's enemies, in cooperation with intelligence agencies. All such activities to be coordinated at the highest political level.
- Disruption of terrorist groups through targeting their leadership.
- Train indigenous groups within the region in unconventional warfare and assist them in building a guerrilla force.
- Partner friendly countries and help them build their capacities to provide for their own defence. Here, it would be beneficial to have units oriented towards specific countries, who possess advanced training levels; language capability and cultural knowledge of the host country and to seek to develop rapport between own SF personnel and those of the host country to create an informal special operations network. This would also help to build trust with friendly countries in furtherance of strengthening the relationship as such relationships are based on trust.
- Creating synergy amongst the SF for joint operations.
- Promoting consistent engagement through small-footprint, distributed operations,
- Managing the support networks.

Capabilities sought to be created must be commensurate to the envisaged tasks. Mere numbers do not matter. What is required is a small number of well trained SF personnel, possessing a broad range of skill sets, with the right hardware to achieve the mission. It would be good to remember that SF cannot be mass produced. Neither can they be created once an emergency occurs. This small elite force must be in a state of high mission readiness at all times. The type of non-SF support that would be required for the mission, such as maps, electronic sanitisation of areas, real time satellite imagery, intelligence etc. must be pre-coordinated and made available in real time from the respective agencies involved.

Conclusion

SF can play a useful role in shaping the security narrative. Their roles must be clearly enunciated and the requisite wherewithal provided in terms of training and

equipping the force to enable successful mission accomplishment. It is essential that the unique nature of their operating philosophy is clearly understood, both by the political and military leadership, and the force is provided the requisite support from within other agencies as may be required by them.

The aspect of a centralised overarching control headquarter (SFC) for all SF assumes significance in the light of present day challenges that we are facing and will likely face in future. The SFC must be mandated to optimise resources, ensure operational dominance and accomplishment of the mission in acceptable time frames. Creating aSFC will go a long way in enhancing national security and must be taken up on priority.

*Maj Gen Dhruv C Katoch (Retd) is a veteran army officer who served as the Director of CLAWS. Presently, he is the Editor of SALUTE Magazine.

Special Operations Command
A Strategic Imperative

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

Much has been written and deliberated by the Armed Forces and defence strategists over the years on the need to empower and equip India's Special Operation Forces (SOF) to make them a force multiplier, a game changer, a rapid deployment force, a threat in being, and a major component of our Comprehensive National Power, however, not enough has been done.

On 03 November 1988, 50 Independent Parachute Brigade/ 6 Battalion,The Parachute Regiment spearheaded Operation CACTUS (Maldives) to rescue the then President Mr Maumoon Abdul Gayoom, and restore the duly elected government of Maldives after Abdullah Luthufi had taken over the island nation in an early morning coup. The operation launched conjointly by the Army, Navy and the Air Force was successfully accomplished without a single casualty. Consequent to Op CACTUS, Time magazine carried a cover story on 03 Apr 89 acclaiming India as a regional power. The success of this operation at home mostly went unnoticed as did a few important lessons learnt. Had it failed, maybe India too, would have created structures and organisations to exploit the full potential of SOF to safeguard national interest and assets. The United States established the US Special Operations Command (USSOC) comprising the SOF of the three services and Marines, in the aftermath of the failure of Operation EAGLE CLAW to rescue American diplomats held hostage at the US Embassy at Tehran in April 1980. Ever since , the US SOF as an integral part of USSOC have spearheaded and projected US hard power across the world safeguarding the national interests. The synergy and the structured jointness of USSOF and command and control also ensured a flawlessly planned and surgically executed Operation GERONIMO to neutralise Osama Bin Laden at Abbottabad, Pakistan in May 2011. As Op CACTUS was executed with surgical precision and total success, it failed to highlight the most important lesson, the need for a tailor made joint organisation, comprising all elements of SOF fully integrated ,equipped, trained and designated under a single command and control structure, with direct access to the countries highest decision making body (CCS) .

MOD Website on India's security environment overview defines the strategic space. Quote *"India's size, strategic location, trade interests in a security environment that extends from Persian Gulf in the West, to the States of Malacca in the East and from the CAR in the North to near the Equator in the South, underpin India's security response. In view of the strategic spread, it is essential for the country to*

maintain a credible land, air and maritime force to safeguard its security interests." India's security concerns are impacted by a dynamic global and regional security environment. As India transforms from an emerging and rising power to a risen responsible power, it will need credible military capabilities to project military power, assist friendly foreign countries in times of crisis from unconventional threats, HADR and assuming the role of net security provider in the region.. The continuing proxy war with Pakistan, the ever increasing and omnipresent threat from terrorists, the imperative to safeguard our national interests and assets dictate that we enhance capacities and build capabilities to face future threats and challenges.

India boasts of the second largest Army, the fourth largest Air Force and a blue water capability for the Navy to ensure our territorial integrity against external threats and internal security. What the nation lacks is a credible rapid deployment and effective Special Operations capability, to meet emerging security challenges in the regional and global context.

What are special operations; these can be defined as *"Unconventional military operations, undertaken in a hostile or politically sensitive environment, to achieve political and military objectives at national, strategic and operational level and to safeguard economic interests. Their arena extends the complete spectrum of conflict and ranges from direct action to covert and clandestine operations. These are undertaken mostly in concert with other elements of national power"* As such operations have international and national ramifications, it is essential to create an appropriate political understanding. The national polity needs to comprehend the options and the associated risk sensitivity compared to out of proportion results and limited escalation dynamics. As India has grown in stature and economic power, it will become more and more vulnerable to unconventional and terrorist threats on its nationals and assets around the world. It is now an imperative to synergise the SOF under a single command to meet future challenges. The structure of SOF is a major indicator of a nation's will and capabilities to safeguard its interests, the capability to project hard power and political signalling.

Each Service has their own SOF which have grown over the years. These are service specific and more often than not, there is competition and conflict of interests, rather than cooperation and coordination, be it their roles and tasks, equipping, training and command and control. Existing SOF of the Armed forces include nine Parachute (Special Forces) Battalions and five Parachute Battalions of the Army, an 800 strong Marine Commando Force (MARCOS) organised on the concept of the US Marine SEALS and a 1000 strong IAF Garud. The NSG (SAG) and the Special Group manned and led by the Army for internal security and hostage rescue are under the MHA. These are elite forces, where every man is a volunteer, highly trained and motivated. This force is among the most battle hardened and combat rich force equal to if not better than the best in the world. The SOF are both force multiplier and substituter. These forces provide the theatre commanders with a low cost option to target high value military objectives in depth areas, thus giving the much needed strategic and operational reach during war. At present, SOF are assigned missions at the strategic, theatre and operational level and tasked to

execute direct action, intelligence, surveillance and reconnaissance tasks during war to delay, disrupt and destroy high value targets in depth areas. During peace they are mandated to execute CT and CI operations, special reconnaissance, hostage rescue, capability building of FFC, and above all, training for war.

There is a plethora of SF in the Indian security context. Without debating on the quality and requirement of the over two dozen self styled and self proclaimed SF ranging from the State Police and the CAPF, the focus of this paper will remain on the SOF of the Armed Forces.

The Air Force has enhanced its lift capability with the induction of the C-130J Hercules and C-17 Globe Master in addition to the already in service IL-76 and AN-32 Aircrafts, thus giving the country the requisite reach to effectively intervene and safeguard our national interests in the regional and global context. The Indian Navy too, is in the process of acquiring four landing craft/multi role support vessels at a cost of 2.6 Billion USD and nine Japanese ShinMaywa US2 amphibious aircraft, to upgrade the maritime lift capability for SOF and Amphibious operations. To fully exploit this credible lift capability, the strategic reach and a battle hardened, combat rich elite SOF there is an urgent need to have integrated structures to effectively safeguard our national interests as mandated.

In 2012, the Naresh Chandra task force recommended creation of a Special Operations Command (SOC), Cyber and Space Commands. With the Modi led NDA government demonstrating an urgency and resolve to address National Security concerns, it is hoped that the three commands, as recommended will be finally sanctioned. Defence Minister Manohar Parrikar in an interview to a TV Channel has committed to pushing for a long overdue CDS. This will pave the way for an effective command and control structure and the much needed jointness and synergy.

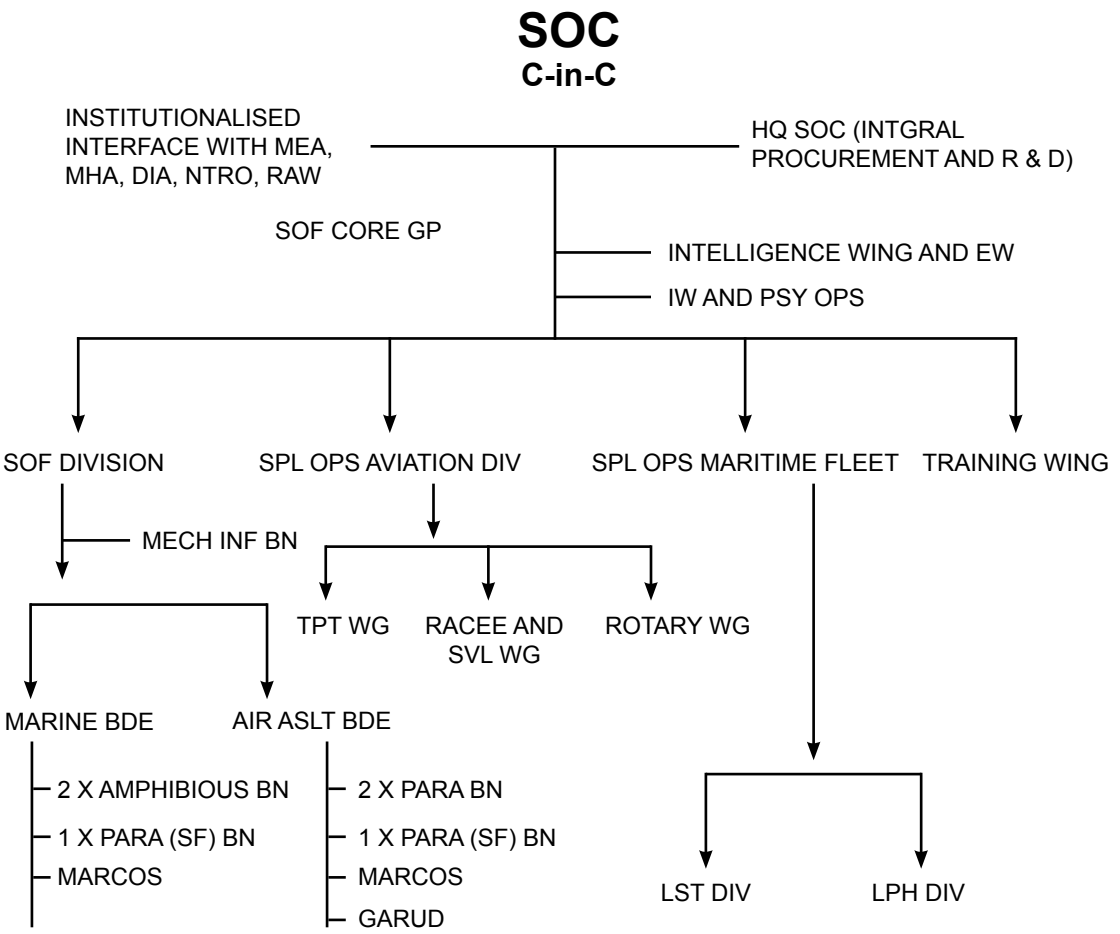
The key question is - Is India as a nation and the Armed Forces fully exploiting the potential of our SOF? A clear and concise answer is NO. There are three major causative factors which need to be addressed.

The major weakness is the lack of a lean and mean, agile and versatile joint force under a single commander. This can be achieved by reorganising part of the SOF under the SOC. The SOC should be structured and organised as a truly integrated tri-service command under the CDS with integral lift capabilities. The roles assigned to the SOC in pursuance of the national security objectives would be power projection and intervention to safeguard our national interests and assets in the region. Assistance to friendly Foreign Countries (FFC), albeit on invitation and augment the war effort.

The tasks assigned to SOC during war could be to secure/destroy high value targets in strategic and operational depth in furtherance of national military objectives. During peace, or rather no war no peace the SOC will be the first responder to any emerging or impending threat to our national interest in the region. The scenarios for its employment could include hostage rescue of Indian nationals and diplomats,

evacuation of Indian nationals, a situation recently faced in Syria. The evacuation from Syria was carried out without any direct military intervention, however, there could be situations wherein military intervention will be required to secure an airhead or an harbour or ensuring safety of Indian nationals pending evacuation. Additional tasks envisaged are, reinforcement or assist in evacuation of United Nations Peacekeeping Missions, assist FFC from threats by inimical elements within, albeit on invitation, assist in HADR missions in the region and beyond and capacity building of Armies of FFC. The SOC should also be responsible for development of SOF doctrine and training. Given the envisaged roles and tasks the SOC should have a direct access to the national decision making body (CCS) in times of crisis.

A suggested outline organisation of SOC is as under :-



The SOF in this model have only certain essential elements of the SOF placed under the direct command of the SOC, while the services continue to retain a major portion of the SOF for the theatre battle and internal security. However there is a need to have inbuilt flexibility for the SOC to take under command additional SOF when required. It goes without saying that joint training during peace is a prerequisite.

Secondly, the constant and continuous employment of SOF in CT and CI Operations is a major detractor. The need for live situation training and combat experience aside, the focus on CT Operations is detrimental to the combat edge, attitude and training required for the primary tasks in war. In effect, on account of the award and reward system of the Armed Forces, CT Operations is the preferred deployment for the Para and Para (SF) battalions, the Garud, Marcos and the Special Group. These tasks adversely impact the focus, training, preparation and planning for war. The SOF should be sparingly employed in CT Operations and that too for specific high risk critical missions. The Services should at the same time, incorporate systems to compensate the SOF cadres in their career progression.

Another major area which needs to be urgently addressed is making up critical equipment voids. SOF are woefully short of equipment, with critical deficiencies in firepower, communications, surveillance, insertion capabilities and mobility. The SOF requirement is of low population, high technology arms and equipment. The procedures to procure equipment for SOF are the same as for all other arms and equipments as per the DPP 2013. This has obviously resulted in near zero procurement. Indigenous development of high technology equipment is not attractive enough for DRDO and OFB due to the limited quantities required. In any case the inordinate delays in development by DRDO leave the services with little option other than imports. It has been over two decades since the Army has been trying to procure essential arms and equipment for the SOF, like combat free fall parachutes, small arms, sniper rifles, light strike vehicles, underwater diving equipment, communication equipment, laser target designators, heavy drop equipment and ATGMs. These still remain in various stages of procurement or development. Even low technology equipment like Parachute Jump Boots and Airborne Helmets being indigenously developed continue to be in the development and trial stages for over two decades. The criticality has been compounded with the raising of additional Parachute and Parachute (SF) units. The envisaged procurements have not kept pace, leading to the existing inventory being rationalised, in effect the poverty has been shared. A proposal to fast track procurements by empowering a special committee, similar to the special clothing and equipment committee for Siachen, has been under consideration with the government for over three years now. It is difficult to comprehend as to how the MHA succeeds in procuring state of the art weapons for the CAPF, where in the MOD succeeds only in delaying all procurements, even of similar weapons which are in service with the CAPF. It is

hoped that this will get corrected by the impetus to modernisation and priority in making up critical voids accorded by the Defence Minister.

The creation of a SOC is a strategic imperative as India embarks on the road to be a responsible and risen regional power.

*Lt Gen Vinod Bhatia (Retd) is Director CENJOWS. He is a Former Director General Military Operations (DGMO), and Colonel of the PARACHUTE REGIMENT

Note: A similar Article by the author was earlier published in the the April 2015 issue of FORCE Magazine.

CENJOWS
CENTRE FOR JOINT WARFARE STUDIES

(Web sit: http:// www.cenjows.in Email: cenjows@yahoo.com)

APPLICATION FOR LIFE/ ANNUAL MEMBERSHIP

To,
The Director
Centre for Joint Warfare Studies (CENJOWS)
Room No.65, Kashmir House
Rajaji Marg, New Delhi 110011

Dear Sir,

1. Please register me as a Life ☐ /Annual ☐ member of the Centre for Joint Warfare Studies (CENJOWS).

2. I undertake to abide by the Rules and Bye Laws of the Institution.

3. My particulars are given below:-

(a) Name in full ……

(b) Address:-

(i) Office/Unit……

……

Pin Code …… Phone No ……

.

(ii) Permanent/Residential ……

……

Pin Code…..... Phone No …… Mobile No(Optional)……

(iii) Email ……

Optional Fields

(c) Parent Service Army/Navy/Air Force/Civil Services …….....…….…..

(d) Rank/ Designation…….……...…. (e) Decorations …….....…….……....

(f) Appointment ……...……. (g) Personal Number ……...……..…....

(h) Date of Commission ……...…….. (j) Serving/Retired……...……..……

4. Areas of expertise or interest:-

(a) ……..……..

(b) ……

(c) ……..……

5. Any other information that may be of interest to the CENJOWS (including important exposures):-

…….....…….……..

……..……

6. Proof of my identity (Copy of passport/ voters ID Card/ Aadhar Card) will be produced after approval of membership.

7. The following are enclosed:-

(a) Demand Draft/Cheque in favour of CENJOWS payable at New Delhi:-

(i) DD/Cheque No…….....…….dated….....……

(ii) Amount …….....…

(iii) Drawn on …….....……Bank.

(b) Two stamp sized photographs for membership card.

Place : …….....…...……

Date : …….....…...

Yours faithfully,

FOR OFFICE USE ONLY

Identity Card/Document No: …….....…….. To be verified by Secretary.

New Delhi

Date …….....….. Secretary, CENJOWS

Accepted/Rejected

Membership Number ……..…….

New Delhi

Date …….....….. Director CENJOWS

Note:-

1. Life membership is presently open only for members of Joint Fraternity viz. officers who are serving or have served in any capacity with HQ IDS since its inception.

2. Membership Fees:-

(a)	Life Membership		-	Rs 1500/-
(b)	Annual Membership:-			
	(i)	Veterans of the Joint Fraternity	-	Rs 500/-
	(ii)	Serving Offrs	-	Rs 300/-
	(iii)	Serving Offrs of the Joint Fraternity	-	Rs 200/-
	(iv)	Members of Govt Services	-	Rs 500/-