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 : www.cenjows.gov.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$**

ISO 9001:2015

WWW.CROWNSOLAR.COM

ORIGINAL EQUIPMENT MANUFACTURER

PROVIDING SECURITY SOLUTIONS TO THE NATION

CROWN SOLAR IS A LEADING BRAND IN THE FIELD OF POWER FENCE SYSTEMS IN INDIA. WE ARE BASED IN HYDERABAD AND HAVE BRANCHES TO COVER ALL STATES IN INDIA FOR AFTER SALES SERVICES.

WE ARE THE APPROVED OEM FOR DEFENCE SECTOR
AND OUR PRESTIGIOUS INSTALLATIONS INCLUDE

- NAVAL DOCKYARD
- INS HANSA
- NAVAL AIRCRAFT YARD
- WEAPON EQUIPMENT DEPT
- AIRFORCE STATIONS
- SHIP BUILDING CENTRE
- INS DEGA
- MATERIAL ORGANIZATION
- HAL UNITS
- MILATARY ENGG. SERVICES
- INDIAN NAVAL ACADAMY
- MANY MORE...

CROWN SOLAR POWER FENCING SYSTEMS

123/A, USHODAYA TOWERS, SHAPURNAGAR, JEEDIMETLA,
HYDERABAD-500055. INDIA. PHONE: +91 40 23091373 / 23195702.
www.crownsolar.com; Email: Chandra©crownsolar.com; crownsolar@yahoo.com
MOBILE - +919391016607

Celebrate the Festival of more!

pnb Festival Bonanza

More savings More opportunities to upgrade your life

Full waiver of

- Upfront / processing fees
- Documentation charges on

Housing

Car

Two Wheeler Loans

PNB Mera Apna Bank

Virat Kohli

*Conditions apply

For Banking Services & Products Dial **0120-2490000** or All India Toll Free No. **1800 180 2222, 1800 103 2222**
SMS **PNB PROD** to **5607040** @indiapnb www.pnbindia.in

पंजाब नैशनल बैंक ...भरोसे का प्रतीक !

punjab national bank ...the name you can BANK upon !

FUTURE SECURITY CHALLENGES OF INDIA

Garden Reach Shipbuilders & Engineers Ltd.

(A Govt. of India Undertaking)

43/46, Garden Reach Road, Kolkata-700 024
Tel : +91-33-2469 8100 to 8113, Fax : +91-33-2469 8150, Website : www.grse.nic.in

MAKE IN INDIA

RAKSHA MANTRI'S AWARD FOR EXCELLENCE 2015-2016

IN-HOUSE DESIGN EFFORT FOR
OFFSHORE PATROL VESSEL FOR MAURITIUS

Anti-Submarine Warfare Stealth Corvette Built for Indian Navy

INS Kiltan

First Ever Warship Built in India Using Carbon Composite Super Structure – INS Kiltan

Landing Craft Utility Ship for Indian Navy

INLCU L-52

Second LCU, L-52 delivered with "NIL" Shipyard Liability & Weapon & Sensors Trial Completed

WARSHIPS

★ Frigates ★ ASW Corvettes ★
★ Missile Corvettes ★ Offshore Patrol Vessels ★
★ Landing Ships ★ Fast Attack Crafts ★
★ Survey Vessels ★

ENGINEERING PRODUCTS

★ Pre-Fabricated Steel Bridges ★ Railless Helo Traversing System ★
★ Boat Davits ★ Capstans ★ Anchor Windlass ★

For Further Information Please Contact
Deputy General Manager (Mktg. & CC/CCP)
Tel: 033-24691177/Ext. 311 • Mob.: 8420008819 • Fax : 033-24696975 • E-mail : marketing@grse.co.in

In Pursuit of Excellence & Quality in Shipbuilding

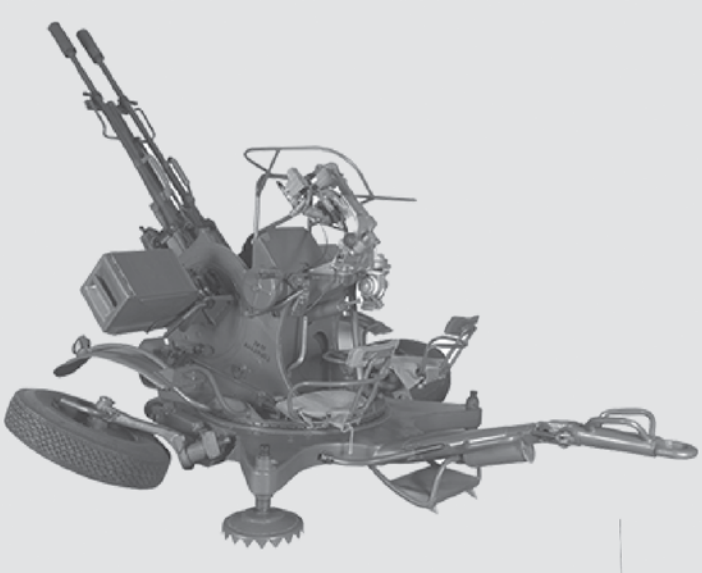
Silver Jubilee International Seminar

Directorate of Army Air Defence

AIR DEFENCE INDIA 2018

Kothari Auditorium, DRDO Bhawan, New Delhi
26-27 July 2018

Integrating New Technologies and Optimizing Legacy Systems



- Air Threats and Challenges
- Countermeasures
- New Technologies and Weapon Systems
- Upgrades to Legacy Systems
- Air Defence Battle Management
- Indigenisation

25 1994 2018 Silver Jubilee

Army Air Defence Corps

Event Partner

INDIAN MILITARY REVIEW IMR

Industry Assn Partner

HARMONY PROGRESS DEVELOPMENT PHD CHAMBER Estd. - 1905

www.imrmedia.in/events

CONTENTS

FOREWORD

FUTURE SECURITY CHALLENGES OF INDIA

Eternal vigilance is an imperative to ensure national security. A vigilant nation should identify emerging security challenges much before they manifest and endanger the people. Existing challenges often mutate to form new ones in more serious forms. External security threats posed to India by China and Pakistan take a new shape on account of collusion and collaboration. China is posing new challenges especially in space and cyberspace domains while Pakistan sustains and reinforces the Proxy War expanding the scope and sphere. Internal security challenges created by insurgents and Maoists often encouraged and abetted by external forces inimical to India also keep changing forms and modus operandi. A wholesome assessment can enable India to ensure effective capability building and capacity enhancement to ensure continued peace.

A nation is often alert to the expected external and many internal challenges. The economic, technical (Cyber, IW, Space, ICT, and Autonomous Weapons) and non traditional challenges (Water, Food, Energy, Demographic Dividends/Disaster, Climate Change, Health and Education, Security of National Interest – Terrorism, Migration, Piracy and Drugs trafficking) often assume dangerous proportions, threatening national security.

India has to initiate proactive and pre emptive measures against future security challenges. Efforts to identify the future security challenges of India through well researched articles written by outstanding,

experienced and domain specialist authors, in one volume of synergy journal is a laudable endeavour. The articles cover future security challenges in the Indian Context, from multi domain warfare, China, Pak, collaborative threat, Maritime, Space and Outer Space, Cyber, technological threats and the changing role in UN peace keeping.

(Satish Dua)
Lt Gen
CISC & Chairman CENJOWS

EDITOR'S NOTE

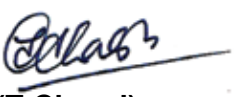
The dictum "Forewarned is forearmed" is true for a nation state too. Identification of existing and emerging security challenges is essential for fine-tuning a strategic response. Canvas of security challenges to India is perhaps the broadest among the large and fairly developed nations. Contested borders with the colluding nuclear weapon states demand the wisdom of a genius to keep the nation out of harm's way. Consolidation from a fragmented polity of princely hue to a modern emerging global power while facing varied security challenges is no mean achievement of the people of India. While old challenges still persist, many more have also emerged and assumed threatening proportions. Along with traditional land, sea, undersea and air domain challenges, space and cyberspace challenges with all pervasiveness demand new responses. Therefore, this issue of the Synergy Journal is devoted to identify the major future security challenges of India.

The case of "Building Capabilities and Deterrence for Threats from China" has been analysed by Maj Gen Umong Sethi and the "Essentials of Pakistan's strategic Security Policy and how this needs to be countered by India" have been outlined by Lt Gen Syed Ata Hasnain. "China-Pakistan Strategic Nexus - Collaborative Threat: India's Two Front Dilemma" has been detailed in depth by Lt Gen Vinod Bhatia including policy options for India. Security challenges emerging from ICT technologies, Autonomous Weapons and the Cyberspace have been explained from various angles by Air Mshl PP Khandekar and Lt Gen Arun Sahni respectively. Development as a panacea will have to address the non traditional security challenges holistically. Challenges such as Economic, Water, Food and Energy Security have been elaborated by Brig Rahul Bhonsle. Globally, ccurrent and future challenges of UN peacekeeping affect all nations in some way or the

other. India has been contributing substantially to the UN Peacekeeping Missions over the years. Lt General Chander Prakash has brought to the fore, issues involved in these missions.

CBRNe threats with colossal destruction capability have not only persisted but are increasing by the day. Brigadier (Dr.) Rajeev Bhutani in his scholarly article has touched upon all aspects of these challenges. Also, IOR is an area of great significance for ensuring security of India. A recent naval agreement with Singapore is a step in this direction. “Relevance of India-Singapore Naval Agreement for Addressing Future Security Challenges of India” has been brought out by Vice Admiral Pradeep Kaushiva. The question of Demographic Dividends or Disaster has been debated on several occasions in various forums. Brigadier Navjot Singh has explained this subject in detail through his essay on “Demographic Dividend–India’s Silent Security Challenge for Future”. India’s Future Security Challenges from the Outer Space are multiplying by the day. Gp Capt GD Sharma has studied this subject from all angles and recommended a course of action for India. Days of assessing future security challenges from single domain seems to be coming to an end as more and more platforms and entities responsible for their command and control are interconnected, sharing information on real-time and getting assistance from self learning machines. Multi Domain Warfare therefore is a logical outcome. Dr Manabrata Guha has written a scholarly essay on this subject giving a broad overview of the shape of things to come.

There are many more emerging security challenges such as hypersonic weapons and Directed Energy Weapons which need attention not only from technology development entities but also in the war planners and war fighter forums. This issue of the Synergy Journal is also intended to highlight this aspect.



(T Chand)
Air Cmde (Retd)
Editor

BUILDING CAPABILITIES AND DETERRENCE FOR THREATS FROM CHINA

Major Gen Umong Sethi, AVSM, VSM (Retd)*

In Asia, power play between major powers is manifesting in multi-domains. China wishes to create a unique place among comity of nations that commands 'awe and respect'. Her growing national capabilities have resulted in greater display of assertiveness and increased involvement in world affairs. Vigorous promotion of 'Belt and Road Initiative' is indicative of promoting core national interests. Any spin-off advantages from the endeavour accrued to the partner nations are incidental but projected as intentional. India has always considered South Asia her sphere of influence. The dynamics are fast changing as a result of Chinese forays into South Asian neighbourhood. Investments, strident propagation of 'belt and road' initiatives by partnering with more countries than originally envisaged and mediation on the Rohingya and Afghan disputes are impacting the geo-politics of the region. A post-Doklam analysis by IDSA states, 'On the ground it is increasingly evident that China, through its economic bullishness, is trying to impose itself culturally in South Asia, and this should worry India more than the military brinksmanship. Because shared culture and history have always been the links that legitimized India's status as a natural leader of South Asia.[1]

China has strongly underscored claims to territories along its continental borders and its maritime periphery. As her economic prowess increases and military capabilities grow, experts anticipate more assertiveness in pressing territorial claims in ways that challenge

1 Post Doklam, India needs to watch china's bullish economics led cultural embrace of South Asia, IDSA Issue Brief January1, 2018

many of the existing paradigms. It is instructive to note the comments of Yuan Peng, Vice President, China Institutes of Contemporary Relations at an event to discuss the recent National Congress of the Communist Party of China, "China will remain 'assertive and strong' on territorial issues, including incidents like the stand-off with India in Doklam. Safeguarding territory is core interest and we will always be assertive and strong because there is no room for compromise on these issues. In the past we thought that we will shelve differences and now we can face them squarely." Yuan said China would safeguard territorial interests in an incremental way. "Even if we can shelve differences, the other party may not do so or agree to do so. So we can face them head on and safeguard our legitimate interests."[2]

G Parthasarathy, a former Indian diplomat has commented, "The rise of Chinese power and China's territorial assertiveness, both on land and sea, are disturbing and need to be addressed strategically. Beijing now claims that its territorial frontiers with India extend across the entire state of Arunachal Pradesh, with its borders lying just adjacent to the strategic Siliguri corridor in the east, while also claiming large tracts of Ladakh in the west." He goes on to say, "Chinese "assertiveness" on its maritime boundary claims across the South China Sea is accompanied by its growing naval presence, including nuclear submarines, across the sea lanes of the Indian Ocean, extending from the Straits of Aden, where China has established a naval base in Djibouti, across the Straits of Hormuz to the Straits of Malacca."[3]

China watchers have inferred her behaviour towards boundary issues is characterised by a multi-pronged strategy that follows a trajectory of 'creating precedence and set of rules; legitimising the

2 http://indianexpress.com/article/world/china-territorial-issues-india-china-doklam-stand-off-yuan-peng-4939472/ Written by Apurva | Beijing | Published: November 16, 2017 6:18 am

3 http://www.tribuneindia.com/news/comment/getting-around-beijing-s-ways/498129.html Posted at: Nov 16, 2017, 12:39 AM; last updated: Nov 16, 2017, 12:39 AM (IST)

claim by legal and historical arguments; aggressive diplomacy and propaganda; expand the conflict and then negotiate'.

In absence of delimitation, delineation and demarcation, India China boundary has potential for different interpretations and hence Doklam like incidents might recur. China is likely to adopt a mix of customary and legal approach for justifying claims in future. She has demonstrated willingness to accept or reject legacy treaties in a given situation to her advantage. Exploiting the Tibetan and Buddhist cultural card in the future is something that cannot be ruled out. China's sensitivity to the SLOCs implies Beijing's willingness to assert presence in areas of strategic interest such as the Indian Ocean Region more particularly the Andaman Sea and funnels as the Malacca Straits. However, it is also a truism that a number of agreements for maintaining peace and tranquillity, CBMs and Special Representatives meetings between the two countries have prevented an armed confrontation over the years. Due credit must be given to the maturity of military-diplomatic-political construct of both the countries that has not allowed border situations to spiral out of control.

Prudent caution dictates that India continues to identify triggers that may lead to a possible military confrontation along the land borders. It would be pragmatic to undertake a similar exercise for the maritime domain as well. The analysis should take due note of President Xi's message to the People's Liberation Army at the 19th National Congress of the Communist Party of China "to become a modern fighting force by 2035, the world's best military force by 2050; and, intensify its combat readiness by focusing on how to win wars."

The reorganization and regrouping of PLA is likely to enhance its capabilities in the medium to long term. In the short term, reorganization of the Western Theatre Command is a work in progress and is likely to remain a weakness until it is fully ready to conduct of joint operations. Transition of command and control, integration of the PLA Rocket Force (PLARF) and the Support Force into to the joint set- up are likely to

poise challenges.[4] Modernisation and emphasis on 'Jointness and informationisation' is likely to contribute to achieving strategic surprise and conduct of fast paced, precise operations at comparatively short notice. The ever improving state of infrastructure and added importance being given to joint logistics will further enhance capability of PLA to conduct operations swiftly and sustain over long periods. However, due to nature of geography in Tibet, build up and forces are likely to remain vulnerable to aerial detection and threat from air power as well as missiles. The inherent weaknesses in the force structures of PLAAF in terms air-refuellers, radar coverage abetted by low load capacity of aircrafts operating from the plateau will render PLAAF at a disadvantageous position vis a vis the IAF for at least a decade or so.

The PLAN has a formidable fleet of nearly 70 submarines and has acknowledged 'Brown water' capability. The force is rapidly transforming itself into a 'Blue water Navy' with acquisition of aircraft carriers, tankers and fleet support ships and serial production of Landing Dock Platforms (LPDs). Her ability to mass produce naval platforms in a relatively short time stands proven having produced as many as 64 platforms in 2013-14. The 'string of pearls' and facilities at Hambantota, Gwadar and Djibouti lend it capacity to operate with ease in the Indian Ocean Region. China owns largest number of merchant ships flying her flag in the world giving her phenomenal capacity to trade and enhance national wealth.

China will have to take cognisance of a few security concerns in case of a military confrontation with India. Strategically, notice will have to be taken of alliances and partnerships of US in the neighbourhood; India's expanding economic and military capabilities; status of Indian influence over her neighbouring countries; asymmetry that exists vis a vis Bhutan where China does not have diplomatic relations and India has considerable clout and a treaty for defence. From conduct of operations perspective, concerns would include, catering for both the continental

4 Kevin McCauley. Snapshot: China's Western Theatre Command. Publication: China Brief Volume: 17 Issue: 1. Jamestown Foundation USA.

and maritime borders - a 'la two front scenario' with appropriate resources tailored to ward off threats along the Eastern seaboard and vulnerable Sea Lines of Communications (SLOCs) in the Indian Ocean. Second, the fringes along her periphery are not fully integrated into the national main stream and possibility of foreign support to fan ethnic dissent in these areas will have to be considered. Third, terrain configuration of the plateau poses enormous challenges for conduct of ground as well as air operations. Lastly, exterior lines of communication and logistics challenges would manifest adversely despite availability of pre-dumped stocks.

A crisis along Indo-Tibet border could manifest in many forms. It could be in the form of a local crisis that does not endanger overall national security; posing threat to Indian vulnerabilities; a punitive operation for strategic signalling; conflict with strategic intent of seizing claimed or disputed area(s); or even to ward off any perceived threat to SLOCs. The nature and timing of crisis will take cognisance of state and status of India's national leadership, military capability and other vulnerabilities at the time of choosing of unfolding of the crisis. The endeavour will be have an assured degree of success as the Chinese will not like to lose face. To that end, detailed planning and build-up of forces, networks and logistics is likely to precede any such exertion. Availability of very good infrastructure and appropriate forces within easy reach would abet undertaking small scale military operations at short notice.

Post Doklam, an article by Long Xingchun, Director at the Centre for Indian Studies at China West Normal University, in the Global Time brought Pakistan and Kashmir into the narrative for the first time. He wrote, "A 'third country's' Army could enter Kashmir at Pakistan's request, using the "same logic" the Indian Army used to stop the Chinese military from constructing a road in the Doklam area in the Sikkim sector on behalf of Bhutan."[5] Though this seems a conjecture in response to Indian MEA's statement of June 30, 2017 giving out the rationale and

5 //economictimes.indiatimes.com/articleshow/59517202.cms?utm_source=-contentofinterest&utm_medium=text&utm_campaign=cppst

highlighting Indo-Bhutan treaty obligations, it would be prudent to take a note of it as a possibility. When seen in light of development of China-Pakistan Economic Corridor (CPEC) and huge stakes China has in the project, this prospect might be 'constructed to manifest' in order to coerce India or to undertake a collaborative military action in the garb of 'coming to aid on request' of Pakistan.

Bertil Lintner in his article on Sino-Indian War of 1962 mentions, "Once across the border, it was also apparent that the Chinese had detailed knowledge of the terrain, where the Indian troops were stationed, and how to best attack them….China depended entirely on human intelligence collected by its agents in the field, which would have taken time in the North-East Frontier Agency [NEFA]'s rough and Roadless terrain. But China's agents would also be confined largely to areas where the local population spoke languages and dialects related to Tibetan. It was nearly impossible for the Chinese to penetrate most parts of the NEFA where the local tribal population spoke other, non-Tibetan languages and dialects.[6] Hence, due notice must be taken of Chinese attempts to espouse religious-spiritual-ethnic-cultural linkages of Tibet with Ladakh, Sikkim, Bhutan and Arunachal Pradesh. Cultivating influential spiritual heads and exploiting traditional linkages of monasteries with inhabitants on the Indian side is a distinct possibility.

China is making rapid strides towards 'informationisation' of weapon systems, battlefield and all other aspects of warfighting. Taking cue from past incidents in the world to use cyber prowess to take over control of critical infrastructure, security analysts would do well to cater for such an eventuality also. Chinese have made significant investments in India's telecommunications, surveillance (CCTV cameras and access control systems) and power generation sectors. They are keen to make more investments in other sectors of infrastructure as well. India is live

6 China went to war against India on this day 55 years ago. But the planning began much earlier-Bertil Lintner https://scroll.in/article/854615/china-went-to-war-against-india-on-this-day-55-years-ago-but-the-planning-began-much-earlier Oct 20, 2017 · 12:30 pm

to the threat and is revisiting policy for awarding contracts to foreign firms. CEA Chairman R.K. Verma is reported to have spoken about the possibility of a crippling cyber-attack on India's power systems being a key consideration while re-drafting the new policy for awarding contracts to foreign players.[7]

Developing capabilities to preserve India's territorial sovereignty and strategic interests in the wake of any attempt by adversary(s) to alter the status quo ante with a view to impede country's march to become a prosperous nation calls for developing a long term vision and relevant national security strategy. In order to achieve that in a vibrant democracy, political consensus and continuity of policy irrespective of the party in power is a fundamental necessity. This is assuming greater importance with time as the stakes of being an emerging power manifest in manner unknown hither-to-fore. As can be inferred from experience of other democracies, greater involvement of political class in matters of national security impels greater understanding of national security dynamics and brings about closer parliamentary scrutiny and oversight. The aim is to ensure that the Executive Wing of the government remains on course to develop capabilities and provides resources accordingly. It would also bring the entire security establishment including the Armed

Forces to greater accountability and lead to developing more efficient ways and means of war avoidance and war fighting in a technogically fast changing world.

Dissuasion and deterrence are two sides of the same coin. Both concepts are vital in the Indian context. Deterrence and dissuasion result from the cumulative effects of capability development. In that, building capacity of forces, developing infrastructure, logistics and transportation across land, sea and air, cultivate employable capabilities in cyber, space, Special Forces, and nuclear domains assume ascendency over

7 http://www.businesstoday.in/current/economy-politics/india-silently-countering-chinese-influence-on-its-sensitive-markets-china/story/258565.html

others. Force enhancement of Air Power and Navy's power projection capability must proceed as planned.

In order to anticipate crisis before it develops, use of predictive techniques should be made. Predictive crisis anticipation will require creating data bases that have information of terrain, historical record of events, weather, environmental factors and responses from real time multi-domain, surveillance and communication networks (capable of withstanding sustained cyber and electronic interference) as well as human intelligence. These inputs will be processed using big data analytics to create algorithms that can forecast the next crisis. This will become a reliable tool to assist Commanders take appropriate pro-active or pre-emptive actions. India should take measures to plug vulnerabilities that can be exploited using the ethnic and cultural construct with people of border areas. They must be made partners in the endeavour.

Developing capabilities and infrastructure is both time consuming and cost intensive. Warfighting doctrines guide development of force structures, accoutrements and new technologies hence, these must be developed keeping a specified time perspective in view. Capability outcomes should be clearly enunciated for all organs of Armed Forces with an aim to deter war, win one if it comes and in the interim dissuade the adversary from any misadventure.

Development of defence science and technology by partnering with and academia and private industry is critical need of the day. Identification of critical technologies including non-lethal ones that render networks paralysed and new weapons to be developed in a time bound manner must be put on mission mode. In order to boost indigenous development of weapons and equipment prototypes should be used for further research. A clear plan for technology leapfrog should be developed. Trends indicate developments of BoTs, artificial intelligence and machine learning for military purposes have the potential to transform the battle space. In this regard, India's prowess as 'software giant' needs to be exploited by seeding research by the industry. Policy

frame work should be designed to allow the industry to commercially market the 'spin off' technologies for civil use. A leap in military robotics and artificial intelligence can be leveraged to acquire other state of the art technologies that are needed.

Theatre and infrastructure development in areas close to the border is quite inadequate. Both need to be developed synergising the resources of the Centre and concerned State by catering to the needs of both the local populace and Armed Forces. An integrated plan for developing facilities that can cater to both and manned by locals can boost economy and bring down costs. While developing facilities, due care needs to be taken to take into account the fragile ecology that may give away and cause great environmental disasters of the kind that occurred in the form of mud slides in Leh in 2010.

Aerial lift capacities will have to be enhanced to support rapid deployment of forces as it might not be possible to keep large number of troops deployed for prolonged periods due to environment that exists in bordering areas. An integrated plan of transportation, transit facilities, landing strips, heli-dromes and logistics needs to be implemented to aid rapid reaction. It will be useful to create capacity to rapidly deploy a brigade group in a theatre in the medium term. Jointness in logistics if brought about will enhance sustainment and improve ability to beat adversary's time frame of operations

It is recommended to pillar military strategy on deterrence, early warning and predictive border management; leverage technology, develop infrastructure and enhance capability of Armed Forces to dissuade misadventures in the short and medium term and deter it in the long term. War and diplomacy are closely intertwined. Therefore warfighting and negotiations will have to be combined to control and limit escalation. The interplay between the two will need orchestration and the strategic levels. India needs to develop new linkages and structures in the higher direction of war architecture for rhythmic play of various elements of national power. The Integrated Staff at HQ IDS should be

considered as the military wing of the government in the decision making process. Capacity building of leaders and staff and re-structuring of the crisis management design at the highest level needs to be addressed.

In conclusion, various dimensions of Sino-Indian competition, collaboration and contest are beginning to unfold. The relationship is likely to change its dynamics as capacities, roles in the international arena, alignments and orientation of the two undergoes changes over time. It would be imperative for India to dissuade and deter any attempt to undermine her sovereignty and peaceful rise by sophisticated application of military force, diplomacy and other elements of national power. To aid and abet such an endeavour a long term view need to be taken to build capacities of the Armed Forces, strategic and operational surveillance and fires, theatre development, joint logistics and above all, new structures duly empowered to guide actions during a crisis or conflict be put in place.

***Major Gen Umong Sethi (Retd)** is well known Defence Analyst

PAKISTAN: CHALLENGES & STRATEGIES

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

A generic essay on the essentials of Pakistan's strategic security policy and how this needs to be countered by India

There is an interesting anecdote about the partition of India and the creation of Pakistan. It is said that when the first Chief Justice of Pakistan was appointed he decided he would rather function from New Delhi than any future capital of Pakistan. The assumption obviously was that there was nothing serious about the creation of Pakistan and the situation would probably retract in a few years, if not a few months. The lesson – even those at the apex level, involved in Pakistan's foundation, remained unconvinced about the new state. That unfortunately has remained the situation with Pakistan; never has it been able to come to terms or picked itself up to seriously set goals and achieve tenable aims to create peace for its people and give them an honorable national identity. Much less populous than India and far less diverse in terms of demographics it continues to remain beset with ethnic, sectarian and ideological issues which have threatened to tear it apart. True democracy eludes it, although regular elections have been held for the last two decades or so. Its Army has never detached itself from political power which it exercises on the back of its direction of the nation's foreign and security policy. Lessons from the Indo Pak Conflict of 1971 and the loss of its former eastern half never seem to have dawned on it. Instead of launching into a campaign of nation building it has preferred to remain mired in a self-defeating game with intent of seeking retribution against India who it blames for its loss of face, dignity as a nation and half its territory and population.

Retribution drives Pakistan's India policy; more correctly retribution drives the Pakistan Army's approach towards India. While civil society in

Pakistan does harbor traditional animosity it is willing to move on for the sake of the nation and future generations; the Pakistan Army is not. From the memory of 1971 is drawn the energy for retribution which helps keep the Army center stage in the complex social and political labyrinth of Pakistan. That contributes to power and at the end it's only a power game which drives Pakistan's relations with India. Joining the Army in its policy of using India as prop for its power are willing politicians and the judiciary besides retired generals, diplomats, bureaucrats and two of Pakistan's most powerful entities – the Inter-Services Intelligence (ISI) and the Inter -Services Public Relations (ISPR). This conglomeration often referred as the deep state also has a clutch of radicals and terrorists all designated as friendly to Pakistan's interests. Some of the strangest perceptions of national security prevail in the Pakistani nation and the core center of the perceived threat remains India. It is around this threat that Pakistan has built its entire security policy.

The Jammu & Kashmir (J&K) issue helps drive the agenda of antipathy against India. If generational change and civil society's natural progression and aspirations tend to dilute this antipathy, J&K helps exacerbate it. It needs to be remembered the Pakistan Army adopted the strategy way back in 1977 and thence onwards whereby it accepted its incapability to challenge India in the conventional battlefield. However, it aimed at reducing and virtually negating the asymmetry through adoption of a nuclear weapons program; this it achieved through the Eighties but used various ruses of alternating denial and acceptance, until transparency finally emerged in 1998 when it went overtly nuclear. The central aspect of its policy was and has been to place itself firmly as a core Islamic power and draw the international economic and emotive support from that linkage. To do that it needed to pursue the internal promotion of Islamization. It was supposed to be a calibrated approach to draw maximum strategic advantage that went completely awry. Alongside this it has followed a policy of exploiting India's various fault lines, the prime being the communal one. The belief remains that India's minorities must not be allowed to be mainstreamed and their Islamic fervor enhanced such that they perceive isolation and persecution within. The J&K proxy conflict controlled from Islamabad provides the dual adrenaline of attempting to wrest that state and exacerbating divisiveness within India.

Significant Aspects of Pakistan's Geo-strategic Importance

Pakistan's occupies a geographical location which gives it an automatic strategic importance. Five different civilizations surround it, each with a mutual set of interests resting within its territory or its people. With Iran in virtual international pariah status it is Pakistan which provides access to Heart of Asia and outlet from the latter to the oceans. No sustained and major operations can be fought in Afghanistan without access from Karachi port to the Afghan heartland; the feasibility of such operations through an airhead in the Central Asian Republics (CARs) is militarily impossible. The long and troubled border between Pakistan and Afghanistan is in itself a battleground of no mean proportion and Pakistan considers Afghanistan its natural 'strategic depth', a term which has been differently interpreted by different analysts. The aspect of accessibility to the oceans plays out most significantly in the context of China's One Belt One Road (OBOR). The China Pakistan Economic Corridor (CPEC) is the flagship project of OBOR, with an investment of 62 bn USD, which Pakistan wishes to make the major binder for an even more profound strategic relationship with China.

Pakistan's current cockiness in foreign policy may appear a brave front to minimize US coercion to pry maximum cooperation in Afghanistan. It is playing out its strong equation with China and the obvious advantages of its geostrategic location to set up its own significance and attempt to gain maximum from the international community, including possible concessions on J&K and its relationship with India.

Among major vulnerabilities is its lower riparian status in the regional drainage of waters from the catchment areas in the north; with the upper riparian being India the status of the Indus Waters Treaty assumes greater significance especially if India is continuously needled in other domains which impinge on its security.

Pakistan's Strategic Security Priorities

Perceiving an existential threat both on the borders and within, Pakistan's current priorities for its strategic security are as follows (not in any order):-

- Besides its Islamic linkages the partnership with China forms the bedrock of its foreign policy. From it Pakistan draws tremendous support and a degree of freedom from coercion from larger and stronger countries such as the US and India. However, security policy framers in India need to be aware that the economic relationship between China and Pakistan is not based on aid but on loans which are reasonably expensive. The effect of repayment of loans is yet to be fully comprehended or analyzed with difference of opinion more rampant than any single view.

- It is seeking fresh partnerships with countries such as Russia on basis of mutuality of interests in a world now examining different equations. However, a set of military cooperation exercises and sale of a few helicopters does not spell a new strategic equation.

- It seeks to secure a major part of the strategic space vacated by the US and the INSAF in Afghanistan, through proxies such as Taliban and the Haqqanis and deny that space more specifically to Indian influence.

- In the pursuance of the stabilization of the internal security scenario within Pakistan its security forces have suffered a major toll. In recent times it has executed two major operations – Zarb e Azb, to establish internal domination in the restive areas along the western front where the 'bad terrorists' (as against the friendly ones focused against India) have had a long run, and Radd - ul – Fassad, an operation to clean out areas in its hinterland by neutralizing the 'bad terrorists' and sectarian elements.

- It follows the continuation of proxy conflict in J&K using 'friendlies' and by default in other parts of India where it seeks to cause instability through disturbance of social cohesion. This gains major priority each time a trigger is either available by circumstances or successfully set up by the 'friendlies' primarily represented by the United Jihad Council (UJC). The possibility of such triggers in the near future becomes more relevant considering the wide open political space in Pakistan in its run up to the elections which are due in Jul 2018. With mainstream political parties largely

weakened there are elements such as Hafiz Sayeed's Jamat ul Dawa (JuD) (with a brand new political party – Milli Muslim League, to boot) and other friendly terrorist groups who could attempt to morph into political entities to garner credibility. Most of these groups follow a radical Islamist line and the political color they adopt is perceived to receive a fillip by a more strident anti India stance. The latter could result in attempts to execute high profile violent actions on Indian soil.

- Lastly, the pursuance of nuclear weapons is a very significant strength Pakistan possesses. Sanctions on the proliferation of its program were laid to rest as soon as it regained 'frontline status' for the US in its fight against radical jihadi elements in Afghanistan. The potential of the nuclear weapons falling into Jihadi hands as a result of a possible implosion of Pakistan remains an abiding concern among big powers. It offers scope for continuous impingement of this notion on the international community through effective Indian communication strategy.

- Pakistan now boasts of having developed tactical nuclear weapons (TNWs) as it claims, to counter India's offensive thrusts which could be a part of the latter's pro-active strategy on the western front. It does not yet have an answer to the feasibility of the employment of such TNWs crossing the rubicon of India's declared No First Use policy in the employment of nuclear weapons as weapons of war fighting.

One of the subsets of Pakistan's strategic security strategy which it has developed and refined is communication strategy, the art of effective propaganda and perception management. It appears to have partially borrowed this from China's doctrine of 'war under informationized conditions'. It is learnt that Pakistan is avidly studying India's successful handling of the Doklam standoff with China. What can be expected in future is greater collusion between Pakistan and China in the approach to India and the disputes that exist with it.

Lastly, J&K still rules the roost as far as immediacy is concerned. Pakistan has been surprised by the speed with which Indian security

forces (SF) have regained dominance in the Valley. However, as long as alienation among the populace in the Valley runs high the scope to overturn the situation in favor of Pakistan sponsored anti-national elements always remains. In a situation where Pakistan's control over turbulence in the Valley is only marginal it is violent exchanges at the Line of Control (LoC) which becomes the symbol for projection of the J&K issue to the international community; keeping it in the focus, so to say.

India's Counter Strategy

Considering the takeaways from the strategic security priorities of Pakistan India can ill afford not to have an updated view of the threats that are likely to be at play in 2018 and beyond. A counter strategy would already be under evolution as work in progress under the National Security Adviser (NSA). The possible areas on which such a strategy may focus are analyzed in succeeding paragraphs.

There are some assumptions and truisms we need to keep in mind while considering such a counter strategy:-

- War is not an option to resolve issues but coercion of different kinds and different levels backed by credible deterrence remains one of the key elements in diluting threats.
- The world is undergoing change in terms of strategic relationships. Past foes can be friends and vice versa with no dogma of history of antipathy attached to future dispensations.
- Partnerships between nations or membership of groups today are important and contribute to greater security as complexities and inter linkages within strategic situations have enhanced.
- Communication strategy and narrative dominance are equally important tools in dealing with adversaries and grappling for advantage. Nations which lack this capability suffer from the perception they cannot evolve in favor of their own cause, in terms of justification of stands taken.
- Diplomacy is usually of the structured kind, conducted upfront by

a nation's official diplomatic corps. However, narrative dominance is more likely to be achieved by under radar diplomacy conducted through employment of a corps of competent former diplomats, scholar warriors, bureaucrats and intelligence officers. Pakistan has itself mastered this art.

Indian Strategic Approach. With the above truisms and assumptions in mind we may outline a broad strategy to tackle security issues thrown up by India's overall standoff with Pakistan:-

- India should no longer look upon Pakistan in isolation. That is the difference 2017 made. While threats from China and Pakistan have often in the past been viewed in tandem the tendency has more often been to view each in isolation. China and Pakistan are likely to assess avenues of cooperation which can place India at disadvantage. For example in the field of cyber capability China's greater assistance to Pakistan will bring to bear a modern element of warfare along an enhanced front. India must therefore seek ways of countering this through counter cyber warfare techniques and systems.

- India must continue to seek strategic partnerships with important countries on the basis of context of threats it faces. In the specific case of the collusive Sino-Pak threat the emerging Indo-US strategic partnership is the most significant. There may be occasions when India may have to re-examine its current interests and not be guided by the past. The apparent dilution of the Indo-Russian relationship must be kept in focus and ways to retract and recover it need to be considered. In the post 'post-cold war' world to expect that an Indo-Russian relationship will be based on the threat perceptions of the pre-cold war period is unrealistic. However, there is enough convergence of interest, probably well identified. The emergence of a Russian-Pak relationship must be viewed from an angle of new equations with no major compromise on the Indo-Russian relationship.

- There appears to be a negative narrative created around India's current military capability. Besides low budgetary allocations, and

procedural inefficiency in procurement of weapons and equipment a very awkward civil-military relationship has eroded India's deterrent capability vis-à-vis Pakistan. The solution lies within and how it needs to be done is the subject of another analysis.

- The world is increasingly looking at the hybrid form of conflict which encompasses below threshold covert operations, economic warfare, resource threats such as those based on water, terror, separatism, sabotage and subversion. The range of hybrid threads can be many times more manifold and do not remain the purview of one nation. 'Two can play the game' – still remains a truism as everything thing can be paid back in kind and that includes 28 years of tolerance for Pakistan's one sided hybrid aggression. There is every possibility that Kulbhushan Jadhav was kidnapped from Chahbahar to brand and project Indian espionage and subversive activities in Baluchistan. It was also contrived to send a message to India's intelligence leadership that Pakistan had a measure of control over the intelligence space. This must not dissuade India from setting up its own proxies in Pakistan, especially Baluchistan and cultivate its capability beyond the usual niceties between neighbors.

- The J&K issue makes India vulnerable, takes away out of proportion focus of officials and the strategic community and needs out of the box handling to strengthen India's stand. Military domination is important but equally important is the strategy evolved and executed to dilute alienation, take the population on board and involve it in nation building. While it may be easier said than done the efforts towards that end need to be seen as sincere and holistic. For this India needs to develop its overall communication strategy capability to counter Pakistan's nefarious agencies and have its own versions of storytelling.

- Storytelling is an essential part of communication strategy. There is much to learn from Pakistan in this regard and better it through willingness to adopt change. Our capability of outreach to important international institutions, think tanks and simply the

right circles which matter, through unofficial diplomacy supported and briefed by the Government, is a must. The Indian narrative on all contentious issues must be heard and be absorbed.

- Embassies and high commissions abroad have their hands full and are under staffed. India's diplomatic corps is insufficiently large to undertake a full scale official diplomatic offensive. Hence the need for supplementing it with academics, army officers and others who show proficiency in understanding strategic affairs. On matters of core concern for India, such as J&K or Doklam (at the height of the crisis), the ability of our missions abroad to sell the Indian narrative needs to be progressively enhanced.

- The oldest phrase and probably the most appropriate in all matters concerning Pakistan is –'setting our own house in order'. If internal harmony between communities is in place no power can weaken India but the moment political interests override national interests we open ourselves up for exploitation.

- Economic strength will override all other capabilities in the future. Pakistan is expecting to reach a figure of 7 percent GDP growth in the next three to four years on the back of the perceived CPEC benefits. Although economists are all skeptical about such expectations India's GDP growth must outmatch Pakistan to allow the truth to sink in. Managers of India's economy need to be mindful that apart from social parameters which are affected by economic growth so is projection of capability and power.

- There is a certain position of respect acquired by India over years on the basis of its democratic and secular credentials and indices of human freedom and free media. This is soft power that India carries over and above its military and economic capability. It lends out of proportion credibility and enhances comprehensive national power which too is a deterrent for rogue nations undertaking adventurism against India.

- Pakistan is unlikely to be coerced by US in the usual ways adopted thus far. If it has to be pulled back from the activities it is indulging

in India and the US need to be in much more consultation. The US will have to be prepared to go the full mile and refrain from stopping mid-way and resorting to sops. In the short term it is unlikely to happen as historical US and particularly the US Military's support to Pakistan will not wane overnight.

- India's risk propensity for undertaking one off punitive operations against Pakistan and its surrogates has to increase. There can be no perfect situations and solutions; much imperfection and a degree of crudity have to be accepted. It is only then retribution capability will increase. This should be left to the Army to handle with no encumbrances just as has been demonstrated at the LoC through 2017.

- The experiment with countering terror, separatist and other financial networks has been a runaway success. Much more time and energy needs to be invested in this field as it has immediate effect. With reasonable success in the J&K theatre we now need to expand our counter finance operations to other states where the jihadi scope runs high.

- In terms of the nuclear field India's relative silence and maturity has somehow given Pakistan an erroneous perception of its (Pakistan's) decided superiority in this field. Subtle correction of perception may be necessary to allow deterrence to take more effective shape.

The recent NSA parleys at Bangkok have been met with confused signals even from well informed circles. The truth remains that even at the height of standoff in relationships a window remains open. It may not be a process in place but one off meets to take stock and examine feasibility of changing course. Given the political events in the offing in both India and Pakistan in 2018-19 major initiatives for peace may not be forthcoming even in the absence of any major tensions. However, in the context of the times things can change overnight if bold initiatives are taken by political leaders. Inevitably such initiatives will need to come from India in view of the light political leadership in Pakistan and its guidance under Army control. The spoilers will remain the 'good guys'

who deliver Pakistan's perceived interests with regard to India. Pakistan needs to get this clear that its stance on talks and more talks has to be matched by sufficient initiative to ensure future talks if at all, are not sabotaged at the hands of maverick 'good boys'.

Lastly, the feasibility of Doklam 2 looms large and in that are opportunities for Pakistan which it will not forego. India has to be more than ever mindful that lower intensity two front situations without the full spectrum being unleashed could well be on the cards; a kind of test of collusion for the future. Its strategic partnerships must ensure that India is not isolated in the event of such testing. It will need much support and that support will equally set the stage for future standoffs.

***Lt Gen Syed Ata Hasnain** is a Delhi based renowned defence analyst and a former Corps commander of the Srinagar based Coprs

CHINA- PAKISTAN STRATEGIC NEXUS - COLLABORATIVE THREAT : INDIA'S TWO FRONT DILEMMA

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

In 1965, a Pakistani military delegation traipsed to Beijing in hope of replacing equipment they'd lost in the war with India. Premier Zhou Enlai, meeting the delegation, was bewildered by their request for only 14 days' ammunition. 'How can a war be fought in that short time?' Zhou asked: 'I would be interested to know if you have prepared the people of Pakistan to operate in the rear of the enemy...I am talking about a People's Militia being based in every village and town'. The Western trained and educated Pakistani generals were taken aback. 'What does Zhou Enlai know about soldiering anyway?' This story appears in Andrew Small's book The China- Pakistan Axis: Asia's New Geopolitics. It is a reminder that the two countries are odd bedfellows, lacking the cultural affinity that might be implied by General Xiong Guangkai's quip that 'Pakistan is China's Israel'. China - Pakistan may be odd bedfellows but the geostrategic concerns have historically remained largely congruent and converge around many common areas and bilateral interests. The relationship between the two countries mainly hinges on four shared areas of interest that include 'economic cooperation, energy security concerns , internal security, and geostrategic interests to balance India. Many among the strategic community are of the view that Pakistan is China's proxy and is being exploited to contain India's growth as a global player.

India faces full spectrum of security threats from a proxy war, sub conventional or Low Intensity Conflict (LIC), 4G war, hybrid war, small wars, conventional war, nuclear war, as also a collusive and/ or collaborative threat from Pak and China. We have a mischievous

Pakistan in the West and a strong adversary in China in the North. The India - Pakistan line of control (LC) extends 772.1 kms and the Actual Ground Position Line (AGPL) along the Siachen glacier extends another 126.2 kms. Pakistan also occupies 78114 sq kms of Indian territory in J&K . Pakistan has waged four wars on india and continues to wage a proxy war for nearly three decades. The ongoing proxy war is a state policy driven by the Pakistan Army. India shares the longest disputed borders in the world, the Sino-Indian border extends 3488 km, with China laying claim to over a 1,10,000 sq km of Indian territory. The two nations have maintained Peace and Tranquility along the Line of actual Control (LAC), with the last shot in anger fired over four decades ago. India faces "India has to be prepared for a two-front war and build deterrence that ensures conflict is not an option for its adversaries" National Security Advisor (NSA) Ajit Doval said at the Hindustan Times Leadership summit on 23 Nov 2014. "India has two neighbours, both nuclear powers (which) share a strategic relationship and a shared adversarial view of India,"

China has risen to superpower status. However, a deeper look at China's internal dynamic raises uncertainties about its rise. For India, the main consequence of China's rise is that India will have an adversarial and competitive superpower at its borders. The differential between India and China's comprehensive national power is only going to increase. Chinese presence in Pakistan Occupied Kashmir (PoK) is increasing; China has expressed its disapproval regarding the presence of Indian oil companies in the South China Sea; it routinely describes Arunachal Pradesh as South Tibet; and its position on the diversion of the Brahmaputra waters is ambiguous. It has undertaken massive modernisation of infrastructure in Tibet and has constructed a state of the art multi modal multi dimensional infrastructure to enable rapid build up and sustenance of combat power in Tibet. China says the border dispute is confined only to 2,000km mostly in Arunachal Pradesh. But India asserts the dispute covers the western side of the border spanning 3488 kms.The Chinese President's visit to India in September 2014 was overshadowed by a border crisis when PLA troops entered Indian Territory in Chumur, Ladakh. The 73 day standoff at DOKLAM is an indicator of the fragile peace at the borders. On account of differing perceptions of the LAC, an assertive and aggressive China and a growing new India, the

peace and tranquility along the LAC will be constantly and continuously under severe stress, with increase in frequency, intensity and depth of transgressions, leading to more and more 'Standoffs'. The Doklam is likely to be the new normal.

In the case of China , what cannot be denied, first is its global power ambition and implementation of its massive military modernisation programme, which raises questions on its intentions to peacefully rise. "It follows a "two-pillar "approach in its foreign policy; the first pillar is stated as securing "win-win cooperation "in international relations and the second as not making any compromise on territorial sovereignty issues. The second aspect is leading to China's assertiveness with all its neighbours which have territorial disputes are becoming increasingly concerned. They see a contradiction in the "two pillar" external approach of China; the PRC on its part denies the same. It is in any case clear that the Chinese foreign policy has become 'core interest-based' since 2008; post the 19th congress national security imperatives dominate Chinese foreign policy. As China increases its comprehensive national power, it has projected its influence into India's neighbourhood. China has provided crucial strategic nuclear and missile technologies to Pakistan. China has ignored international norms in these transfers of technology. China's intentions are clear. Pakistan provides a proxy for its policy of boxing in India and tying it down within its region.

The game changer within China could be a slowdown of economic growth leading up to internal instabilities and changes in foreign policy behaviour. With the rise of China, its influence in South Asia will grow. This is already visible, particularly in Pakistan, Maldives, Nepal, Sri Lanka and Myanmar. India will come under pressure to restructure its neighbourhood policy to ensure that India does not get drawn to an unsavoury competition with China. The trajectory of Sino-Indian relations will have a decisive influence in the emerging strategic construct in South Asia. The continuing China-Pakistan nexus and China's strengthening its strategic presence in India's neighbourhood, will always act as pressure points of Beijing against New Delhi. The asymmetry between India and China in terms of national strengths is real and may persist for a long time; this factor will always influence China's policy towards India.

Pakistan has emerged as most volatile state in our neighbourhood with grave disputes that have remained unresolved with India. Though it may not portray a grave military threat but will continue to be the most irritating adversary. It is unlikely to come to any settlement on existing disputes and our security forces are likely to be embroiled in Proxy war waged by Pakistan. A section of the Army has got radicalised reflecting the broad trend in the society. Parts of Pakistan might become ungovernable. The escalating violence and the inability of the government to control it is a symptom of the deeper malaise in Pakistan. The military will continue to play an important role in Pakistan's governance and will drive Pakistan's India Policy.

Future protends number of uncertainties in a geopolitical and regional scenario.In the backdrop of India's security concerns it is essential to factor certain key uncertainties which can lead to a conflict situation. These are:-

- Impact of politico-eco-military shift to Indo - Pacific.
- Changing nature of conflict - WAR 2.0.
- India's ability to manage flashpoints.
- Competition for resources with China.
- More nuclear powers - terrorist groups acquire NBC weapons.
- Way ahead of India - China strategic partnership.
- What after Dalai Lama???
- Nuclear threshold of Pakistan.
- Impact of increasing domination of IOR by China.

India has adversarial relations with both China and Pakistan. It will be of interest to understand the drivers for conflict with the adversaries to mitigate the chances of conflict. With Pakistan the likely drivers for conflict are:-

- India's response to a major terrorist strike orchestrated by Pakistan based terror organisations, and the counter thereof, surgical and/or precision strikes.

- Pakistan based terrorist organisation gaining covert control of nuclear weapons.
- An imploding Pakistan, makes a last ditch effort at unification by playing the anti India card.
- With the US drawdown from Afghanistan, India should be prepared for a shift in Pakistani controlled terrorist organizations from Afghanistan to J&K, thus upping the ante. A more vigorous proxy war by Pakistan in Kashmir will be unacceptable to India.

Likely drivers for conflict with China are:-

- A flare up along the Line of Actual (LAC) (DOKLAM STAND OFF), with the potential to spiral into a skirmish or a conflict.
- A perceived threat by China to China-Pakistan Economic Corridor (CPEC)/ Karakoram Highway (KKH) would lead to a collaborative threat from China and Pakistan. The plausibility of this collaborative threat to the disputed Siachen glacier and Aksai Chin is much more as it provides strategic depth to the CPEC. Pakistan has been the major benefactor from this corridor as it achieves strategic domination of Afghanistan, balances India and gives a much needed boost to a failing Pakistan economy.
- China's one belt, one road has major political, economic, strategic and security implications for India. As it further strengthens Beijing's 'string of pearls' strategy
- China's exploitation of non-contact warfare capability in the cyberspace, information, psychological, space and electronic warfare domain.
- China's covert and overt support to Indian insurgent groups in the NE, though not a driver for conflict but could manifest into a collusive support to Pakistan.

Collusive and Collaborative Threat

The history of the military collusion between China and Pakistan goes back over fifty years. During the 1965 and 1971 India-Pakistan wars, China had made some threatening military manoeuvres in Tibet in support of Pakistan. It is also noteworthy that during the Kargil conflict in 1999, Chinese military advisors were reported to have been present at Skardu in POK. In fact, given its internal instability, fissiparous tendencies and doddering economy, it would not be possible for Pakistan to wage a proxy war against India in Jammu and Kashmir and other parts of the country, but for China's military backing and support. In as much as that, it is also China's proxy war with Pakistan acting as China's proxy. While a semblance of stability prevails at the strategic level, in recent years China has exhibited marked political, diplomatic and military aggressiveness. However, China has not directly intervened or aided Pakistan during the four conflicts.

Gen V P Malik former COAS of the Indian Army while delivering the thirtieth USI National Security Lecture on the Grand Design between China and Pakistan stated "The possibility of a concerted twin strike in a grand design by China and Pakistan has very serious implications for India: nuclear, aerospace and maritime dimensions. It may also involve Bhutan, Nepal and Bangladesh. As India would be the main sufferer, it could legitimately hurt maritime interests of China and Pakistan in the Indian Ocean and even rescind its No First Use (NFU) of the nuclear doctrine to send warning signals to both countries." In all these manifestations, China-Pakistan military collusion in the Karakoram Pass region can be considered as the most likely scenario. A collaborative threat by Pakistan and China though may seem far fetched to some, but is plausible especially so if there is a perceived Indian threat to the China - Pakistan Economic Corridor (CPEC), as it passes through disputed territories close to the borders.

China's One Belt One Road (OBOR) has changed the strategic equation. The China - Pakistan Economic Corridor (CPEC) which passes through PoK is pivotal to OBOR and the China Dream. The CPEC project implies that the Chinese presence and strategic interests in Pakistan

and specially in PoK will become quasi permanent. The CPEC has direct strategic and security implications for India. Though China's stated position is that 'Kashmir' is a bilateral issue between India and Pakistan, however, now with the CPEC, Chinese economic and strategic interests make it a direct stakeholder in a hither-to-fore bilateral issue. While the Sino-Pakistan axis is not new, the sheer magnitude of the CPEC makes it clear that it is not only dictated by economic considerations but more to exploit strategic payoffs. CPEC enhances the collaborative and collusive threat China and Pakistan pose to India. Another major concern for India will be the deployment of PLA troops in POK to safeguard Chinese interests and assets. Any perceived threat to these interests may elicit a military response and has the potential to spiral into a conflict duly aided or manipulated and orchestrated by Pakistan. Hence the CPEC has changed the strategic equation prevalent in the region.

Another critical issue which needs to be factored is that there have been 16 transitions of world power in the last 500 years of which only 4 have been non violent. As China grows in military, political and economic power it will challenge the United States for the sole superpower status. The first indicators were evident during President Xi's visit to the United States, wherein he asked the United States to treat China as a strategic equal. President Xi in his speech on 22 September 2015 contradicted experts who have talked about 'Thucydides Trap" where an emerging power like China threatens an established power like the US. To quote president Xi " There is no such thing as the 'Thucydides Trap" in this world, but should major countries time and again make the mistake of strategic miscalculation, then they might create such a trap for themselves" he warned. Coming immediately after the 3rd September military parade where China demonstrated its military might with 500 pieces of different weapon systems of which 84% were publically displayed for the first time is a paradigm shift from "Holding one's capabilities and biding one's time" As and when the transition of power takes place, it will directly impact India's security, India being a ' Balancing Power".

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

without any direct attribution and without any overt physical military application of combat power ab-initio. A collusive or collaborative threat from both China and Pakistan is a probability which India should consider seriously. However, China mindful of its national and economic interests is not likely to overtly either support or collaborate with Pakistan. In the event of a China threat, Pakistan will only be too willing to support it's all weather friend China and a collaborative threat from Pakistan would be imminent, as it takes on a mightier India preoccupied with China along the Northern Borders. Hence, it would be prudent to conclude that during a future Indian military conflict with China, Pakistan will come to China's military aid but reverse may be likely but not a serious threat.

China will definitely continue to support Pakistan in the diplomatic domain. In addition in the event of a military confrontation, CPEC infrastructure will facilitate an uninterrupted and timely flow of military aid to Pakistan, thus enhancing the war endurance. Future wars are not likely to be large scale, conventional wars in the backdrop of a nuclear umbrella, neither a nuclear war leading to mass destruction nor a totally non-contact war in the cyberspace, and informational domain. Future conflicts will be a continuous, long drawn war conducted in many battle spaces by multiple means driven by collective ideas, waged by proxies and non state actors with or without any covert physical military application of combat power. India should be prepared for China to support Pakistan in all dimensions except possibly direct conflict. China may not support Pakistan by employing their growing hard power, but do so in multiple domains particular by exploiting a "grey zone" where aggression and coercion work just below the level that would risk military confrontation with India. Essential support will be in the asymmetric-warfare strategies, C4ISR, cyber, space and outer space, electromagnetic-spectrum warfare, information wars and military coercion.

Options for India

A two front war is not an option for India and hence it is an imperative that India has a credible war prevention strategy with China and a war waging strategy waging/ proactive strategy against Pakistan, mitigating a collaborative threat or a two front war. The nation has to prepare for a war in all its dimensions and intensity from small wars to space wars,

hybrid in content and possibly collusive and collaborative in context. India's security concerns must match with the apparent dichotomy in the Chinese policy pronouncements. It should also be based on its own core-interests. We should note that the Chinese declared military strategy does not rule out 'Local Wars Under Information Conditions' and such local wars, as many analysts believe, can happen in China's periphery. India should not fail to see that in South China Sea and East China Sea, China is resorting to a show of force to assert its territorial claims. India should anticipate China's indulging in similar show of force to assert its border claims against it, at an opportune time, Doklam is an indicator. China's intention seems to be towards resolving the 'Boundary Question' with India, on the premise that a status quo would be in India's favour. The early resolution of the 'Boundary Question' as enunciated by President Xi is a shift from the earlier Chinese position. India will have to resist pressure from China on settling the 'Boundary Question' on unfavourable terms. On the whole, India will be compelled to increase its own economic and military strengths while improving governance in the areas bordering with China. Both the countries have taken precautions to declare that they are in favour of developing a cooperative relationship. However, China's recent assertiveness in border areas like Doklam are indicative of the heretofore peace and tranquility being under severe stress.

India's China policy should be pragmatic; it should continue to 'engage' China while at the same time ensuring that its national interests are not compromised. Why can't India develop its own pressure points against China? Revisiting Taiwan and Tibet policies, strengthening strategic ties with China-wary nations in East Asia like Japan, Vietnam and the Philippines as well as with ASEAN nations, can be India's options. A risen and responsible India will do well to 'Bind to Balance" with the extended neighborhood. The QUAD is an excellent initiative which needs to be consolidated. The fact that the heads of states of ten ASEAN nations attended the Republic day 2018 as the Chief guests is also an indicator of a new India which can forge meaningful strategic partnerships as an alternative to a growing China.

There has been a shift from "Balance of Power" to "Balance of Interest", hence it is a strategic imperative to ensure equilibrium,

peace and tranquility along the Northern borders with China and further economic interdependencies. The strategic partnership with China should be strengthened and taken to the next level. Early resolution of the 'Boundary Question' is a must, as this is possibly the only driver for conflict between the two Asian giants.

There is a section among the strategic community who theorize that as the armed forces have not fought a war since 1971 and given our nuclear deterrence, the armed forces need to be pruned. The modernisation of the armed forces too has not kept pace with the security needs and the intent of the government. Though the DPP has been revised the procedure and process remain the same hampering an effective and planned modernisation. The defence budget too is at best incremental catering for inflation as announced on 01 Feb 2018. At 1.56 % of the GDP it is the lowest since 1962, indicating the focus and concern of the government towards national security despite the adversarial relations both with Pakistan and China being a matter of grave concern in the immediate term. The Shekatkar Committee was set up by the then RM Mr Parrikar to " Enhance the combat effectiveness by rebalancing the Defence budget". The MoD has implemented only 65 odd of the two hundred odd recommendations. These recommendations are at best the proverbial low hanging fruit as the macro issues have not been implemented. The report was submitted in December 2016. It is an imperative that the MoD initiate the right changes and implement the recommendations of the Shekatkar committee in totality thus rebalancing the defence expenditure ensuring addition funds for the much needed modernisation of the armed forces.

China respects STRENGTH, and hence it is an imperative that India and the armed forces build the requisite capabilities and enhance capacities.

***Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd),** a Former DGMO is presently Director CENJOWS

ICT, AUTONOMOUS WEAPONS AND FORTUNA

Air Marshal PP Khandekar, AVSM (Retd)*

"We have an illusion of security, we don't have security". – Isaac Yeffet

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards".
– Gene Spafford

"We are facing very immediate choice- constraints on autonomous weapons or an arms race". – Stuart Russel

The Background

The above three statements give us just a glimpse of what is in store as the 21st century is unfolding before us. The challenges emanate from the definition of each word in the title of the article. Due to the complex interaction between them, the challenges are equally complicated. The reader is requested to draw up the list of the challenges as he goes on reading the referenced articles as well as the reservoir of literature available in the open source. Technological progress is a driving force behind economic growth, citizen engagement, and job creation. Information and Communication Technologies (ICT), the fourth industrial revolution are reshaping many aspects of the world's economies, governments, and societies. Many American and other defence giants such as Boeing and Lockheed Martin have started pushing hard for a specific framework in India to ensure the safety and security of critical technology and classified defence information when they are shared with the private sector for joint ventures in India. Benjamin Schwartz, senior director for Washington-based USIBC (US-India Business Council) said, "They (India) need to establish procedures to ensure the security of defence technology here. What I

mean by it is that the reality in India and also in the US and around the world is that information is being stolen. We have to set up procedures to make sure that our defence technology is secure (in India)".

Security is a concept and is all pervasive for every nation. The security challenges emerge from the adequate resources such as land, minerals, oil, water, food, people and other aspects such as economy to include business and corporate not to forget disruptive technologies and innovation, asymmetry and inequality, power and dominance in a region, political alignments, growth or lack of it, safety of assets, play of non-state actors, mistaking "trees for woods" or "leaves for trees", lack of transparency in response of the adversary, darknet and so on. The wars also accordingly have changed in definition, domain, size, shape, intensity and effect. In the realm of ICT security, we may not use the word "battle" but use "incident" or "attack", the concepts remaining same. The field of ICT has opened new vistas of power structure and has posed new set of challenges. The rules of the game are yet to be involved for the "invisible enemy". Perpetrator motivations (read threats) are one or more of gain notoriety, undermine confidence, revenge, financial gain, influence opinion, gain competitive advantage, conduct espionage, steal intellectual property, effect a change of government, destabilise a country, elevate status within own clique, shutdown enemy offensive/ defensive systems and so on.

Security

When we talk of security and challenges, there is a need to first understand security and its connotations in the changing times first. Under its overarching definition lie ICT security and autonomous weapons aspects. Security simply put is the state of being free from danger or threat, which changes from time to time based on many factors such as technologies, individual and group values, faiths and beliefs, sense of injustice and inequality and so on.

Tom Madsen, Security Advisor, Fort Consult has applied statements of Sun Tsu the great author of "The Art of War" to cyber security and are being also interpreted by the learned to apply them in the context of technological advances. While reflecting on Sun Tzu's

statements, Ray Bernard realized that he had written a very basic security status scale.

Know The Enemy	Know Yourself	Security Status	Result
No	No	No threat or vulnerability assessment	You will succumb in every battle
No	Yes	Vulnerability assessment but no threat assessment	For every victory gained you will also suffer a defeat
Yes	Yes	Both threat and vulnerability assessments are current	You need not fear the result of a hundred battles

Sun Tzu Security Status Scale

Speaking on the relevance of Kautilyan thought on national security, at IDSA, Professor Balbir Singh Sihag, said that Kautilyan understanding of economics and prosperity was based on much more solid foundation of ethics than Adam Smith's idea of justice being the foundation. To Kautilya, there was no room for idealism in pursuing national interests. He understood that national security was not any abstract concept and a nation needed to compare its strength to that of its potential adversary.

Machiavelli, the modern day Chanakya came up with the idea of virtu and fortuna while discussing Power of the State. Virtù can be summarized by his recommendation that the Prince above all else, must acquire a "flexible" disposition. What is the conceptual link between virtù and the effective exercise of power for Machiavelli? The answer lies with another central Machiavellian concept, Fortuna which is the enemy of political order (similar to a violent river), the ultimate threat to the safety and security of the state. Machiavelli realizes that only

preparation to pose an extreme response to the vicissitudes of Fortuna will ensure victory against her. This is what virtù provides: the ability to respond to fortune at any time and in any way that is necessary. ICT and autonomous weapons are in this way, violent rivers that will lash out unless well prepared to face them well in time.

Sofie Skouras has nicely brought out what happened in today's world to the story of Adam and Eve. Instead of the Garden of Eden, Eve is based in a local business park in Kent and works for a tech company. She gets an email one day that looks like it's from her boss, reading: "Action this immediately" with a link below. Of course, like any diligent employee she does so. Eve then turns to her colleague Adam asking if he got the email and letting him know she's looking into it, he then, also clicks the link. Turns out, the email was actually a serpent and now a cyber criminal has access to their company's systems. The reality is there will always be people – like Adam and Eve – who fall victim to the traps of cyber criminals. And as technology becomes more sophisticated, the challenge only increases. Cyber criminals are using Artificial Intelligence (AI) technologies and Machine Learning (ML) to remove the element of human error and identify vulnerable targets and make attacks more effective. According to Tarun Kaura of Symantec, Internet of Things (IOT) enabled devices, like smart TV and smart watches are likely to be more prone to ransomware attacks. With automated algorithms, the speed of the attack is much faster and does not give an organisation enough time to register the threat. File-less malware generally do not leave any trace of its infection and is usually hidden in the computer's memory.

INFORMATION AND COMMUNICATION TECHNOLOGIES

"Information and Communications technology unlocks the value of time, allowing and enabling multi-tasking, multi-channels, multi-this and multi-that". – Li Ka-Shing

Tanenbaum in his famous book on Computer Networks has defined seven layers in the Open Systems Interconnection (OSI) model. These are Physical, Data Link, Network, Transport, Session, Presentation and Application. Thus, security of information is ensured in these

layers and so the breach of security can be also done in the same. Security can be classified in different ways such as Physical security, Information security, Application Security, Cloud Security, End Point Security, Internet Security, Mobile and Network Security, etc. In today's identification and data collection methods on traffic entities, many traffic and logistic systems use one of the Automatic Identification and Data Capture (AIDC) technologies. The mentioned group contains information and communication technologies such as Radio-Frequency Identification (RFID), Real-Time Location Systems (RTLS), Near Field Communication (NFC), Global Positioning System (GPS), and beacon and advanced tagging technologies such as barcode and Quick Response code (QR code) which can be implemented with function of mobile traffic entities identification in traffic environment.

The phrase "Information and Communication Technologies" has been used by academic researchers since the 1980s, and the abbreviation ICT became popular after it was used in a report to the UK government by Dennis Stevenson in 1997. It is an another/ extensional term for Information Technology (IT) which stresses the role of unified communications and the integration of telecommunications computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information. The term is also used to refer to the convergence of audio-visual and telephone networks with computer networks through a single cabling or link system. However, ICT has no universal definition, as the concepts, methods and applications involved in ICT are constantly evolving on an almost daily basis.

The broadness of ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form, e.g. personal computers, digital television, email, robots. For clarity, Zuppo provided an ICT hierarchy where all levels of the hierarchy contain some degree of commonality in that they are related to technologies that facilitate the transfer of information and various types of electronically mediated communications. This commonality itself may be a security threat. Skills framework for the information age is one of many models for describing and managing competencies for

ICT professionals for the 21st century.

ICT and Security

"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image".

– Stephen Hawking

Security, in Information Technology (IT), is the defence of digital information and IT assets against internal and external, malicious and accidental threats. This defence includes detection, prevention and response to threats through the use of security policies, software tools and IT services. Security is critical for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat. Security in IT is a broad concept that blankets many different ideas and principles. Some of the most important security concepts and principles are defence in depth, least privilege, vulnerability management, risk management, application lifecycle management etc.

According to Steve Hudson, ICT security refers the enterprises all incidents like controls, procedures and growth level in an organization in order to ensure integrity, confidentiality and availability of their data and overall information and technology systems. Cyber security is to cater for common attacks like malware, data theft, unauthorized access and theft on your devices like laptop or mobile etc. It should come under both physical and technology theft. For both the security, some organisations are using endpoint protection software to avoid data theft or damage or physical theft. There are security standards such as PCI DSS 3.0 or HIPAA that are in place.

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."

– Kevin Mitnick

AUTONOMOUS WEAPONS

Autonomous weapons described as the third revolution in warfare, after gunpowder and nuclear arms, have opened up a whole new set of challenges on warfront as well as on social and ethical front. Autonomous weapons select and engage targets sans human intervention. They might include, for example, armed quadcopters that can search for and eliminate people meeting certain pre-defined criteria, but do not include cruise missiles or remotely piloted drones for which humans make all targeting decisions.

Lethal Autonomous Weapon Systems (LAWS), Lethal Autonomous Robots (LAR), robotic weapons, or killer robots and Lethal Autonomous Weapons (LAW) are military robots designed to select and attack tactical and strategic military targets (people, installations) without intervention by a human operator as brought out earlier. These are different from UCAVs or "combat drones", which are currently remote-controlled by human pilots and are considered a subset of combat drones. Even though combat drones can fly autonomously, they do not fire autonomously, but rather by a trained human operator. LAWs may operate in the air, on land, on water, under water, or in space. The autonomy of current systems as of 2016 is restricted in the sense that a human gives the final command to attack - though there are exceptions with certain "defensive" systems. A word about offensive and defensive systems is in order.

The oldest Automatic Defensive System perhaps is automatically-triggered lethal weapon- the land mine- used since at least the 1600s, and naval mines, used since at least the 1700s. Anti-personnel mines are banned in many countries by the 1997 Ottawa Treaty, not including the United States, Russia, and much of Asia and the Middle East. Some current examples of LAWs are automated "hard kill" active protection systems, such as a radar-guided gun to defend ships that have been in use since the 1970s (e.g. the US Phalanx CIWS). Such systems can autonomously identify and attack oncoming missiles, rockets, artillery fire, aircraft and surface vessels according to criteria set by the human operator. Similar systems exist for tanks, such as the Russian Arena, the

Israeli Trophy, and the German AMAP-ADS. Several types of stationary sentry guns, which can fire at humans and vehicles, are used in South Korea and Israel. Many missile defence systems, such as Iron Dome, also have autonomous targeting capabilities. The main reason for not having a "human in the loop" in these systems is the need for rapid response. They have generally been used to protect personnel and installations against incoming projectiles.

Autonomous Offensive Systems need a higher degree of autonomy would include drones or unmanned combat aerial vehicles. The unarmed BAE Systems Taranis jet-propelled combat drone prototype may lead to a Future Offensive Air System that can autonomously search, identify and locate enemies but can only engage with a target when authorized by mission command. It can also defend itself against enemy aircraft. The Northrop Grumman X-47B drone can take off and land on aircraft carriers (demonstrated in 2014); it is set to be developed into an Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) system. Russian Federation is actively developing artificially intelligent drones, unmanned vehicles, military robots and medic robots. Israel announced that it is developing many types of military robots including some as small as flies in order to assassinate leaders of Hezbollah and Hamas.

Fully Automated Weapons (FAW) lower the threshold of going to war as soldiers are removed from the battlefield and the public is distanced from experiencing war, giving politicians and other decision-makers more space in deciding when and how to go to war. Once deployed, FAWs will make democratic control of war more difficult - something that author of Kill Decision - a novel on the topic - and IT specialist Daniel Suarez felt that it might recentralize power into very few hands by requiring very few people to go to war.

AI technologies have made deployment of such systems feasible within years, not decades, and the stakes are high. When artificial intelligence and robotics come together, there are two different outcomes that can occur. On the one hand, we see major improvements being brought to our society, making life better for everyone. On the other

hand, the military uses these tools to create new weapons of mass destruction.

Ethical and Legal Issues

The possibility of LAWs has generated significant debate, especially about the risk of "killer robots" or the "Slaughterbots" roaming the earth - in the near or far future. The group Campaign to Stop Killer Robots formed in 2013 and in July 2015, over 1,000 experts in Artificial Intelligence and Robotics signed a letter warning of the threat of an arms race in military artificial intelligence and calling for a ban on autonomous weapons. The letter was presented in Buenos Aires at the 24th International Joint Conference on Artificial Intelligence (IJCAI-15) and was co-signed by Stephen Hawking, Elon Musk, Steve Wozniak, Noam Chomsky, Skype co-founder Jaan Tallinn and Google DeepMind co-founder Demis Hassabis, among others. In October 2016 President Barack Obama stated that early in his career he was wary of a future in which a US president making use of drone warfare could "carry on perpetual wars all over the world, and a lot of them covert, without any accountability or democratic debate". Elon Musk led 116 experts calling for outright ban of killer robots 20 Aug 2017.

Stuart Russell, professor of computer science from University of California, Berkeley stated the concern he has with LAWS is that it is unethical and inhumane. The main issue with this system is it is hard to distinguish between combatants and non-combatants. There is concern (e.g. Sharkey 2012) about whether LAWs would violate International Humanitarian Law, especially the principle of distinction, which requires the ability to discriminate combatants from non-combatants, and the principle of proportionality, which requires that damage to civilians is proportional to the military aim. This concern is often invoked as a reason to ban "killer robots" altogether - but it is doubtful that this concern can be an argument against LAWs that do not violate International Humanitarian Law. Other risks are that, just like with remote-controlled drone strikes, LAWs will make military action easier for some parties, and thus lead to more killings. LAWs are said to blur the boundaries of who is responsible for a particular killing, but Thomas Simpson and Vincent Müller argue

that they may make it easier to record who gave which command.

There are issues with US policy about autonomous weapons their use and compliance at "appropriate levels" and other standards that bring in inherent ambiguity. Semi-autonomous" hunter-killers that autonomously identify and attack targets do not even require certification. Authoritative regimes in all probability will authorise the machine to decide and act lethal autonomously.

The Pros and the Cons

Though in the article the issues have been discussed, following table summarises some:-

S.N.	Pros	Cons
1.	Reduce soldier casualties.	Easy to go to the battle with small provocation.
2.	Efficient use of AI.	AI arms race in weapons.
3.	Cost effective	Easy for anyone to adopt like AK-47s unlike N-weapons.
4.	Ideal for specific tasks such as assassination, ethnic group cleansing,	Can be misused and can create devastation and unstable govts.
5.	Battlefields safer for civil populace.	Can mistake one for another due to complexity in identification etc.
6.	More social benefits by way of IoT etc. in diversified fields.	Dual use technology, can be disruptive.

Peter Singer has very aptly stated that there are a lot of weapons that we've developed which we've pulled back from- biological weapons, chemical weapons etc. This may be the case with armed autonomous robotics, where we ultimately pull back from them.

It can be seen that the issues are complex to put it simply and many steps need to be taken. A White Paper submitted by AKS IT Services at Delhi has submitted the following recommendations related to cyber

systems and applicable to autonomous weapons control:-

- Security auditing of networks (Data centres, Telco systems, Industrial Control Systems, Local networks), applications & databases (Web applications, web services, mobile applications, database).
- User awareness training for understanding cyber systems, vulnerabilities & exploitation at various levels.
- Govt should take Cyber Security as a priority task and encourage development of cyber security products, tools and technology within our country with preferential treatment. Cyber security products like DDoS mitigation, firewall, Intrusion Detection/ Prevention Systems and Vulnerability Assessment & Penetration Testing, Cyber Forensics, Log Analysis, Fraud Detection and Auditing should be developed indigenously. Critical software products like Operating System, Browser, Mail Servers must also be developed indigenously.
- Information Sharing and Analysis Centres (ISAC) should be created of each vertical of critical information Infrastructure like for Power, Communication, Transportation, Defence, Space etc. Honey net project and lawful interception should be done for getting advance threat intelligence.
- Indigenously developed products should be tested and evaluated by STQC with mandate at reduced rate for Start-ups. This will help acceptance of products not only within our country but also globally. STQC should have the mandate to test, evaluate and certify and award the global CCTL rating (EAL 1 – EAL 7).
- Indian Start-up Companies/ OEMs must provide accurate threat intelligence to Govt. for taking timely action for mitigation of any threat to our critical information infrastructure.

Jeroen Bismans has rightly stated that protect your network as if it is a hotel and not as if it would a castle. It is virtually impossible to protect the networks as castles- impregnable due to various aspects discussed herein. Easily available cheap technology, changing perception about "Haves" and "Have nots", unhindered interaction transgressing international borders, sense of depriving and injustice are aspects that make the issue of security a serious one. Hence there will be a need to continuously evolve oneself, create new means and ways of security.

As Shashank Reddy says, there are more questions than answers as of now- a ripe opportunity for India to develop the weapons before a ban is in the offing and take lead to define standards and engagement rules. Dependency, threat and vulnerability in ICT domain make it the Fortuna of Machiavelli that needs to be controlled well in time by full might at the command of the nation and the leadership.

"At the end of the day, the goals are simple: safety and security".

– Jodi Rell

REFERENCES

1. Interview with Tarun Kaura of Symantec- ToI
2. 'Slaughterbots' and Other (Anticipated) Autonomous Weapons Problems, Nicholas Weaver, Tuesday, November 28, 2017, 9:00 AM
3. Pros and Cons of Autonomous Weapons Systems Amitai Etzioni, PhD Oren Etzioni, PhD Military Review Jun-Jul 2017.
4. INDIA'S Contemporary Security Challenges Edited by Michael Kugelman
5. Grand Strategy for India 2020 and Beyond Editors Krishnappa Venkatshamy Princy George IDSA
6. Future Cyber Security Landscape A Perspective on the Future Australian Govt.

7. India's Security Challenges: Perspectives and Prospects -Nancy Jetly, Senior Fellow, IDSA

8. Lethal Autonomous Weapons Systems: Future Challenges By Matthias Bieri and Marcel Dickow CSS Analyses in Security Policy Nov 2014

9. How Artificial Intelligence Will Impact the Human Workforce: Threats Of A Jobless Future- Abdullah Khan Jun 17

10. Cyber Physical System CSI Communications Dec 2017.

11. White Paper on Cyber Security by AKS IT Services, NOIDA.

12. Wikipedia.

13. India and the Challenge of Autonomous Weapons by R Shashank Reddy Carnegie India 2016.

***Air Marshal PP Khandekar** is a former AOM of the IAF

THE CHALLENGES OF FUNCTIONING IN A CYBER ENVIRONMENT

Lt Gen Arun Sahni, PVSM, UYSM, SM, VSM (Retd)*

Introduction

The world is witness to a very exciting and challenging era, as we are in in the thores of Digitisation, precipitated by the ICT Revolution that started at the end of the last century. It is making a major impact on all aspects of our life and at a pace of change never witnessed before. The internet has provided a communication highway, making this abstract commodity called information with its unique attributes, available at the click of a button, without constraints of time and place. This convergence of communication with computers, seamlessly integrated through the cyber space, has resulted in an unprecedented integration of individuals, organisations and processes. The numbers of connected things are increasing in geometric progression, with approximately 30 % increase, year on year. It is estimated that by 2020 nearly half the world's population will be connected and by 2025, there will be 6 machines connected to every human on this earth.

In the last decade there was another concurrent revolution. Web 2.0 provided the ideological and technologial foundations to build social media platforms, like Facebook, Instagram and Twitter, while there was proliferation in the availability of information through Wikipedia, You Tube and Google. Simultaneously, the mobile added to this chatter with growing dependency on networking through 'What's App'. The cumulative impact has led to pervasive changes in the means and intimacy of communications between organizations, communities, and individuals. The time spent on these platforms is increasing disproportionately, with nearly 15 to 20% increase,

year on year. It provides highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content.

The Spectrum

India is no exception and every day there is an increased dependence on cyber space and its applications. This is increasing rapidly in almost all spheres of'governance' and 'security'. Daily better and intricate software's and applications are addressing the ever-evolving requirements or the shortcomings that are noticed. The current Government has given tremendous impetus to digitization with its laudable initiatives of 'Smart City', 'Digital India', cashless transactions, etc. This has resulted in rapid changes in the field of communication for unfettered and unhindered accessto cyber space. The future is only going to demand greater bandwidth and reliability from this medium, to support the breakthroughs in Big Data Analytics and Cloud Computing.

It would be right to state that the rules & means of interfacing with the Government are changing dramatically, with focus on initiatives like E Kranti / E Governance. Concurrently, in the domain of services and facilities we have transcended to a period of Smart Systems. InCritical Infrastructure, the integration of Information, Operations and Consumer Technology, along with the influx of Cyber Physical Systems, has optimised their functioning. The ongoing revolutionary changes in the domain of 'Artificial Intellegence','Machine learning'and the breakthroughs in the ongoing research in the 'Internet of Things' will have a profound impact on ease of doing business and availability of basic facilities in a reliable and cost effective manner. This has enhanced the overall effectiveness of vital systems, be it the transportation systems of air travel or railways, move of gas and oil over long distances via pipelines, power generation & transmission, water management, banking and financial services, home automation remotely controlled through the smart phone and wearable devices in e- health domain. The list is unending and the area of its penetration is restricted by our capacity to visualize.It will not be wrong in stating that we are transiting from functioning in cyber space to being part of

the cyber eco system It has not only changed our life style, but has permeated into our DNA.

Simultaneous, to the exploitation of cyber space for governance, commercial and financial services, it has had a corresponding impact on the Defense Forces. And towards this the armed forces are moving towards Network Centric Operations an umbrella term for what encompasses the concepts of Network Centric Warfare (US), Network Enabled Capabilities (UK), Network Based Defense (Sweden). In the Indian context there are ongoing efforts to operationalize the 'Management and Operational Information Systems' and the Armed Forces are transiting from an era of C3ISR to C4I2SR/ C5ISR. The exploitation of this medium is setting the stage for the future military leaders to have not only enhanced science of control but be able to exercise the art of command.

In all the organization's, military and non – military, the landscape is altered irreversibly, because exploitation of cyber space has enhanced 'efficiency' and 'productivity'.

The Challenge

On the flip side, advantages enabled by this disruptive capability has created new 'threat' vectors', for exploitation by inimical elements, non-state actors or adversial states. Achieving political aims by exploiting this medium or in conjunction with kinetic elements of military power is in the realm of 'Cyber Warfare'.Elements of this by Distributed Denial of Services (DDOS) was witnessed in Estonia and Georgia for achieving political gains. The other dimension of this warfare is psychological manipulation of the population for perceived advantages, as it is alleged happened during the last US Presidential election and earlier voting for Brexit. In the non-military domain this illegal use of the medium is in the realm of Cyber Crime and Cyber espionage. In case of InternalSecurity, it is Cyber Terrorism. A major area of concern is the increased susceptibility of individuals and organisations to financial fraud. In the worst case the financial loss is estimated to be as large as 1.6% of the GDP of a country. In India we are facing nearly double-digit cases of ransomware daily, misuse of cloned debit/credit cards

and ATM fraud due to breach of security protocols. Also, there are innumerable cases of hacking and manipulation of e-mail accounts of important personalities in the country.

India is assessed to be one of the top few countries in the world that faces cyber attacks daily. A report of a cyber security company, Fire Eyerevealed that Chinese hackers have been spying regularly on Indian Government and businesses since 2005, with reports of breaching sensitive computer systems at key establishments and disrupting the critical infrastructure of power, transportation and banking. The defense forces have also not been spared with intrusions within their captive nets. From Spear Phishing, to use of Intelligent and Vacuum Trojans, etc, the computer networks in our country have been compromised.

Therefore, there is an urgent need for the policy makers to put in place measures to safeguard the security of the private citizen to function in cyber space,especially with the national quest for digitization; concurrently there is a need to safeguard India's national economic, institutional and military structures, from the machinations of our adversaries with unscrupulous intentions. In addition, there is a need to simultaneously enhance national security by developing effective cyber defense and offensive capabilities. There is also a need to understand the legal provisions to safeguard interests and empower Law Enforcement Agencies to arrest cyber crime.'Cyber security' and 'cyber hygeine', data security regulations, relevant laws and capability for protection of critical infrastructure are a priority. Going by the experience of other nations who are ahead in this field, the security officials have to be conscious that there is nearly a ten-year gestation period before there is a semblance of coherence and synergy in the diverse fields of cyber defence and offence. The USA started addressing this issue in the late 1990s, laws were promulgated in 2003 and the formal structures dealing with cyber came into being in 2009 under the US Strategic Command and National Security Agency. The raising of 'Cyber command' was thereafter done only about two years back.

Also, they will have to actively interface with International organizations to carve out internationally acceptable norms on the 'Do's

and Don't's' of functioning in Cyber Space. As Asia becomes the digital pivot of the world, India will have to be proactive and be part of future cyber policy making structures.

Simultaneously, the technological mandarins will have to enhance the security of our networks with innovative harnessing of technology. There is a need for ensuring that the IT operations have self-secrecy, self-healing and preventive capabilities Use of AI and minimalizing of human interface in IT processes / operations for repetitive operational tasks, is the road for enhancing security and resilience in the 'cyber eco space'.

Threat Manifestation

The recent events across the world in the poltico- military - economic space, from disruption of critical public services as in the Ukrainian power crisis of 2016, to political arm twisting in Estonia/ Georgia/Ukraine and manipulation of mass perceptions for limited gains by interested parties or by non-state actors like ISIS for achieving their stated aim, has shown the potency of this new form of warfare. It has highlighted the following:

- Political and strategic goals can be achieved without armed conflict.
- Cyber-attacks are not restricted by national boundaries and are characterized by deniability, anonymity, non-attributability and relative impunity. Hence, traditional and physical boundaries are not relevant in this kind of warfare.
- It is characterized by extreme speed, lack of warning or indicators, ambiguity regarding the specified areas of battle, and lack of posturing. Therefore, traditional deterrence strategies are ineffective in this form of warfare.
- Blurring of the lines between the military and non- military targets to achieve political objectives by Nation States.
- Access to the Internet and easy availability of cyber tools also enable "Non- State Actors" to launch cyber-attacks.

- The tools and elements for waging ''Cyber Warfare'' are similar for both offensive and defensive actions.

The aspects enumerated above would provide the necessary direction of formulating the National Cyber Defence Strategy..

How do Major Nations Approach/Understand Cyber Warfare

The existing doctrine and proactive cyber defense programs have evolved globally over the past two decades. Presently USA, Russia, Israel and China have advanced capability in the field of Cyber Warfare. So a quick look at some of the important facets and key pointers.

USA sees this form of warfare as analogous to conventional warfare, with Cyber as another medium for conflict. It is conceptualised in technical terms, ie sending or implanting 'lines of malicious code from one computer to another, while protecting own IT systems and retaining the capability to cripple similar facilities of the adversary. IW or Info Ops are separate functions wherein cyber is a sub set that can be used to achieve IO objectives.

Russian doctrine emphasizes that an "information weapon" can be almost anything that has the desired impact on the targeted minds. It is important to note that minds are viewed as the target, rather than electronic or physical systems. As observed by Timothy L. Thomas, a US expert on Russian and Chinese cyber and information warfare strategies, Russian thinkers tend to break IO issues into specifically "information-technical" and "information-psychological" components. The "information-technical" component essentially overlaps with the American conception of cyber war. "Information-psychological" conflict, however, brings in a broad Russian understanding of the potential usefulness of the Internet and mass media in affecting the beliefs and attitudes of the adversary — not just its military or senior political leaders, but also its civilian population as a whole. Towards this the Russians have developed theories of what they call "reflexive control," in which information is manipulated in order to elicit favourable actions by the adversary.

Russia's new military doctrine, published in 2010, notes the importance of using IO tools not just to degrade an adversary's command-and-control functions, but to help create a positive view of Russia's actions. It suggests in particular an acute need for "prior implementation of measures of information warfare" — in advance of a conflict, in peacetime — in order to potentially 'achieve political objectives' without the utilization of military force.This is evident in their new form of hybrid warfare, also called the 'Gerasimov doctrine'.

China's overall conception of cyber conflict is like Russia, bound up with the control of information and the manipulation of adversaries' views and decision-making processes. This manipulation is meant to occur not just in wartime, but also during peacetime, so that it can ensure maintenance of a favourable peace, or in achieving victory without actually having to fight.

Modern Chinese writings say that the objective of information warfare is to subdue the enemy without a battle, and to trick him into adopting your goals as his owns(Gaining Initiative).Therefore, some Chinese writers identify communications and media as the main strategic focuses, suggesting that the key to success lies in a state's ability - "to gain the initiative over information resources and control of the production, transmission, and processing of information so as to damage information-based public opinion on the enemy's side."

A white paper released in 2010 and earlier remarks of a Senior Chinese General in February 2000, have highlighted that the objectives of cyber attack not only includes penetrating computer systems and transmitting disinformation to enemy military leaders, but also using cyber tools to "dominate" the enemy's "entire social order."

Preparation of the Battle Field

To cripple a country during cyber war, relentless peace time cyber activities will be focused towards identifying vulnerabilities in the adversary's critical infrastructure so that the systems can be hijacked and injected with cyber tools for use in future ops. To create these 'leverages' every potential adversary is covertly in the process of harnessing the

strengths of the cyber domain for exploitation at an opportune time, for it to gain ascendancy. This preparation of the cyber battlefield is achieved by placing logic bombs and trap doors in targeted computers. This is achieved by spear phishing, or through a human interface to infect host computers with intelligent and or vacuum trojans.The enormity of this activity can be gauged from the fact that 2,30,000 Malware are produced in a year. The defence forces have also not been spared with intrusions in their captive nets. Even the Pentagon during its penetration testing last year, identified 838 vulnerabilities. I am sure similar penetrative testing is being done in our official nets. These periodical checks or defensive /passive measures being adopted is part of 'cyber defence'.

It needs to be noted that internationally traditional espionage, subversion and sabotage has been overtaken by implanting malwares and exploiting botnets in thecomputer dominated work spaces. From the days of' wiper' for targeting computers in Iran, Israel and Middle East, to 'gauss' a surveillance virus in West Asia to spy on banking transactions, to the disclosure by mandiant about the APT attacks by Chinas PLA Unit 61398 on companies in the US and elsewhere in the world for economic & technological espionage, the cyber space has become extremely dynamic with newer threats and exploitation. Another dimension is exploiting the software vulnerability unknown to user and often the developer of the software, what is termed as'zero day' vulnerability.

Contours of Road Map and Present Status

Reports indicate that Japan & India are amongst the top nations that experienced major cyber attacks on a daily basis. China is now considered one of the foremost players in the field of cyber attacks. Role of Chinese hacking units has been detected in a large number of breaches that have been reported in different parts of the world. India continues to be a prime target of the Chinese cyber warfare effort. So our priority areas for firming in a measures for cyber defense, should study the Chinese 'modus oprendi' for 'preparing the battle space' in India. Some of the actions that we need to look at on priority are:-

- Study the measures being taken by the advanced nations to meet these threats and replicate the 'best practices'.

- Effective Cyber defence demands a change in the mind set of meeting this challenge. There is a need to be disruptive in meeting this challenge by forging partnerships between the Government agencies and the private players of cyberspace across disciplines, including manufacturers, service providers and individual citizens.

- The future cyber warriors need not only be military personnel, but include members of the industry, intelligentsia, hackercommunity and the student community. In fact, anyone having access to the ubiquitous computer can be a part of this team.

The country has started to put in place measures to meet the threats by promulgating the 'National Cyber Security Policy' in 2013. Also, the Govt cleared the National Cyber Security Architecture the same year. There is a National Cyber Security Coordinator but the impact is still not apparent. Defensive mechanisms like Cert -In under the Dept of Electronics and IT/ Ministry of Comn and IT (MOCIT),and a few others for specific sectors including by the Armed Forces are in place but purely defensive mechanisms and policies to protect own assets have not and will not stand the test of time. Where as, theNational Critical Infra Information Protection Center (NCIIPC) is in place and functions under the aegis of NTRO, Sector specific SOPs are still under finalization. We also have the Data Security Council of India (DSCI) set up by Industry to safeguard Data. In addition there is a special committee to look at enacting regulations for 'data security', while safeguarding the privacy of the individuals. However, there is a lot that still needs to be done.

Recommendations

To mitigate the cyber challenges there is a need for the following:-

- Requirement to outline India's National Cyber Security Strategy/ doctrine, in which Cyber Warfare is integrated from inception.

- Presently in India, we have a large number of stakeholders with concurrent or merging jurisdiction. Numerous agencies are responsible for Cyber Security, but no agency can be held specifically accountable for any incident. This needs to be

resolved by laying down boundaries and responsibilities so that convergence is achieved in this complex task.

- In addition there is a requirement for a single accountable agency at the national level which needs to function with military precision. It should be empowered for both the offensive and defensive operations in Cyber space. Need to move away from traditional org structures – implying that the new organization should have a permanent nucleus with the work force on contractual engagement, staffed with technically proficient cyber professionals with expertise across all formats of operations.

- Adopt a Multi-stake holder approach of government associating with the right partners through a public-private partnership to circumvent the existing shortcomings and challenges.

- Take stock of legal, regulatory and economic aspects of digital development in India, including development of frontier technologies in the financial sector. There is a need to specify working norms for the green field advanced technologies like Artificial Intelligence and Internet of Things.

- Evolve a model to strengthen the legal support system to address cybercrime-related cases. There is a need to expedite the process of enacting new, dedicated cybersecurity legislation, as the Information Technology Act 2000 is incapable of addressing cybersecurity challenges of the current times.

- Ensure Technological Sovereignity of critical hardware. There is a requirement to be oriented towards 'Security by Design'.Also, there is a need for stepping out of compliance-driven security mind sets and start the practice of self-regulated security within organizations. In addition need to prioritise development of tools and processes for effective offensive and defensive elements of Cyber Warfare.

- There is a need for an Incident Response Mechanism. It should have the capability to map risks arising from evolving threats. Towards this a workable private-public partnership model is needed, with a strong information sharing platform on a real-time or near real-time basis, providing feeds on malicious cyber threats

and attacks and appropriate mechanisms to address these. This would require development of a resilient cyber security model. Also, making it binding for all to report/ sharing information of breaches in real time to be able to stem proliferation of malicious malaware.

- There is a need for increased awareness of this threat spectrum and enhanced security consciousness. Also need for Skill development for creating a technically proficient work force. There is an urgent need for upgraded resources in terms of manpower & technology.
- Develop robust and resilient ICT Infrastructure, with in built security, across fields and processes.

Conclusion

There is no doubt that there is a lot of focus on cyber security at the highest level, as was evident with India hosting the last Global Conference on Cyber Security and this being highlighted by our Prime Minister at the recent Global Economic Forum at Davos. But it is reiterated that at the national level we need to look at a vast array of related issues that will impact us in the near future while putting in place security organisations / mechanisms. The spectrum includes issues of data protection, ethics of AI for applicability in IOT, privacy of the individual, the responsibilities/ legalities of Data Mining (jurisdiction of Google for data that it collects while setting up free wifi facilities at 100 stations), the role of ICANN, India's activism in IETF, Net Neutrality, Internet Governance etc. In conclusion the wise words of cyber gurus is highlighted that is "Cyber Security is not a technology problem that can be 'solved.' Rather, it is a risk to be managed by a combination of defensive technology, astute analysis and traditional diplomacy."

***Lt Gen Arun Sahni** is a former C-in-C, Indian Army

NON TRADITIONAL THREATS – ECONOMIC, ENERGY, WATER, FOOD

Brig Rahul Bhonsle, SM (Retd)*

"A single man-made stock market crash, a single computer virus invasion, or a single rumour or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the internet, all can be included in the ranks of new-concept weapons" - Colonel Qiao Liang & Wang Xiang Sui, PLA Air Force & Authors of "Unrestricted Warfare"

Security – The Widener's View

Security is commonly linked with the existential or transitional threats related to nation states impacting survival of the whole or part of a country, its region and peoples. There was a physical aspect to security entailing a direct or indirect act of violence and bloodshed. Under the Westphalian model which is the basis of modern states, the government is the only entity that can justify use of controlled violence for survival. Security is also seen as justification by State authority to secrecy, denial of information and use of extraordinary legal means to pursue an objective of peace and tranquility.[1] However this narrow definition of security is found to be incongruent in the post modern world with growth of individual rights and liberties, non state actors and tools employed by state entities to sustain their national goals and objectives without the use of violence. This school in international security known as the Widener's School propagates a paradigm of security that goes beyond the use and control of military force.[2]

In the context of the Widener's School also known as the Copenhagen School the scope of issues that can be included into security are based on referent objects which will require emergency and survival measures. These referents are all in the military domain and can be applied to varied sectors ranging from the military to political, economic, societal and environmental. The main factor to determine securitisation of a particular referent object is the type of existential threat posed. For instance in the context of the military this would be survival of the state as a whole in terms of territorial sovereignty whereas in the political could be the form of government and ideology. In the economic sphere denial of an opportunity for growth and development poses a survival threat for a state in many different ways ranging from bankruptcy to failure of institutions and the people. Similarly energy security entails access to sustained supply of resources for not only survival but for sustainable development and increasingly clean environment. Thus there are two facets which can create insecurities – deficit and politics. This dimension of security more popularly known as non traditional security mainly economic, energy, water and food are being examined in the Indian context as per succeeding paragraphs.

Economic Security

Economic security in a globalised World has varying dimensions. Defining economic security has posed a major challenge for inter dependencies built in economies implies that no state or group of people can be regard as fully secure from the economic point of view. In the Flat World described by Thomas L. Friedman in his seminal work, "The World Is Flat: A Brief History of the Twenty-first Century", under ideal conditions there is a level playing field for all entities but as such conditions seldom prevail in the real world insecurities are bound to arise even from a high level of interconnectedness. For instance a stock market crash in any of the large exchanges in the World from New York to London or Tokyo has an immediate impact on Bombay or National Stock Exchange in India. However in the definitional sense this cannot be classified as survival threat to the nation as a whole but may have a combined effect leading

to security of the fiscal, monetary and fiduciary resources impacting large number of individuals leading to slowdown in development and growth. In extreme cases this will also have spiralling impact on the political or national security and sovereignty leading to capitulation of the system. The Soviet Union is a ready example of a state collapse due to non tenability of economic performance.

To examine the challenge more closely, economic security can be seen as an outcome of unequal distribution of resources be it natural, capital, manufacturing and so on that provides unfair advantage to a state over another. Another manifestation of economic security is constant risk associated with impact on freedom and choice due to a number of factors.[3] Vincent Cable chooses to describe economic security in varied ways to include, "those aspects of trade and investment which directly affect a country's ability to defend itself, freedom to acquire weapons or related technology, reliability of supplies of military equipment or threats of adversaries acquiring a technological advantage in weapons".[4] If economic activity is viewed as a major source of power as indicated by Samuel Huntington then economic security also entails economic nationalism through means as protectionism and sanctions on an adversary to coerce him in doing what is in one's own interest. [5]

Advocates of security of supplies can be found in many countries. This is a political tool for generating nationalist fervour while reducing dependency on external sources. In the wake of India China standoff at Doklam from June to August 2017, there was a large movement against import of Chinese goods with demonstrations held in various cities. As the two countries came to an agreement resulting in disengagement this movement has petered out. South Korea faced a constriction in 2016-17 after the national leadership decided to deploy the United States made Terminal High Altitude Aerial Defence (THAAD) system in defence against a possible North Korean missile threat. China objected to the deployment stating that this will adversely impact strategic deterrence with the United States as the THAAD will be able to monitor effectively any missile launched from Beijing. China imposed severe restrictions on

South Korean companies and even curtailed tourist movement having a deleterious impact on the economy of the country. While this did not lead to a state collapse, it did lead to South Korea seeking a compromise assuring the Chinese that it will not deploy any more THAAD batteries in the future indicating the power of economic muscle flexing.

Resources are a perennial cause of economic insecurity particularly oil and gas given the dependency on the same for running of national systems from transportation to power generation. While this aspect will be covered in detail in the subsequent section, suffice to say those states having abundant supplies can be considered as more secure than others and more so are able to exercise a greater degree of influence by manipulating supply. Cartelisation is another phenomenon with the formation of the Organization of the Petroleum Exporting Countries (OPEC) dependencies to price manipulation has greatly impacted economic security of countries as India and in turn the power that is exercised by the grouping.

An alliance of resource rich and developed economies is another mechanism that is being exploited to advantage by what can be said as the haves over the have-nots. “Historically those countries which industrialized first and controlled most of the advanced technology and capital supplies enjoyed a position of leadership in international affairs” says Lester Brown, “but the shift is occurring due to growing dependence of the countries that industrialized earlier on imports of energy fuels and raw mat1erials and the growing global scarcity of raw materials.” Control by developed and industrialised economies of developing countries provides substantial political leverages which have been used in tandem with resource rich countries. United States strategic partnership with Saudi Arabia and the Gulf countries is an example of combination of strengths with interests for mutual advantage. This is used as a coercive tool against adversaries as Iran – which is seen as an enemy nation indicated in the US National Security Strategy 2017 released by President Donald Trump in December 2017.

The Gulf countries were challenged by removal of economic sanctions against Iran after the Joint Comprehensive Plan of Action, was signed on 14 July 2015 by Tehran with the EU 3+3 or UK, France, Germany, China, Russia and the US. This led to the United Nations Security Council removing decade's old sanctions on Iran freeing the economy releasing resources for expansion of Iranian national power in many dimensions including defence and security. It is no surprise that Saudi Arabia welcomed the proposal by the United States President Donald Trump to renege on the nuclear deal stating that Iran has not stopped manufacture of missiles and sponsors terrorism in the region.

Some conclusions that can be arrived at is that economic security is a soft yet all encompassing threat impacting a far large cross section of the population in a country than perhaps even military security. This can take varied forms such as triggering a stock market crash described in the book, "Unrestricted Warfare" by two People's Liberation Army Air Force Colonels.[6] Trade wars and economic sanctions are another tool used especially by the West frequently for political ends. What is important to note however is that these measures have a limited time span before states devise strategies to overcome the encumbrance. For instance India and Afghanistan have now opened the Chabahar route for supplies in conjunction with Iran thus offsetting the transit blockade by Pakistan. Iran adopted what is popularly known as the Resistance Economy to beat American sanctions – propelling economic growth internally.

Money laundering and counterfeit currency is another major form of economic warfare that can be waged by states against adversaries. "Hawala," transactions or informal network for transfer of money have been used to fund terrorism in Kashmir with flow of money supporting the large Separatists network which is presently under scrutiny of the National Investigation Agency (NIA) in India. Pakistan's counterfeit war against India was spread geographically from Nepal to Bangladesh using pliable Indian agents to flood fake money in the Indian economy.

While the network was exposed first in the 1990's the same continues to flourish and it is apparent that demonetisation has been but a temporary pause for agencies operating on the behest of Pakistani handlers from across the border. On November 14, 2017 for instance, the NIA, Kolkata Branch team seized Fake Indian Currency Note (FICN) valued at Rupees 9.1 lakh [in the denomination of INR 2000 which were introduced post demonetisation in November 2016] from the vicinity of Howrah Railway Station, Kolkata, from four persons.[7] Bit coins could be the next level in money laundering as presently the sector is completely unregulated and exchanges are operating across national domains.

A strong, effectively regulated economy with inherent strengths and effective governance devoid of corruption remains the most efficient option to ensure economic security.

Energy Security

Energy security is related to sufficiency in resources particularly oil and natural gas as human activity today is dominated by consumption of fossil fuels. Uncertainty of supply and risk of breakdown creates a major challenge to national security even impacting war waging capability of nations. India remains dependent on imports of oil and gas. With the government committed to provide fuel to the masses at affordable prices there is a huge subsidiary burden which also impacts debt. India has not had much success in discovery of domestic oil reserves, however it is apparent that there is a good prospect for gas in the offshore belt be it Bombay High or the Krishna Godavari Basin on the East Coast.

Resource alone is not sufficient to sustain energy security but there is a need for overall capacity of exploration, extraction, refining and delivery for the nation to have assured supply of oil and gas. The other non fossil fuel on which India has been dependent is coal. While there were some estimates that India may have vast coal reserves that would last for 200 years this has been recently revised to 40 years based on peak production level of about 700 million tonnes per annum (MTPA).

[8]As per Indian Energy Security Scenarios India's dependency on oil imports is unlikely to come down and in fact rise up to 87 % in 2047.[9]

The Government of India has planned to create strategic crude oil reserves in the country. Indian Strategic Petroleum Reserve Limited (ISPRL) is setting up strategic crude oil reserves with storage capacity of 5.33 Million Metric Tonnes (MMT) at three locations viz. Visakhapatnam (1.33 MMT), Mangalore (1.5 MMT) and Padur (2.5 MMT). In 2016, existing tankage of 14.8 MMT of crude oil and 13.7 MMT of petroleum products were available in the country which provided coverage of approximately 63 days as per consumption. The Vishakhapatnam cavern has been commissioned and filled with crude oil. Mangalore and Padur caverns are reportedly under various stages of completion.[10]

In the long term, alternative for energy security remains harnessing vast potential of renewable resources such as wind, solar, hydro power and so on. While nuclear energy is one option, dependency on foreign companies for construction of plants and the controlled regime poses own challenges. Never the less other alternatives will have to be explored to harness resources for growth and development so that there is adequate leverage and the country is not bogged down by denial or suturing of supply in one sphere. Initiatives such as International Solar Alliance (ISA) conceived as a coalition of solar resource rich countries to address their special energy needs will go a long way to synergize resources and technologies for the effective use of solar energy. Similarly India has ample wind energy resources which need to be harnessed to advantage. Finally the right mix of energy to include fossil and non fossil fuels, renewable and non renewable with a view to sustain economic growth will remain the challenge.

Water Security

Water is an essential source required for human survival without any substitute for varied human activity ranging from agriculture, manufacturing to construction as well as daily consumption. India is

a water scarce country. Essentially the agrarian human ecosystem in India is dependent on ample availability of water at an appropriate time coinciding with the sowing of crops. The availability of water is under stress due to a variety of factors including inability to harness the vast resources in the Peninsula. Surplus water from the Himalayan ice melt or the monsoons has been drained off resulting in deficiency in many parts of the country. Conflict over water between States is also an indicator of the challenge of water security. The Cauvery water dispute between Karnataka and Tamil Nadu has been debated extensively with the Executive as well as the Judiciary failing to come up with a viable formula for equitable distribution that is acceptable to people of both the states. There are other disputes which have potential for creating challenges to state governments such as the Mahadayi River between Maharashtra, Goa and Karnataka.

Declining water table is another factor which is leading to stress in the long term. The water table in South Asia is receding at an alarming rate of 1 meter every year. Conflict can also arise from water scarcity due to politics over disparity of supply between states and nations, depleting reservoirs, lack of water sharing agreements and allegation of over exploitation by upper riparian states.

The last named factor has been a source of tension between India and Pakistan over sharing of waters of rivers despite the Indus Water Treaty of 1960. There is a growing perception in India that China has been over exploiting waters of the Brahmaputra in Tibet by building dams over the same and is unwilling to share information despite existing agreements. This phenomenon is not uncommon as 17 river basins across the World which are shared by 31 nations are identified as having potential for water wars, Importantly the Ganga - Brahmaputra – Meghna Basin is in the category of highest threat identified as, “basins at risk”.[11]

To avoid conflicts over water actions at multiple levels are necessary ranging from multilateral treaties to bilateral agreements

on the lines of the Indus Water Treaty of 1960 which has withstood bitter hostilities between the two countries in the past many decades. Information sharing is another important confidence building measure which has to be implemented in letter and spirit. At the subterranean level there is a need for conservation and preservation with best practices being adopted by individuals and communities. Crisis prevention and mitigation measures are thus required to be implemented across the board.

Food Security

Food and Agriculture Organization (FAO) of the United Nations defines food security as, "a situation that exists when all people, at all times, have physical, social and economic access to sufficient, safe and nutritious food that meets their dietary needs and food preferences for an active and healthy life".[12] The expanded definition of food security underlines importance for adequacy of food to lead an active and healthy life which will remain a key challenge for countries as India. While legislations as Right to Food have been enacted in India, there are serious concerns over food security as mapped by the Global Hunger Index (GHI) 2017 where India ranks at the 100th place along with Djibouti, Rwanda and Uganda.[13] Clearly much more will have to be done to ensure food security as defined by the Right to Food Act and conforming to the global norms set by the FAO. Focus will have to move from enactment to implementation outlining the underlying challenges in governance.

Conclusion

While the scope of state on state conflict in the world has reduced non traditional threats have emerged as major concerns particularly for developing countries as India. These are also giving rise to the, "Two India's," phenomenon. India is the third largest economy in the World based on GDP PPP, yet faces numerous challenges in multiple spheres which have manifested in the scores of insurgent and rebel movements that span the country from Jammu and Kashmir in the North to Left

Wing Extremism in Central India to the North East. Apart from political issues as identity and self determination a major factor spurring these movements is existence of insecurities outline above to include economy, water, food and energy. Development as a panacea will have to address the non traditional security challenges holistically.

ENDNOTES

1. Barry Buzan Et Al. "Security a New Framework for Analysis. Lynne Rienner. Boulder, USA. 1998. P 21.
2. Klare, Michael T. The New Geography of Conflict. Foreign Affairs, Vol 80. ON 3. P 49.
3. Cable, Vincent. What is International Economic Security? National and international Security. Ed Michael Sheehan. Ashgate. Adler shot. 2000. P 310.
4. Ibid. P 311.
5. Ibid. P 316.
6. Colonel Qiao Liang &' Colonel Wang Xiangsui. Unrestricted Warfare: China's Master Plan to Destroy. Translation. 10 Nov 2015
7. Press Release NIA seized fake currency of over 9 lakh. Available at http://www.nia.gov.in/writereaddata/Portal/News/219_1_PressRelease 16112017.pdf. Accessed on 24 December 2017.
8. India's energy security: new opportunities for a sustainable future. Available at http://www.teriin.org/events/CoP16/India_Energy_ Security.pdf. Accessed on 21 December 2017.

9. India Energy Security Scenarios. Available at India's energy security: new opportunities for a sustainable future. Accessed on 21 December 2017.

10. Government of India. Ministry of Petroleum and Natural Gas. Strategic crude oil reserves in the country. Available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=136696. Accessed on 21 December 2017.

11. Postel, Sandra. Et Al. Dehydrating Conflict. Foreign Policy. Sep/Oct 2001. P 65.

12. FAO. 2002. The State of Food Insecurity in the World 2001. Rome. Available at http://www.fao.org/docrep/005/y4671e/y4671e06.htm#fn31. Accessed on 21 December 2017.

13. 2017 global hunger index: The inequalities of hunger. Available at http://www.ifpri.org/publication/2017-global-hunger-index-inequalities-hunger. Accessed on 23 December 2017.

***Brig Rahul Bhonsle (Retd)** is a renowned Delhi Based Security Analyst

CURRENT AND FUTURE CHALLENGES OF UN PEACEKEEPING

Lt Gen Chander Prakash, SM, VSM (Retd)*

Introduction

Peacekeeping is one of the cornerstones of the United Nations and is an essential tool for bringing about peace and stability in war-torn societies. The international system has changed in many ways since the first deployment of peacekeepers in 1948; new actors and challenges have emerged and the mandates have evolved over the years. With the end of the Cold War, many important changes have occurred. Armed conflicts are now more often than not, at the intra-state level with regional and international involvement and ramifications.

The traditional model of UN peacekeeping developed during the Cold War era as a means of resolving conflicts between States, involving the deployment of unarmed or lightly armed military personnel between belligerent parties, has undergone a change. With rise in number of intra-state conflicts, there is a shift towards multidimensional peacekeeping. This trend is likely to continue in the foreseeable future, and could lead to an increase in the size of the military component of peacekeeping operations, however its success to a great extent will also depend on the work of the civilian experts in key areas such as the rule of law, human rights, gender, child protection, and elections. However, a robust military presence would be essential, particularly during the initial stages of a peacekeeping operation in order to deter potential spoilers and establish the mission's credibility.

Currently most of the large UN peace operations are facing situations of open conflict. Even after so many years of UN peacekeeping

in the Democratic Republic of Congo (DRC), the situation in the eastern part of the DRC with the presence of over dozen armed groups remains politically instable and volatile. Situation in Mali, South Sudan, and the CAR is no different. War broke out in South Sudan two years after the deployment of the UN peace operation and the armed groups continue to operate in Northern Mali and different parts of the CAR despite the presence of UN operations. Noteworthy from this is that the UN peacekeeping operations are being mandated to operate in areas where there is no peace to keep. The fact is that UN peacekeeping operations are being authorized by the Security Council in the absence of clearly identifiable parties to the conflict or a viable political process. The UN peacekeepers are increasingly operating in more complex environment than what prevailed few years ago. In future, the peacekeepers will also have to deal with asymmetric and unconventional threats. In such increasingly volatile and unstable environment, the UN peacekeepers will be confronted with threats that would directly challenge their ability to operate. Is the international community adequately prepared or preparing for it, is a moot question that remains to be answered.

Evolution of UN Peacekeeping

The founders of the UN made no explicit provisions for peacekeeping in the UN Charter that came into force on 24 October 1945. Lacking specific legal provisions, peacekeeping has emerged largely through precedence. The principles and customs of peacekeeping have been moulded by the actions of various missions in order to manage crises, mostly post-occurrence of a crisis and lessons learnt from thereon. Therefore, any discussion on the future challenges of UN peacekeeping must start by highlighting how the peacekeeping has evolved other the last 70 years.

During the period of Cold War peacekeeping operations were largely military in composition and their tasks were to monitor cease-fires, control buffer zones, investigate alleged arms flows, and prevent resumption of hostilities. They were required to maintain calm on the front lines and give time for the diplomats and others to negotiate a settlement of the dispute that had led to the conflict. Notwithstanding the

outcome of the political negotiations, UN peacekeeping forces prevented the further expansion of many conflicts and contained it. This is referred to as the classic or traditional peacekeeping operations.

Post-Cold War era, the contemporary United Nations peacekeeping operations were more nuanced and are multidimensional in nature. In 1992, in the aftermath of the Cold War, then Secretary-General Boutros Boutros-Ghali had put together a report detailing his ambitious concepts for the United Nations and peacekeeping at large1. The report, titled "An Agenda for Peace", described a multi-faceted and interconnected set of measures he hoped would lead to effective use of the UN in its role in post-Cold War international politics. This included the use of preventive diplomacy, peacemaking, peacekeeping, peace enforcement and post-conflict reconstruction.

Now, the UN peacekeeping had grown in numbers and complexity. After the Cold War ended, there was a rapid increase in the number of peacekeeping operations. The Security Council authorized a total of 20 new operations between 1989 and 1994, raising the number of peacekeepers from 11,000 to 75,000. In 1988, the UN operated just five peacekeeping missions. In 1990, the UN had only 10,304 peacekeepers from 46 Troop/Police Contributing Countries (TCCs/PCCs). There has been a surge in uniformed UN Peacekeeping personnel from 1991 to the numbers today. As on September 2017, there are approximately 110,000 personnel serving in 15 UN peacekeeping operations and the financial outlay is approximately USD 8 billion as against USD 2.5 billion in 2003.[2] The emergence of conflicts such as Syria and the Middle East spreading beyond local and regional boundaries signal that the demand for field peacekeeping missions will be high and peacekeepers will have to handle most complex operational tasks.

---

1 UN Documents, Gathering a body of global agreements, 17 June 1992. Available at http://www.un-documents.net/a47-277.htm. Accessed on 15 December 2017.

2 Statement of ASG Ms. Jane Holl Lute, Officer-in-Charge of the Department of Field Support to the Special Committee on Peacekeeping Operations on 10 March 2018.

Challenges of UN Peacekeeping

UN peacekeepers, as the trend is emerging, are going to be increasingly charged with large number and varied tasks to include providing assistance to the political processes, assisting in reforming the judicial systems, training law enforcement and police forces, disarming and reintegrating former combatants, and supporting the return of Internally Displaced Persons (IDPs) and refugees. Electoral assistance will also be an essential feature in UN peace operations. This is not something new. The UN peace missions in the past have supported elections in severalpost-conflict countries, such as Nepal, Afghanistan, Burundi, Haiti, Iraq, Liberia, the DRC and Timor-Leste, with populations totaling over 120 million people, giving more than 57 million registered voters the chance to exercise their democratic rights.[3] Therefore, peacekeeping has become challenging due to the sheer magnitude and complex nature of the mandate and tasks involved.

Post-conflict societies lack institutions of governance; there are issues of human security and development challenges. Lessons from past operations in Bosnia and Herzegovina and in Rwanda, have led the UN to mainstream the protection of civilians in peace operations, often as a priority task of the mission. The fact that the peacekeepers will be deployed in conflict theaters where there is no political agreement or peace to keep and hardly any support from the host nation, the protection of civilians will continue to present complex challenges to the peacekeeping missions. In its 2015 report, the High-Level Independent Panel on UN Peace Operations (HIPPO) stressed on several occasions that UN personnel operate in "increasingly dangerous environments." UN peacekeeping has undergone significant evolution … [resulting in] asymmetric hostile acts against UN personnel becoming a more regular feature of many missions.4 Peacekeepers while providing protection

3 UN Peacekeeping Fact Sheet. Available at http://www.un.org/en/events/peacekeepersday/2008/factsheet.shtml. Accessed on 01 December 2017.

4 Haidi Willmot, Scott Sheeran, and Lisa Sharland, "Safety and Security

to civilians under imminent threat will be increasingly confronted with asymmetrical threats emanating from armed groups, terrorists or organized crime groups or even for that matter rogue elements of a State security apparatus.

Attacks on UN peacekeepers, most recently on 07 December 17 in the Democratic Republic of Congo in which 15 UN peacekeepers were killed,[5] and previously attacks in Mali are not a new phenomenon. However, the modus operandi of the armed groups, particularly with the use of Improvised Explosive Devices (IEDs) and suicide attacks on UN Bases could create new vulnerabilities for the peacekeepers. Two major challenges emerge from this. First is, how and when should the peacekeepers respond. This carries the risk of dragging the UN contingents into military confrontation with some of the hardened and fundamentalist armed groups.

The other issue is how these new vulnerabilities impact the peacekeeping operations' mandate, for example protection of civilians vs force protection (protection of UN personnel and UN assets). Any configuration where Blue Helmets are directly and repeatedly targeted and ill-equipped to respond or even protect themselves is likely to reinforce the temptation of risk aversion and inactivity at the expense of mandate implementation.

As highlighted above, the UN peacekeeping missions operate in an ever-changing and volatile environment that directly impacts their organization and overall effectiveness. From the Democratic Republic of the Congo (DRC) to Mali or South Sudan, peacekeepers face huge challenges in the implementation of their mandate. The management of Internally Displaced Personnel (IDPs), which are likely to be large in numbers, is also going to be a major challenge for the peacekeepers.

Challenges in UN Peace Operations," International Peace Institute, July 2015.

5 Islamist attack kills at least 15 UN peacekeepers and five soldiers in DRC, The Guardian 08 Dec 17. Available at https://www.theguardian.com/world/2017/dec/08/peacekeepers-killed-in-attack-on-un-base-in-dr-congo

The first and most demanding challenge stems from the very nature ofa peace operation in a sovereign country. More often than not, in the future, peacekeeping operations will be undertaken in States undergoing internal conflict, usually based on ethnic, racial or religious grounds that are manipulated by various factions seeking political power and control of vital economic resources. This would create large displacement of population who will be victims of human rights violations. Managing the IDPs is one of the most sensitive issues. The achievements of the uniformed peacekeepers can be undermined if necessary care is not taken by the military element of the UN Peacekeeping Mission. Therefore the sensitivity and complexities need to be understood. The Troop and Police Contributing Countries (TCCs/PCCs) will need to impart specialists training to their personnel as part of the pre-deployment training.

As peacekeeping becomes more complex it will be difficult for the military component of a peacekeeping mission to remain completely neutral. There will be situations when peacekeepers will be required to take coercive action against the spoilers and others trying to undermine the peace process and impinging on the wider peacebuilding mandate. Whatever be the case, the peacekeepers will have to remain impartial in their dealings with the parties to the conflict but not neutral in execution of their mandate and retain their credibility and legitimacy. The challenge will be to remain even-handed with the parties and being criticized for action or inaction for a behavior that is seen as clearly working against the furtherance of the peace process.

The problems will get further accentuated when there are gross human rights violations but the legal systems remain ineffective. Generally, political considerations and compulsions of the UN Member States and TCCs/PCCs will prevail over military operational requirements. This leads national caveats or weak mandates which are going to be exploited by war lords and armed groups often leading to attacks on the UN peacekeepers. The experience of the Indian Brigade deployed in the North Kivu province of the Democratic Republic of Congo highlights this issue. The directions given to the peacekeepers and the legal provisions very often severely limited the actions required to be taken to prevent civilian causalities. In many cases, in the Indian peacekeepers could not

retaliate despite provocations due the complex rules of engagements, the possibility of collateral damage and lack of clarity in the mandate.

For the peacekeeping operations to be successful, it was essential that the parties to the conflict offer their collaboration and support. However, in recent conflicts, involving ethnic-based disputes, internal political struggle or the collapse of State institutions, the UN has been acting without the clear consent of the parties to the conflict. The result is that, the environment for peacekeeping is no longer benign. Therefore, in the future, the waters in which the peacekeeping will be undertaken are going to be muddy. The equipment requirement and standard operating procedure will need to be revisited. In addition to the traditional peacekeeping tasks, the emphasis will have to be on disarmament, human rights observation and robust peacekeeping.

The non-availability of optimal levels of personnel, equipment and other resources in peacekeeping missions is one of the major challenges leading to failure of peacekeeping efforts. The peacekeeping missions in the field sometimes have to deal with a lack of adequate and the right kind of resources. This is a major issue that is likely to limit their effectiveness. Modern peacekeeping is a complex task; it requires appropriately trained and resourced troops to form an effective and efficient force. The right type of equipment - vehicles, armoured personnel carriers, engineering equipment and helicopters are all essential to enforce the given mandate in strife ridden areas with poor infrastructure. However, there is often a great discrepancy between the quantity, quality and serviceability of resources provided by some of the countries.

Finding troops with the necessary training, equipment and logistical support to effectively undertake these complex and often dangerous tasks will be a challenge but will remain a key determinant of a peace operation's success. However, this is easier said than done, since the Member States who possess such capabilities have often expressed nuanced unwillingness to make them available for UN peacekeeping operations. Equipping the UN peacekeepers with enablers such as engineers, police, medical and aviation assets etc. will always pose

challenges as their availability with the Member States especially the developing countries is limited and the demand is high.

Recently the UN peacekeeping missions have also been mandated to undertake peace enforcement tasks. Peace enforcement missions are undertaken when there is a lack of consensus between the warring parties. This type of mission entails additional military risks to the peacekeepers and a strong military structure in the UN. Maintaining the fundamental distinction between peacekeeping and peace enforcement will pose a great challenge both at the operational and strategic level.

The tendency to combine peacekeeping with peace enforcement actions as is the case with the United Nation's Operation in the Democratic Republic of Congo, carries with it considerable operational and political risks. This is likely to get more complex by virtues of what is being camouflaged under the term "robust peacekeeping" to overcome the political limitations of peace enforcement. There will always be the challenge of managing the tensions and fall out of varied interpretations of the mandate by those involved in mandate formulation at the UN Security Council and those implementing it on the ground. TCCs/PCCs especially the large troop contributors and emerging countries like India, will demand more strategic space in mandate formulation and decision making, which the big powers are likely to resist.

At the political level, the missions' strategy, actions and mandate renewal are subject to Security Council approval, therefore, vulnerable to bargaining and shifting political alignments among members of the UN Security Council. Another important aspect is that the peacekeeping and peacebuilding efforts require a long term commitment of resources and finances. However, the ever present concern among the finance contributing Member States in particular the United States over the reduction in the peacekeeping budget, exit strategies and avoidance of quagmires have led to formulation of unrealistic time frames and quick impact projects which fail to serve the long term interests of developing sustainable peace.

Moreover in the future, at the conceptual level, there is going to be challenge over defining what the scope of the peacekeeping mission

should be and the limits of its responsibilities once the operation has been decided. The reality is that the boundaries of commitment are not decided as per the requirement of the UN but the interests of States that contribute financial and other resources. Hence, the interpretation of the mandate tends to vary. The outcome therefore is that there is a conflict in the priorities and the commitment shown by the powerful Member States is according to their interest which implies that some operations will be given more attention than others.

Another challenge to the peacekeeping operations, particularly with respect to the protection of civilians, will be the issue of sovereignty. Globalisation and the rise of intra-state wars have diminished the power of States as the main players in conflicts and more often than not, the State too is a party to the conflict but authority of the State needs to be ensured. The contradiction is that the UN was set up, not to protect governments and States, but to 'save next generations from the horrors of war.' In the changed landscape, the challenge is how the UN does upholds principle of sovereignty and how the peacekeepers conduct their operations without being perceived as impinging on the sovereignty of the sovereign State whose elements are a part of the problem.

Finally, irrespective of the degree of the political support and the institutional efficiency that may come about in the future, given the explicit mandate of protection of civilians (which will always be the case in future); the UN peacekeepers will have to carry a heavy weight of managing expectations. With an active and intrusive media, putting in place effective strategic communications is always going to be a challenge.

Conclusion

The peacekeeping operations have been changing its dimensions and spectrum from the cold war era to post-cold war period. The most prominent change is the transition of conflict from interstate conflict to intra state conflict with regional and international players being involved. The nature of peacekeeping will continue to evolve as per the nature of conflict. The changing nature of peacekeeping to keep pace with the changing nature of conflict will throw up new challenges. Whatever

be the case, the humanitarian issues will be most prominent where the peacekeepers will need to prove their worth while working in parallels with civil agencies. While working in the conflict area, troops will need to act neutral and impartial and keep a balance amongst the belligerents and will need to know the difference between being neutral and inactive and act accordingly. There will always be challenges with respect to the issues of sovereignty, right and reasonability to protect, alleviate human suffering and balancing between the three cardinal principles of UN peacekeeping i.e. consent, impartiality and use of force in self-defence and in support of the mandate. New and complex environment, together with the ambitious objectives of the United Nations and ever-growing pressure on scarce resources will continue to make the peacekeeping a more challenging and demanding enterprise. Important troop contributing countries like India, will need to define its peacekeeping policy and address the doctrinal and resource issues.

***Lt Gen Chander Prakash** is a Deputy Director USI, New Delhi

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND EXPLOSIVE (CBRNE) THREATS

Brig (Dr.) Rajeev Bhutani (Retd)*

Introduction

The chemical, biological, radiological, nuclear and explosive (CBRNE) threat is not new. The usage of biological and chemical agents as weapons of war can be traced to the earliest days of human history - somewhere around 1500 and 1000 BC respectively.[1] However, evolved over time, first the use of chemical weapons became more pronounced during World War I and thereafter other facets of this threat emerged as we face today. Although there have been many attempts to ban chemical, biological, radiological, and nuclear warfare agents, their devastating potential makes them still attractive for regular armies as well as for terrorists. The terrorists' obsession with CBRNE devices is considered a major threat because weapons of mass destruction place the greatest number of people at risk. Therefore, it is appreciated that the emergence of CBRNE terrorism is going to be a significant security challenge in the 21st Century.

More recently, the prospective linkage between terrorist organizations and state actors with weapons of mass destruction programmes has become an acute security concern. Though each element of the CBRNE threat has its own peculiar characteristics and needs altogether different counter-measures to handle it, the common features which bring them together under a common head or acronym are: the ability of even small groups of individuals to cause massive damage and extensive human sufferings with little or no warning; and perhaps the most difficult aspect of the terrorism problem to assess or predict the time, place and choice of weapons and tactics, as it was

demonstrated by the September 11, 2001 attacks.

CBRN can be weaponized or non-weaponized and both can cause great harm and pose significant threats in the hands of terrorists. Weaponized materials can be delivered using conventional bombs (e.g., pipe bombs), improved explosive materials (e.g., fuel oil - fertilizer mixture) and enhanced blast weapons (e.g., dirty bombs). Non-weaponized materials are traditionally referred to as Dangerous Goods (DG) or Hazardous Materials (HAZMAT) and can include contaminated food, livestock and crops.[2]

CBRNE Incidents: Accidental vs Incidental. The Armed Forces will be required to handle CBRNE threats both as an accident or as an intentional incident. An ***accidental CBRNE incident*** is caused by human error or natural or technological reasons, such as spills, accidental releases or leakages, for example: accidental leakage of methyl isocyanate gas from Union Carbide India Limited (UCIL) pesticide plant in Bhopal on 3 December 1984, the worst industrial accident in history at that time - with a final death toll estimated to be between 15,000 to 20,000 and some half a million survivors continued to suffer with lifelong medical problems because of exposure to the toxic gas[3]; Earthquake induced damage to Fukushima Daiichi nuclear power station, Japan on 11 March 2011 resulting into leakage of 20 to 40 becquerels of radioactive tritium into the ocean and evacuation of an estimated 200,000 people from the area - considered the nuclear disaster since the Chernobyl meltdown in Ukraine in 1986[4]; Outbreaks of infectious diseases, such as SARS or pandemic influenza are naturally occurring biological incidents. An ***intentional CBRNE incident*** consists of: terrorist acts that involve serious violence to persons or property for a political, religious or ideological purpose and / or that for a matter of national interest; the malicious poisoning of one or more individuals; and criminal acts such as the deliberate dumping or release of hazardous materials to avoid regulatory requirements.[5]

First Responders. It may be interesting to note that first responders in any of these CBRNE accidents / incidents will be firefighters, police personnel and civilian volunteers etc. Further, rescue

and treatment of victims and control or containment of fire and other hazards will be greatly complicated by the fact that the site may also be contaminated with chemical, biological, nuclear or radiological substances that pose an immediate danger to the health and safety of the emergency responders. Also, the immediate impact of such attacks may travel much farther than the scene of the disaster. Multitude of injured and potentially contaminated victims may depart the scene, returning to the suburbs and neighbouring cities where they reside, or privately seek medical assistance.[6] This predictable exodus from the place of such attack has to be handled quickly. Thus the first responders have to be as conversant as the security forces or disaster relief experts who arrive later, in dealing with situations created by CBRNE agents or weapons.

To find appropriate answers for current and future CBRNE threats, we need to understand and analyze the peculiarities of each of its elements, beside knowing their history (History of CBRN weapons usage in condensed form is given in Annexure 1) so that a suitable response mechanism can be created at various levels.

Chemical Weapons

Chemical weapons are defined as “non-living, manufactured chemical agents combined with a dispersal mechanism that, when activated produce incapacitating, damaging or lethal effects on human beings, animals or plants.” These weapons are difficult to design and build; and non-state terrorist actors face technological challenges in building such weapons. However, intent to use chemical weapons by non-state actors is reportedly there.[7] There have been multiple chemical attacks by non-state actors - most notably the Tokyo Sarin gas attacks by Aum Shinrikyo in 1995. Analysis of an al-Qa’ida document recovered in Afghanistan indicated that the group had crude procedures for making mustard agents, sarin and VX.[8] Further, the Monterey WMD terrorism database states that from “1988-2004, 207 of the 316 CBRN incidents recorded involved chemical weapons.”[9]

The toxic component of a chemical weapon is thus “chemical agent”. Based on their mode of action (i.e., the route of penetration and their effects on the human body), chemical agents are commonly divided

into several categories: choking, blister, blood, nerve and incapacitating agents:[10]

- **Choking Agents**. These chemicals attack the lungs causing them to fill with fluid. Chlorine gas and phosgene are typical choking agents.
- **Blister Agents**. Blister agents also known as vesicants attack the skin of the victim resulting in blisters and skin burns. Mustard gas and Lewisite are common blister agents.
- **Blood Agents**. Blood agents attack the ability of the blood to hold and deliver oxygen. The victim suffocates. Cyanide gases and compounds are the most common types of these agents.
- **Nerve Agents**. Nerve agents attack the victim's nervous system. Most belong to the family of chemicals known as organophosphates. Many common pesticides belong to this family of chemicals such as parathion.
- **Incapacitating Agents**. These agents usually irritate the skin, mucous membranes, eyes, nose, lips and mouth. They may cause vomiting or intolerable pain. While they may lead to serious medical situations such as seizures or heart attacks, they are not designed to kill or cause permanent harm. When used alone, intention is to temporarily incapacitate or harass the individuals, or force them to evacuate the area. However, incapacitating agents may be used in combination with other agents to force responders to remove their gas masks and other protective gear, so that they will be exposed to lethal doses of the other agent. Examples are pepper spray, tear gas, riot control agents, etc.[11]

  A more detailed information on the Chemical Agents is given in Annexure 2.

Motivation, Capability and Consequences. The use of chemical weapons offers many advantages to terrorists: limited capacity of detecting such weapons, the relatively low cost required to develop them, their frightening image and psychological or shock effect on the

population and potential damage (under optimal conditions - i.e., type and quantity of agent, dispersion and weather).

Once a terrorist group has decided to use chemical weapons and obtained them, the final hurdle is in dissemination of the same at the target without causing harm to the user. Aum Shinrikyo was an unprecedented terror group - both in terms of the technological sophistication and the wealth at its disposal - and its Tokyo attack was culmination of an elaborate five-year effort to develop viable chemical and biological weapons capability. The cult had acquired enough of the chemical agent to kill more than a million people and a Russian-made helicopter with chemical sprayer. They recruited scientists from Japan's leading schools and abroad, spending millions of dollars exploring nuclear, biological and chemical agents. Yet the attack caused only 12 deaths - in one of the busiest cities of the world, that also during rush hours.[12] The failure to inflict mass-scale casualties is indicative of the enormous obstacles inherent in weaponizing and dispersing chemical agents over wide areas and affect large numbers of people. The attack underscored intelligence failures, the relative ease with which materials can be obtained and dangers of underestimating the imagination of terrorists.[13] However, considering the present trend of religiously motivated jihadi terrorists for whom their own life carries no meaning, dissemination at the target end is not a problem.

Biological Weapons

Biological weapons or Biological warfare agents comprise of disease-producing microorganisms (bacteria, viruses) and toxic biological products, to cause death or injury to humans, animals or plants. Basically, there are two types of biological weapons:

- **Pathogens**. These are disease-causing microorganisms, some of which can reproduce in a host over time and keep spreading long after the attack. The potential for many thousands of casualties is possible but the more likely number is much less because of the problem of efficiently delivering pathogenic agents to large numbers of people. Pathogens can be:

- Bacteria such as Anthrax, Plague, Q Fever and so on.
- Virus such as Smallpox.
- Fungi like Yeast and molds.
- Mycoplasmas that cause pneumonia and similar problems.
- Rickettsiae.

Plague, smallpox, anthrax, haemorrhagic fever, and rabbit fever are known to be probable biological weapons. Not all diseases are contagious and many have a low mortality rate when properly treated.[14]

- **Toxins.** Toxins are poisonous substances produced by living things. Many toxins are extremely lethal and small quantities can kill very large numbers of people. Some possible toxin weapons are:
- **Ricin.** A plant toxin that is 30 times more potent than the nerve agent VX by weight and is readily obtainable by extraction from common castor beans. There is no treatment for ricin poisoning after it has entered the bloodstream. Victims start to show symptoms within hours to days after exposure, depending on the dosage and route of administration. Terrorists have tried to deliver ricin in foods and as a contact poison, although no scientific data is there to indicate that ricin can penetrate intact skin.
- **Botulinum Toxin.** It is produced by the bacterium Clostridium botulinum, which occurs naturally in the soil. Symptoms usually occur 24 to 36 hours after exposure but onset of illness may take several days if the toxin is present in low doses. These include vomiting, abdominal pain, muscular weakness, and visual disturbance. Botulinum toxin would be effective in small-scale poisonings or aerosol attacks in enclosed spaces, such as movie theatres.
- **Anthrax.** Bacillus anthracis, the bacterium that causes anthrax, is capable of causing mass casualties. Symptoms

usually appear within one to six days after exposure and include fever, malaise, fatigue and shortness of breath. The disease is usually fatal unless antibiotic treatment is started within hours of inhaling anthrax spores; however, it is not contagious. Anthrax can be disseminated in an aerosol or used to contaminate food and water.[15]

Biological agents can also be characterized by other features, such as: Infectivity (capability to enter, survive and multiply in a host and may be expressed as the proportion of persons exposed to a given dose who become infected), Virulence (relative severity of the disease caused by a microorganism - different strains of the same microorganism may cause diseases of different severity), Lethality (ability of an agent to cause death in an infected population), Pathogenicity (capacity of a microorganism to cause disease, and is measured by the ratio of the number of clinical cases to the number of exposed persons), Incubation period (time between exposure to an infective agent and the first appearance of the signs and symptoms of disease), Contagiousness (number of secondary cases following exposure to a primary case), Mechanism of transmission and stability (ability of the agent to survive the influence of environmental factors such as air pollution, sunlight and extreme temperatures or humidity).[16] Biological agents of military significance, with important details are given in Annexure 3.

Motivation, Capability and Likelihood. The preference by a rogue regime or terrorist organization to choose biological weapons is due to: their extreme destructive potential being concentrated in a relatively small and difficult to trace package; with virtually no detectable sensor signature; due to agent's long incubation period the perpetrators might disappear before anyone could make out that an attack had been made; finally unlike ballistic missiles, biological agents lend themselves to clandestine dissemination.[17] Depending upon the dissemination conditions, biological weapons can be more destructive than chemical weapons, including nerve gas. A World Health Organization study indicated that 500 kg of anthrax powder, delivered by airplane over a city of 500,000 residents under favourable weather conditions, could produce 95,000 deaths.[18] When compared to the cost of a nuclear

weapons programme, biological weapons are extremely cheap. In one analysis, the comparative cost of civilian (unprotected) casualties is "$2,000 per square kilometre with conventional weapons, $800 with nuclear weapons, $600 with nerve gas weapons, and $1 with biological weapons".[19]

Cost is not much of an issue for advanced groups, since the equipment used to produce biological weapons is not unique, expensive or difficult to acquire. A well-stocked bioweapon facility can be built for as little as $2 million and according to experts simpler biological weapons can be produced for less than $1 million. This is not beyond the capacity of some terrorist groups. However, bringing together all the resources and creating the multidisciplinary team of technical personnel needed in various fields (biology, aerosolization physics etc.) to produce enough agents, stabilize, store, weaponize and ultimately disseminate them, is a formidable challenge. That is the main reason why non-state actors may find this capacity currently out of their reach. However, leakage from State Bio-warfare technologies cannot be ruled out. The Soviet Union had reportedly produced 20 tons of plague, the same amount of smallpox, and almost 100 tons of anthrax. The security of these biological materials and the production knowledge behind them is extremely questionable. Iran and Iraq were known to have recruited assistance for biological projects from Russia and former Soviet Union personnel were reportedly marketing their skills in Europe and North Korea might have smallpox samples.[20]

Radiological Weapons

Radiological weapons combine radioactive material with a means of dispersing it among a target population, resulting in the inhalation or ingestion of radioactive material.[21] Radiological weapons are often referred to as "dirty bombs" or "Radiation Dispersal Devices" (RDD) as they use conventional explosives to disperse radioactive materials to cause destruction, contamination, and injury from the radiation produced by the material. An RDD can be almost of any size, defined only by the amount of radioactive material and explosives. A variety of radioactive materials are commonly available and could be used in an RDD such

as Cesium-137, Strontium-90 and Cobalt-60. Hospitals, universities, factories, construction companies and laboratories are possible sources for these radioactive materials.[22]

There is no record of a dirty bomb attack. However in May 2002, the United States arrested an alleged al-Qa'ida terrorist for plotting to build and use a dirty bomb. Also according to a U.N. report, Iraq tested a one-ton radiological bomb in 1987 but gave up on the idea as the radiation levels generated were not deadly enough.[23] The know-how required for the construction of a dirty bomb is not more than the one needed to make a conventional bomb. For the non-state terrorists, the radiological weapons could be weapon of choice as they are easy to acquire, fabricate and transport.

The degree of damage caused by a dirty bomb greatly depends on the type and amount of radioactive and conventional explosive material in the bomb, the particles' size as well as factors such as wind, the size and number of buildings in the area attacked and the ballistics at detonation. In one particular scenario, people in the immediate vicinity would in all likelihood die from the force of the conventional explosion itself (including suicide-bomb attacks). Some survivors of the blast might die of radiation poisoning in the weeks afterward. Those farther away from the explosion may experience radiation sickness in the subsequent days and weeks, but with a fair chance of recovery. Overtime, cancer cases among the affected populace in the affected area would rise by up to 10 percent. Some experts opine that the explosion of a dirty bomb containing one kg of Plutonium in the centre of an average size metropolis, could ultimately lead to about 150 cases directly attributable to the blast.[24]

The potential of Dirty bomb lies more in causing mass disruption by dispersing radioactive material into the air, carried further away by the wind. The widespread panic over radioactivity and evacuation measures and the ensuing diagnosis of people, unknowingly coming in contact with the radioactive elements and consequently getting ill, could snarl a city and bring it to a virtual halt. Further, the area actually struck by the bomb may have to be kept off-limits for at least several months

during clean up efforts and the consequent monitoring, which can result in paralysis of local economy and reinforcing public fears of being closer to a radioactive area.[25]

Nuclear Weapons / Improvised Nuclear Device

The terrorists are unlikely to have access to a functional nuclear weapon in the near future. However, it needs to be remembered that suitcase-sized nuclear devices were reported missing from military storage areas in the former Soviet Union. This does create a possibility of these devices becoming available to terrorist organizations. Therefore, the possibility of terrorists attempting to transport and use nuclear devices cannot be totally ruled out.

Another likelihood is an Improvised Nuclear Device (IND), which is intended to cause a yield-producing nuclear explosion. An IND could consist of diverted nuclear weapon components, a modified nuclear weapon, or indigenous-designed device. INDs can be categorized into two types: Implosion and gun-assembled. Unlike RDDs that can be made with almost any radioactive material, INDs require fissile material - highly enriched Uranium or Plutonium - to produce nuclear yield.[26]

Conventional Weapons and Explosives

A conventional explosive device is the most preferred terrorist weapon. Some of these conventional weapons pack so much of explosive that can bring down large buildings. The casualties could be in the range of hundreds in these types of attacks. An example of this type of weapon was the fuel oil - fertilizer bomb used for attack on the Alfred P. Murrah Federal Building in Oklahoma City on 19 April 1995.[27]

First responders have to be alert to the potential for structural collapse as well as secondary explosive devices in the area. One needs to be extra-cautious if the explosion seems to have done little damage. A small explosive device might be used to disperse chemical, biological or even radioactive agents. Another objective of a small device might be to bring large numbers of first responders, who are then subjected to a large secondary device.

Older buildings may contain asbestos as insulation, pipe coverings, siding or as ceiling tiles. Any explosion or collapse may cause this asbestos to become airborne in hazardous levels. Beside the asbestos exposure, the primary inhalation threat will be of dust. Recently, terrorists utilized a new type of conventional weapon, the airplane i.e., in 9/11 attack on World Trade Towers in the United States. Quantities of residual, unburnt fuel may remain when an aircraft is used as the weapon of attack. In addition to the resultant fire hazard and blast effect, aviation gasoline and jet fuel are hazardous substances needing decontamination efforts.[28]

Future Employment of CBRNE Weapons

Many inferences can be drawn about the future employment of CBRNE weapons. Future developments in the field of science and technology, and materials will further enhance the threat of a CBRNE attack. In the area of Biotechnology and Biochemistry, tremendous advances in understanding and manipulating genes, cells and organisms are taking place and developments in the field of nanotechnology may revolutionize dispersal methods leading to an increased threat of attack. The increased availability of CBRN materials; potential to engineer materials from scratch; and a growth in the number of dual use materials and technology will pose major challenges to non-proliferation regimes. More importantly, there is reported to be a persistent intention on the part of non-state actors to acquire new types of CBRN capabilities and in some cases an explicit desire to use these capabilities. There is emerging opinion that in the 21st Century, CBRN materials may be utilized and deployed as weapons in innovative ways, both in battlefield as also in the civil domain, in times of war as well as during peacetime.

Implications of CBRNE Weapons for Operations

With the world wide availability of advanced military and commercial technologies and information (including dual-use), combined with commonly available transportation and delivery means, acquisition, development and employment of CBRN weapons by our adversaries cannot be ruled out. Operating in a CBRN environment will potentially impact the freedom of movement and the preservation of combat power.

Keeping in view the devastating consequences of CBRN hazards, measures should be planned, prepared, executed and assessed in order to enable forces to continue effective operations in a CBRN environment; as well as protect and mitigate the effects of CBRN hazards on military and nonmilitary personnel, equipment and infrastructure:

- The intelligence agencies are required to continuously collect, collate and analyze information about our adversaries' CBRN capabilities and intentions along with other potential sources of CBRN hazards.
- CBRN threat assessment will help commanders to make better-informed decisions about what type of protective measures to be adopted. It will also help identify the most likely CBRN threats and hazards that units and personnel will face, thereby enabling units to identify the protective and vulnerability reduction measures to keep them safe. It will enable logistics depots and echelons to maintain adequate stocks of CBRN-related equipment and provide these at the requisite locations.
- If forewarned, commanders can implement protective measures appropriate to all anticipated threats, including terrorist threats or other sources of CBRN hazards.
- There will also be a need for joint coordination amongst the three services and with the National Disaster Management Authority (NDMA) to enable a joint action plan to be executed when the civil areas get affected by CBRN hazards.
- Training at periodical intervals has to be carried out to practise: quick response to arrive at the scene of CBRN attack; initial action by first responders and their smooth relief by the expert teams; contamination mitigation techniques; casualty evacuation; emergency restoration and management of services; and assistance to civil authorities in maintaining law and order.

It may be remembered that operations will slow down as tasks are performed by personnel encumbered by protective equipment

or exposed to CBRN environments. Further, there may be a need to abandon or allow only limited use of contaminated areas, transfer missions to uncontaminated forces or avoidance of contaminated terrain and routes. In a theatre, it could also severely hamper the commanders' capabilities in terms of creation of reserves.[29]

Conclusion

With the instability around the world, and many governments unable to control within their borders, the CBRNE threat has become very real, irrespective of whether it is by states or non-state actors; or it is intentional or accidental. It is very difficult to appreciate their inter-se priority for selection by terrorist organizations or rogue states. However, statement given by Hillary Clinton, former Secretary of State, the United States at Biological and Toxin Weapons Convention Review Conference in December 2011 deserves a special mention:

"Advances in science and technology make it possible to both prevent and cure more diseases, but also easier for states and non-state actors to develop biological weapons. A crude, but effective, terrorist weapon can be made by using a small sample of any number of widely available pathogens, inexpensive equipment, and college-level chemistry and biology. Even as it becomes easier to develop these weapons, it remains extremely difficult….to detect them, because almost any biological research can serve dual purposes. The same equipment and technical knowledge used for legitimate research to save lives can also be used to manufacture deadly diseases."[30]

Thus a country has not only to strengthen its ability of detection and response mechanism but should also work in close coordination with international scientific community to maximise its efforts to fight the CBRNE terrorism.

Annexure 1

HISTORY OF CBRN WEAPONS USAGE

1500 – 1200 BC	First ever use of BW agents - Victims of plague were driven into enemy lands
1000 BC	Employment of chemicals as CW agents – when the Chinese used arsenical smokes
430 – 420 BC	By the application of noxious smoke and flame, the allies of Sparta took an Athenian-held fort in the Peloponnesian War.
184 BC	Hannibal catapulted jars filled with 'snakes of every kind' on to enemy ships.
256 AD	Poisoned smoke was introduced to break the line of Roman defenders.
1346 AD	Plague victims were catapulted over the walls of the besieged city of Caffa.
15th Century	Leonardo da Vinci proposed a powder of arsenic sulfide and verdigris.
1618–1648 AD	Toxic smoke projectiles were designed and used during the Thirty Years War.
1800 AD	French and Indian war blankets from smallpox victims were given to the Native Americans.
1853 – 1856 AD	During the Crimean War, the use of Cyanide-filled shells was proposed to break the siege of Sevastopol.
World War I	The modern chemical warfare agents first used in combat during WW I were 18th & 19th Century discoveries. Riot-control agents such as tear gas (lacrimators) were the first chemicals applied on a modern battlefield, later more toxic chemicals were introduced. The first great attack with CW agents – Ypres in Belgium: Chlorine attack by German troops in the afternoon of 22 April 1915 caused between 800 (realistic) and 5000 (mainly propaganda) deaths. On 12 July 1917, again near Ypres in Belgium, a new kind of CW agent Sulfur mustard was used by the Germans in an artillery attack. During WW I, Russians bore the heaviest burden of chemical casualties – nearly half a million (56000 fatal and 420000 non-fatal). German Army had developed anthrax, glanders, cholera and a wheat fungus specifically for use as a biological weapon.

03 Oct 1935	During the Italian – Ethiopian war, Italian troops dropped mustard bombs and sprayed it from airplane tanks. Mustard agent was selected as a "dusty agent" to burn the unprotected feet of the Ethiopians with devastating effects.
1936	An extremely toxic organophosphorus insecticide was discovered by German Chemist Schrader. The substance had devastating effects on the nervous system and was named **Tabun** (designated **GA,** for "German" agent "A" after WW II).
1938 - **World War II**	A similar agent**, Sarin (GB)** was discovered with toxicity five times higher than that of Tabun. Germans produced and weaponized approx 78000 tons of CW agents but CW agents were not widely used in WW II. The US produced approx 146000 tons of CW agents between 1940 & 1945.
1961 - 1975	Vietnam – chemical weapons used (agent Orange); suspected use of Tricothecene Mycotoxins ("Yellow rain").
1963 - 1967	Egypt in all probability used mustard and nerve agents in support of South Yemen against royalists troops in North Yemen.
1978	Bulgarian exile Georgi Markov assassinated in London using ricin.
1979	*Bacillus anthracis* accidentally released from a Soviet military research facility in Sverdlovsk (66 people believed to have been killed).
1980 - 88	Use of mustard gas and nerve gas in the Islamic Republic of Iran /Iraq War.
1994	Matsumoto, Japan. Terrorist group, Aum Shinrikyo, used nerve agent Sarin and improvised dissemination system (i.e., heater, fan, drip system) to attack an apartment building killing 7 and injuring 300.
1995	Tokyo, Japan. Aum Shinrikyo launched a coordinated attack on the subway using the nerve agent Sarin, in pierced bags, killing 12 people and causing 5,000 to seek care.
2001	Mailing of high quality preparation of Anthrax spores to politicians and media persons in the US.
2006	Former Russian Spy Alexander Litvinenko killed by ingestion of Polonium-210.

Source: Andre Richardt and Frank Sabath; and the Centre for Excellence in Emergency Preparedness,

Annexure 2

CHEMICAL AGENTS

Type	Sym-bol	Phys-ical State	Stability	LCT5O (mg – min/m3)	ICT5O (mg –min/ m3)	Detox Rate	Persist-ence	De-con
Nerve	**GA**	Liquid	Stable	▪ 400	▪ 300	Low	1 – 2 Days	DS2, STB / HTH, or Dilute Alkali
	GB	Liquid	Fairly Stable	▪ 70 – 100	▪ 35 – 75	Low	Like Water	
	GD	Liquid	< GA or GB	▪ 70	▪ 50 - 300	Low	1 – 2 Days	
	VX	Liquid	Stable	▪ 30 - 100	▪ 24 - 50	Low	Like Oil	
Blis-ter	**H/HD**	Liq-uid > 14.5^0 C	Stable	▪ 1500	• 150	Cu mul-ative	1 – 2 Days	DS2, STB or Fire
	HN - 1	Liquid	Fairly Stable	▪ 1500	• 200	Cu mul-ative	< HD	
	HN – 2	Liquid	Unstable	▪ 3000	• 100	Cu mul-ative	< HD	
	HN - 3	Liquid	Fairly Stable	▪ 1500	• 200	Cu mul-ative	> HD	
	HT	Liquid	Stable	▪ 1500	• 200	Cu mul-ative	> HD	
	L	Liquid > 0^0 C	Stable	▪ 1200 – 1500	• < 300	Cum ul-ative	< HD	DS2, STB, Cau stic Soda
	HL	Liquid	Fairly Stable	▪ 1500	• 200	Cu mul-ative	< HD	

	CX	Solid/ Liquid	Unstable	▪ 3200	• > 3	Cu mul- ative	Hours	Water
Blood	**AC**	Vapor or Liquid	Unstable	▪ 2000 – 4000	• Va ried	Rapid	Minutes	None Req uired
	CK		30 Days	▪ 11,000	• 7000			

- Respiratory (Breathing)
- Ocular (Eyes)

LCT5O = Lethal Exposure for 50% Population
ICT5O = Incapacitation Exposure for 50% Population

Source: Robert J. Heyer, “Introduction to CBRNE Terrorism”,p.10.

Annexure 3

BIOLOGICAL AGENTS OF MILITARY SIGNIFICANCE

Disease	Routes of Infection	Un- treated Mortality (%)	Incubation Period	Vaccine	Trans missi bility (Hu- man to Hu- man)
Bacteria and Rickettsia					
Anthrax (Bacillus anthracis)	S, R C, I	S: 5 – 20 R: 80 – 90	1 – 4 Days	Yes	No
Plague (Yersinia pestis)	V, R	60	2 – 3 Days	No	High
Q Fever (Cociella bumetti)	V, R	< 1	2 – 10 Days	IND	No

Tularemia (Rabbit Fever) (Francisella tularensis)	D, V, R	30 – 60	2 – 10 Days	IND	No

Viruses

Smallpox (Variola major)	R	30	10 -12 Days	Available (controlled US stock)	High
Viral equine encephalitis (e.g., Western, Eastern, Venezuelan)	R, V	< 1	2 – 6 Days	IND	Low
Viral hemorrhagic fevers (Ebola, Marburg, Lassa, Rift Valley, Dengue etc.)	DC, R, V	Up to 90 (virus dependent)	3 – 21 Days	No	Moderate

Toxins

Botulism (Botulinum neurotoxins	D, R	60	1 – 4 days	IND: (available only under FDA-approved protocol)	No
Ricin (Ricinus communis)	D, R	30	Hours to Days	No	No
Staphylococcal Enterotoxin B	D, R	< 1	Hours to Days	No	No
Trichothecene Mycotoxins	D, R, S	10 - 60	--	No	Yes (from skin contact)

Note: Cutaneous in this context refers to a break in the skin. A vector is any organism that carries and transmits an infectious pathogen.

Legend

C – cutaneous; FDA- Food and Drug Administration; R- respiratory system; D- Digestive system; I- Ingestion; S- Skin; DC - Direct Contact; ND- Investigational New Drug; V- Vector

Source: Appendix B , www.dtic.mil/doctrine/new-pubs/jp3_11.pdf

REFERENCES:

1. Andre Richardt and Frank Sabath, "A Glance Back - Myths and Facts about CBRN Incidents", pp.4-14., available at www.wiley-vch.de/books/sample/3527324135-c01.pdf (accessed on 22 December 2017).

2. "What is CBRN?", The Centre for Excellence in Emergency Preparedness, Ontario, p.1.,available at http://www.ceep.ca/education/CBRNintrosheet.pdf (accessed on 22 December 2017).

3. https://www.britannica.com/event/Bhopal-disaster (accessed on 22 December 2017).

4. Tanya Lewis, "Fukushima Radiation Leak: 5 Things You Should Know", Live Science, Planet Earth, 21 August 2013, available at https://www.livescience.com/39067-fukushima-radiation-5-things-to-know.html; and "Japan earthquake: Explosion at Fukushima nuclear plant", BBC News, 12 March 2011, available at www.bbc.com/news/world-asia-pacific-12720219 (accessed on 24 December 2017).

5. Ontario, op.cit., p.1.

6. Robert J. Heyer, "Introduction to CBRNE Terrorism" 10 January 2006, p.1., available at http://www.disasters.org/dera/library/Heyer%20WMD.pdf (accessed on 24 December 2017).

7. Andrea Mazzone, "The Use of CBRN Weapons by Non-State Terrorists", Global Security Studies, Fall 2013, Volume 4, Issue 4.,p.25., available at http://globalsecuritystudies.com/Mazzone%20CBRN-AG.pdf (accessed on 24 December 2017).

8. "Terrorist CBRN: Materials and Effects", Central Intelligence Agency Library, available at https://www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm (accessed on 24 December 2017).

9. Andrea Mazzone, op.cit., p.25.

10. http://www.opcw.org/about-chemical-weapons/types-of-chemical-agent/ (accessed on 26 December 2017).

11. Robert J. Heyer, op.cit., p.3.

12. Yaron Schwartz and Ophir Falk / Multiple Authors, "Chemical Biological Radiological Nuclear Terrorism: Assessing the Threat", International Institute for Counter-Terrorism (ICT), 15 May 2003, available at https://www.ict.org.il/Article/873/CBRN-Terrorism-Assessing-the-Threat#gsc.tab=0 (accessed on 26 December 2017).

13. Ibid.

14. Robert J. Heyer, op.cit., p.4.

15. Central Intelligence Agency Library, op.cit.

16. Ontario, op.cit., pp.2-3.

17. Yaron Schwartz and Ophir Falk / Multiple Authors, op.cit.,

18. Ibid.

19. "Biological Weapons", Reaching Critical Will, available at http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/4579-biological-weapons (accessed on 26 December 2017).

20. Yaron Schwartz and Ophir Falk / Multiple Authors, op.cit., [For knowing the detailed capabilities of Former Soviet Union's Biological weapons read "Biological Weapons in the Former Soviet Union: An Interview with Dr. Kenneth Alibek" conducted by Jonathan B.Tucker, The Nonproliferation Review/Spring-Summer 1999 available on https://www.nonproliferation.org/wp-content/uploads/npr/alibek63.pdf (accessed on 30 December 2017).

21. Andrea Mazzone, op.cit., p.26.

22. "CBRN defense", Science Direct, available at https://www.sciencedirect.com/topics/medicine-and-dentistry/cbrn-defense (accessed on 30 December 2017).

23. Yaron Schwartz and Ophir Falk / Multiple Authors, op.cit.

24. Scientific American, November 2002 and www.fas.org ('Radiological Bomb' features) as cited in Ibid., n.13.

25. Yaron Schwartz and Ophir Falk / Multiple Authors, op.cit.

26. Central Intelligence Agency Library, op.cit.

27. Lydia Smith, "Oklahoma City bombing 20th anniversary: 20 facts about the 1995 attack", International Business Times, 18 April 2015 available at http://www.ibtimes.co.uk/oklahoma-city-bombing-anniversary-20-facts-about-1995-attack-1497033 (accessed on 30 December 2017).

28. Robert J. Heyer, op.cit., p.2.

29. To study the details about 'Fundamentals, and Planning, Preparation and Execution of Operations in CBRN Environments see www.dic.mil/doctrine/new-pubs/jp3_11.pdf (accessed on 17 November 2017).

30. Clinton, Hillary Rodham, "Remarks at the 7th Biological and Toxin Weapons Convention Review Conference", Palais des Nations, Geneva, Switzerland, 07 December 2011, as cited in Andrea Mazzone, op.cit., p.27.

***Brig (Dr.) Rajeev Bhutani (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi

RELEVANCE OF INDIA-SINGAPORE NAVAL AGREEMENT FOR ADDRESSING FUTURE SECURITY CHALLENGES OF INDIA

Vice Adm Pradeep Kaushiva* UYSM, VSM (Retd)*

Introduction

The Armed Forces are instruments of state which, barring a few exceptions such as in Pakistan, do not have an independent identity or agenda but are integral to and follow the state objectives, interests and pursuits. They do so, in close coordination with other instruments of the state, either in a coercive mode or through mutually beneficial collaboration. Indian Navy (IN) and Republic of Singapore Navy (RSN) present a shining example of the latter wherein their close professional relationship systematically built up since the early 1990s has greatly supported and facilitated the two nations' diplomatic endeavours. Starting with antisubmarine training exercises for RSN by IN units, Singapore has now become India's most comprehensive security partner.[1]

The emergent bipolar world order after Second World War, heard from a newly independent India the concept of non alignment which soon grew into a full fledged Non Alignment Movement. Even though India did tweak her non-aligned status somewhat through the Indo-Soviet Treaty of Peace, Friendship and Co-operation in response to the 1971 developments in Pakistan, she largely managed to maintain her strategic autonomy. Rise of China as a reckonable power, her quest to unilaterally change the status quo and her aggressively revisionist posturing at all international platforms have lately forced India to progressively adjust her sails to the shifting geo-strategic fulcrum.

To posit the relevance of the India-Singapore naval agreement in the context of India's security concerns, however, it would be necessary to first briefly recapitulate the maritime security challenges and then review India's maritime engagements.

Maritime Security Challenges

The Indian Ocean (IO) contains an estimated forty percent of world's offshore oil production and hosts half of the world's containerized cargo, one third of its bulk cargo and two third of its oil shipment.[2] The ensuing trade and energy flows bring further complexity to this sea space whose littoral states co-exist in extreme diversity due to their vastly different levels of development; differing governance structures & procedures; complex population mix of ethnicities, cultures and languages.

Stake holders in the region are not only the littorals but also resident as well as visiting powers and many distant located others, drivers of whose economies ply the sea lanes crisscrossing the IO.

Maritime Stability

History has it that the IO region has had only one maritime hegemon at a time - US for the last 50 years and UK for the 150 years preceding that. As the region has also not witnessed any major period of maritime instability, no regional platform for maritime security dialogue has evolved.

Responding to the eastward shift of geostrategic centre of gravity, in 2011 the US unveiled plans to 'rebalance' through broadening areas of cooperation with regional states and institutions, strengthen areas of cooperation with allies and partners, engage with China and others, to develop regional norms & rules to support international security and economic order compatible with the global interests of the US. The manoeuvre, subsequently renamed 'pivot to the east,' had the military dimension at its core with reconstitution of the force structure, relocation of military capacities from other theatres and restructuring regional

security arrangements. But all this suddenly lost momentum last year with the change of tenancy at White House.[3]

The China Factor

Funded by nearly double digit growth averaged for close to three decades and powered by military & other technologies acquired from the west through purchase, transfer, theft and stealth; by the dawn of twenty first century China was poised to claim her place under the sun not only in the regional context but on the global scene as well. Enabled by absolute state control under a totalitarian regime since the Communist takeover in 1949, China's power accretion has been systematic and purposeful. Even as it sought to catch up on technology, initially facilitated and enabled by the US itself, China first sought to acquire asymmetric capability to challenge the lone superpower even as it strove to develop its own versions of matching capability.

For the first time in nearly six hundred years Chinese warships deployed beyond the second island chain and then within a decade PLA Navy (PLAN) ships were on sustained out of area deployments. After initial experimentation with infrastructure development assistance to Indian Ocean states, in 2013 China unveiled a nearly trillion dollar initiative called One Belt, One Road or the Belt and Road Initiative (BRI). This international infrastructure development programme seeks to link up global markets, raw material sources and industries through economic corridors, roadways, railways, seaports, hinterland infrastructure, power generation, industrial parks and their interconnects; covering 68 countries across three continents accounting for nearly 40% of the global GDP. The BRI has subsumed in its ambit the earlier maritime infrastructure programmes at various stage of implementation, and at revised estimated cost of US $ 62 billion the China-Pakistan Economic Corridor (CPEC) is its flagship programme.[4]

CPEC is a collective of multimodal overland connectivity from Kashgar in Xinjiang Province of western China, through Pakistan Occupied Kashmir and Indian territory illegally ceded to China by Pakistan, accessing the Arabian Sea via Gwadar port in Balochistan.

Pakistan has forsaken its own sovereignty to help China establish a much shorter route to the Persian Gulf and beyond to the west. China has already established a significant military presence in Pakistan and is all set to acquire a naval base in Gwadar.

On 01 Aug 2017 China formally opened its first overseas military base in Djibouti[5] for logistics support to the PLAN deployments and formally took over Hambantota port in Sri Lanka on a 99 year lease.[6] The Sri Lanka government assurance that the port will not be used for military purpose is just that – an assurance.

The above Chinese build up in the IO is predicated on the premise that capabilities take long to build but once they are built, the intention whether/ when/ how to use those capabilities can be changed at short notice. The flip side however is that, the IO bases notwithstanding, augmentation of PLAN deployments will still need to negotiate the vulnerabilities at western egress from the South China Sea.

Other Players

After dissolution of Soviet Union, the Russian Federation took time to stabilise politically, integrate internally, quell rebellions and separatist movements such as Chechens', bring influential oligarchs to order and consolidate economically through the financial and oil price crises. Since 2014, Russia is stable and back on the international scene to play its assumed roles in Ukraine, Syria, Afghanistan and now in Pakistan even as it plays footsie with Turkey and Egypt. Concurrent with the deteriorating US-Iran relations, Russia found a useful friend in the latter just as, after their border disputes resolution, it made common cause with China. After regaining her place at the global high table, albeit neither as the chair nor as co-chair, Russia now appears getting set to manage the US led alliances westwards and leave China to do so into the Pacific.

Meanwhile the EU, NATO and coalitions of the willing; mobilised to counter piracy, are still deployed in north-western access to the Indian Ocean. Being China's lackey, Pakistan is not being commented upon separately as a relevant player.

In this geostrategic line up, it is China's foray through south-east Asia & south Asia into the IO that is generating turbulence and a dangerously growing potential for grey hull friction. Since no nation can meet geostrategic challenges to its interests alone, the obvious option for India is to join a coalition of partners whose geostrategic imperatives correspond with her own. But a military alliance requires some autonomy to be forsaken to protect the larger shared interests. India has succeeded so far in assiduously maintaining strategic autonomy, and even today does not plan to enter into any Indo-Pacific alliance with the US.[7] This is praiseworthy, but it would be prudent to have a sequence of alternative options ready to be played out at short notice should future contingencies so commend.

Non-Traditional Maritime Security Challenges

In the recent times, sea piracy and terrorism have emerged as the most dangerous of all non-traditional security challenges.[8] Terrorists invariably penetrate and strike through the gaps created by corrupt practices, inadequate law enforcement, scanty surveillance, lax security or a combination of such factors. The second in hierarchical order of threats would be human trafficking, gun running and drug smuggling. These are invariably undertaken by organised crime syndicates which take advantage of human frailties. Further down the order are instances of illegal, unregulated and unreported fishing. These adversely impact the food supply to, and livelihood of, local communities. Climate change invariably features close to bottom rung of the non traditional maritime security challenges but holds out the most devastating portends for future of the mankind. IO littorals are located in one of the most disaster prone areas on this earth. Humanitarian Assistance and Disaster Relief activity innately transcends the barriers of national interests, political persuasions, strategic alignments et al.

The absence of a regional framework for maritime security dialogue is felt more acutely in the context of non traditional challenges because these are common to all and can best be met collaboratively.

India's Maritime Engagements

Indian Navy has historically maintained service to service contacts with friendly foreign navies through port calls, familiarisation visits, bilateral interactions, training exchanges, operational exercises and technical support arrangements. The first initiative for a comprehensive defence relationship between India and the United States came in 1991 through Kicklighter Proposals for consultative mechanisms, strategic dialogue, training and other exchanges, and visits at both senior and staff levels.[9]

Navy-Navy Relations

Malabar series of bilateral annual exercises between IN and US Navy flowed directly out of the Kicklighter proposals. Starting on a modest scale with basic manoeuvres and communication drills, the exercises progressively increased in content and complexity to include fleet air defence, antisubmarine warfare, simulated interdiction, amphibious operations etc. A blip caused by India's nuclear tests in 1998, was ironed out after India joined President Bush's war on terror post 9/11. The Malabar exercises have not looked back since and have grown to include Japan as well. The 21st edition of Malabar exercises in 2017 saw participation of 16 ships including USN nuclear powered carrier Nimitz, IN carrier Vikramaditya, Japanese helicopter carrier Izumo, two submarines and 95 aircraft.

IN also engages with the Russian Navy for exercise Indra, British Navy for Konkan, French Navy for Varuna, Singapore Navy for Simbex, Australian Navy for Ausindex, Sri Lanka Navy for Slinex, Royal Omani Navy for Naseem-al-Bahr series of bilateral exercises in addition to a host of multilateral exercises such as RIMPAC, KAKADU, IBSAMAR, ADMM+, ARF DIRex, KOMODO and co-ordinated patrols with Indonesia, Myanmar, Thailand. Put together, IN has participated in about twenty exercises with friendly foreign navies during 2017.

As IN force levels grew, from a little over 30 coastal ships at the time of independence to multi dimensional, multi spectrum, networked force of 139 ships & submarines and 224 aircraft today, so did the operational deployments and structured interactions. "We have

maintained continuous presence off the Horn of Africa for anti piracy operations since October 2008. In addition, regular deployments of ships and aircraft is being maintained in the North Arabian Sea, Gulf of Oman, Persian Gulf, the Andaman Sea and the approaches to straits of Malacca, Lombok and Sunda. In addition we also undertook joint EEZ patrols of Maldives, Seychelles and Mauritius as well as co-ordinated patrols with Myanmar, Thailand and Indonesia."[10]

India-Singapore Naval Agreement

India was one of the first countries to recognize Singapore in 1965. Following India's economic reforms in 1990s and the Look East Policy, Singapore greatly facilitated India's elevation as ASEAN's Full Dialogue Partner in 1995 and inclusion in the ASEAN Regional Forum in 1996 after initial rejection in 1993.[11] In 2003, India and Singapore signed a bilateral agreement to expand military cooperation, joint military training and developing military technology. Increasing trade, investments and economic cooperation between the two countries provided the impetus to create a new framework for cooperation, which was included in the Comprehensive Economic Cooperation Agreement (CECA) of 2005. This robust relationship was elevated to a Strategic Partnership during the visit of Prime Minister Modi in November 2015 when he signed a Joint Declaration on a Strategic Partnership with Singapore Prime Minister Lee Hsien Loong on the occasion of the 50th anniversary of the establishment of diplomatic relations.[12] The India Singapore Bilateral Agreement on Navy Cooperation signed on 29 Nov 2017 (the Agreement) is thus the logical next step in evolving relationship between the two countries. It is also a part of the other linkages being explored for recalibration by India in furtherance of her strategic interests.

Parallely, IN-RSN relationship has been steadily building up since 1994 when the former started facilitating antisubmarine warfare training to the latter's then newly acquired A/S corvettes. As successive exercises were held in waters off Andaman Islands, east coast of India and Lakshadweep islands; RSN learnt valuable lessons in logistics support and maintenance of relatively small units' out of area

deployments for extended periods. Likewise, based on IN's experiences, useful interactions were arranged when RSN went on to train their submarine crew and then acquire their own boats. With enhancing comfort levels, the scope of cooperation progressively extended. The author recalls that certain urgent operational requirements were cleared by the original equipment manufacturer for import by us at the height of Kargil war, after being diverted from Singapore's order. This exemplifies the scope, width and depth of India-Singapore defence relationship.

Conclusion

The wide ranging bilateral and multilateral engagements of IN have evolved from service initiatives. The Government of India fully backed these but did not publicly enunciate a strategy to pursue. Two recent articulations, appended below, have now bridged this gap and become the policy direction for IN's professional endeavours, engagements and projections.

"...A peaceful and stable maritime environment is critical for the regional and global security. It is also a must to harvest the riches of the oceanic ecosystems. Given the complexity of modern day challenges, the international maritime stability cannot be the preserve of a single nation. It has to be a shared goal and responsibility of all the seafaring nations. To this end, the navies and maritime agencies of the world need to work together and engineer virtuous cycles of cooperation." [13]

"Indian Navy has been mandated to be the net security provider to island nations in the Indian Ocean Region. We would like to assure our maritime neighbours about our unstinted support for their security and economic prosperity."[14]

The India Singapore naval agreement formalises the already cemented relationship between the two navies as indeed between the two nations. It provides for increased cooperation in maritime security, joint exercises, exercise and patrols in each other's waters, visits to each other's naval facilities and mutual logistics support.[15] In nomenclature, none of this is new as many of these were already being undertaken

albeit via full diplomatic procedure route for each, every time. What is new, therefore, is that the above activities and more are now already pre-approved with procedures cleared. So, in practice, much easier routes to a much wider scope in much shorter timelines will follow. The Agreement, thus, is a vital instrument which will enable IN deliver upon its assigned tasks in the South China Sea, its western approaches and to the east of it.

It is, however, important to clarify that this agreement is not a treaty or an alliance which may bind both sides to tactically come to each other's aid under predetermined circumstances. It is, however, a great facilitator for enabling and sustaining IN's prolonged deployments eastwards far from home waters for exercises, routine presence or for maritime security operations. And, it will provide the necessary familiarisation and interoperability for IN and RSN to act, if not in unison, at least in close coordination for mutual support in meeting the future maritime security challenges.

The Agreement can also be used as a template for India to explore building similar bridges of friendship with other powers in the region such as Indonesia. This would provide the necessary operational flexibility to effectively meet the contingencies which may arise in future.

ENDNOTES

1 Look East, Cross Black Waters: India's Interest in Southeast Asia by Jonah Blank, Jennifer D. P. Moroney, Angel Rabasa, Bonny accessed at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1021/RAND_RR1021.pdf on 18 Dec 2017

2 Nazery Khalid, the Role of the Indian Ocean in Facilitating Global Maritime Trade accessed at http://tamilnation.co/intframe/indian_ocean/050628indian_ocean.pdf on 18 Dec 2017.

3 Vice Adm Pradeep Kaushiva, A Regional Maritime Snapshot in the Chanakya Journal December 2016, Vol 1 Issue 2

4 Vice Adm Pradeep Kaushiva, China Pakistan Economic Corridor in the Chanakya Journal Jun 2017 Vol 1 Issue 4

5 Reuters Staff in World News dated 01 Aug 2017 accessed at https://www.reuters.com/article/us-china-djibouti/china-formally-opens-first-overseas-military-base-in-djibouti-idUSKBN1AH3E3 on 19 Dec 2017

6 The Diplomat dated 11 Dec 2017 accessed at https://thediplomat.com/2017/12/sri-lanka-formally-hands-over-hambantota-port-to-chinese-firms-on-99-year-lease/ on 19 Dec 2017

7 Nilova Roy Chaudhury, From Asia Pacific to Indo Pacific in India Strategic Vol 12 Issue 11 November 2017 Page 9

8 Aditi Chatterjee, Non-Traditional Maritime Security Threats in the Indian Ocean in NMF Scholars' Round Table Conference Report dated 18 Jun 2014 accessed at http://www.maritimeindia.org/pdf/Aditi%20rtc%20report,%20final.pdf on 19 Dec 2017

9 Teresita c Schaffer, India and the United States in the 21st Centur y: Reinventing Partnership page 74 accessed at https:// books.google.co.in books?id = V7A03 x O9NeIC&pg=PA74&lpg= PA74&dq=kicklighter+proposals&source=bl&ots=PqJzvUuDnH&sig=xTWPygiN34W7jkHVwtMkWhv57Vg&hl=en&sa=X&ved=0ahUKEwjdp-fim5nYAhWBgI8KHVCJC9QQ6AEITDAG#v=onepage&q=kicklighter%20proposals&f=false on 21 Dec 2017

10 Adm Sunil Lanba, Chief of the Naval Staff during Navy Day media interaction as reported in Indian Military Review Vol 8 No. 12 December 2017

11 David Brewster in India as an Asia Pacific Power, page 107 accessed at https://books.google.co.in/books?id=1RGpAgAAQBAJ&pg=PA107&lpg=PA107&dq=singapore+support+for+india+at+asean+and+arf&source=bl&ots=iXqng81f-B&sig=KTHH26U8ChiMhDYappXXbm3rWm8&hl=en&sa=X&ved=0ahUKEwiWjrr3mZvYAhXIwI8KHXs3B8AQ6AEIWDAI#

v=onepage&q=singapore%20support%20for%20india%20at%20asean%20and%20arf&f =false on 21 Dec 2017

12 High Commission of India in Singapore website https://www.hcisingapore.gov.in/pages.php?id=68 accessed on 18 Dec 2017

13 Prime Minister Narendra Modi addressing the International Fleet Review at Visakhapatnam on 07 Feb 2016 accessed at http://pib.nic.in/newsite/PrintRelease.aspx?relid=136182 on 19 Dec 2017

14 Former Defence Minister AK Anthony addressing the Naval Commanders' Conference 12 Oct 2011 accessed at http://pib.nic.in/newsite/PrintRelease.aspx?relid=76590 on 19 Dec 2017

15 Singapore Defence Minister Ng Eng Hen as quoted in Navy Gets Access to Singapore's Changi Base, Indian Military Review Vol 8 number 12 December 2017, page 14

***Vice Adm Pradeep Kaushiva UYSM, VSM (Retd)** is a Former Commandant National Defence College, New Delhi

DEMOGRAPHIC DIVIDEND –INDIA'S SILENT SECURITY CHALLENGE FOR FUTURE

Brig Navjot Singh*

Introduction

India's security perspectives would inevitably be governed by the interplay of its domestic imperatives, regional balance of forces and the global challenges which impinge on its role and capabilities [1]. India unlike any other nation of the world, faces unique security challenges from many quarters. Besides the obvious threat from China and Pakistan (both nuclear weapon states), India faces a future where security challenges will be less predictable. Some of these threats may be known, but the enemy would be invisible. Before proceeding further, a de-novo look at what defines security.

Defining Security

The traditional view of security focussed on the application of force at the state level and was therefore a fairly narrow view, hinging on military security [2]. However in the backdrop of China having coined the phrase " Comprehensive National power " or CNP, here is a need to revisiting the concept of security. World over also it has now been widely acknowledged that there is more to security than purely military factors.

Threats to a nation emanate both from external aggression and from internal discord. At times internal factors can erode national security more critically than any external danger. A modern day definition of security and National power based on political stability, societal cohesion and economic development, environmental, social and human among other factors that impact the concept of security would thus remain central to the future of India's national security.

Keeping in tune with Maslow's hierarchy of social needs, the concern for security of the 'human being' has resulted in the development of the concept of 'human security', which focuses on the individual. Therefore, the definition of security is definitely broad – and is related to the ability of the state to perform the function of protecting the well-being of its people. This formulation harks back to the days of Chanakya and Arthashastra.

The subject of National Security is immense in its scope and expanse and it would be unwise to even attempt a complete treatment of all issues involved. Therefore, certain key aspects of national security and few known security challenges would be listed out and discussed briefly but one key factor that indirectly impacts India's National Security, would be dwelt upon in detail.

Known Security Challenges

Domination of cyberspace, control of space & Autonomous Weapon Domain are major future threats and challenges to national security. Internal security challenges, Economic warfare and Non-traditional challenges like water, food, energy security and climate change are also few threats that are well known and would have been factored in by various scholars and these need to be studied and analysed in detail. Few of these challenges have been discussed briefly in subsequent paragraphs.

Cyber Warfare and Web Espionage. International cyber espionage is set to be a major threat to national security in the years to come. Primary targets will include critical national infrastructure network systems with electricity, air traffic control, financial markets and Government computer networks taking centre-stage. Reports suggest that few nations have acquired considerable capability in this domain. The Indian Armed Forces are increasingly investing in networked operations, both singly and a joint fashion. India as a nation and the Indian Armed Forces in particular cannot, therefore, afford to be vulnerable to cyber attacks.

Border & Other China & Regional Specific Challenges. The resolution of the border problems, autonomy of Tibet, the China-Pakistan connection, competition for strategic space in the Indian Ocean and management of

water resources would be few of the prime causative factors for any potential tension with China and our diplomatic focus on these issues would have to be maintained [2]. Regional peace and stability is another important issue on India's strategic horizon. The domestic environment in South Asia continues to remain generally characterised by political unrest and regime instability. Proliferation of small arms and drugs in the region is yet another disturbing dimension of cross-border terrorism [3]. Due to its strategic location between two major narcotics producing areas, India may become a transit route for the narcotics trade,

J&K, North East & Punjab. Due to increased awareness of the people regarding the nefarious designs of the terrorists and their handlers the situation in Kashmir has improved. The tiredness of the locals with economic slowdown, has also contributed to the improved situation but it however still remains a cause for concern. The process of rebuilding the economic and political fabric in the state and winning over the confidence of its people needs to be ensured. The appointment of an interlocutor by the government is a right step in this direction. The problem of insurgency in Tripura, Manipur and Nagaland continues despite an uneasy truce. Assam also faces sporadic instances of volatile agitation on the influx of foreign nationals. Punjab is now facing a unique challenge in form of a large percentage of its youth taking either to drugs or migrating to greener pastures abroad.

As stated earlier, these key aspects of national security and few known security challenges listed above have merely been discussed briefly but these would need to be discussed in detail by various scholars. However one key factor that indirectly impacts India's National Security, has been discussed in detail in subsequent paragraphs.

India's Demographic Dividend

Vicious Quartet. Four decades ago in school we used to study about the problems that plagued the Indian nation and the quartet of illiteracy, un-employment, poverty and over population always figured up. It used to be explained to us that these four evils were all interlinked with one another and it was a herculean challenge to break this vicious

quartet which was holding back India from finding its rightful place in the world order. Few wise teachers used to say that out of these four, over population was actually the main culprit and if somehow we could find a way to control our population, rest of the things would follow.

Half a century ago, in a 1967 book titled Famine 1975, America's Decision: Who Will Survive?, U.S. economists William and Paul Paddock even advocated that the population of India should be allowed to starve as the country was a hopeless case. The authors had argued that America should allocate its aid dollars to other countries with greater chances of being able to feed their hungry [4]. 18 years ago, with the birth of Aastha Arora on 10 May 2000 India's population officially crossed one billion. At that time also our population was still considered a liability by many at that time and providing basic needs for all seemed to be a near-impossible task.

Silver Lining in the Cloud. However two years later, in 2012, it appeared that this "cloud also had a proverbial silver lining". The world was aging, but India was growing younger. According to the IMF, studies showed that "in many Asian countries, aging populations are now causing, or are about to cause, a decline in the working-age ratio. The Japanese workforce has been shrinking since 1995, and the Korean workforce will start to decline beginning 2015. China's working-age ratio peaked in 2013 and then will decline by a substantial amount in the next few decades. The second most populous country in the region (and in the world) can afford grounds for cautious optimism" [5]. India's demographic transition is presently well underway, and the age structure of the population is likely to evolve favourably over the next two to three decades." Logically it implies that because most citizens are working, economic growth goes up which is popularly referred to as demographic dividend. This dividend could add two percentage points to per capita GDP growth per annum.

However in order to encash upon and ultimately exploit these seemingly favourable demographics, there are some challenges related to it. The first and the most obvious one is in finding jobs for all these people. Secondly, India's youth need to develop the right skills for the

modern job market. The National Association of Software and Services Companies (NASSCOM) has published a study saying that only 25% of information technology (IT) graduates are employable [6]. However according to the All-India Council for Technical Education (AICTE), the government's accreditation agency, every year, one million engineering graduates and diploma holders are added to the workforce. As per the erstwhile AICTE chairman Mr S.S. Mantha, if the number of unemployed engineers was anywhere near what NASSCOM had claimed, "there would be civil war". This is exactly the ticking time bomb that the government is grappling with and trying to defuse. It is for this reason that the National Skill Development Mission of India has been accorded due importance by the Hon'ble PM of India. The National Skill Development Mission was approved by the Union Cabinet on 01.07.2015, and officially launched by the Hon'ble Prime Minister on 15.07.2015 on the occasion of World Youth Skills Day. The Mission has been developed to create convergence across sectors and States in terms of skill training activities.

Boon or Bane. India will soon be one of the few countries in the world with a working age population that is more than its number of retirees. To quote Mr Ramadorai, Vice-Chairman of Tata Consultancy Services (TCS) and an advisor to the Prime Minister for the National Council of Skill Development NCSD), "By 2020, the average Indian will be only 29 years of age, compared with 37 in China and the U.S., 45 in Western Europe, and 48 in Japan. That means India will experience an age advantage for at least three decades, through 2040. There is thus an unprecedented opportunity for India provided Indians skill themselves to suit the future demand for jobs both domestic and abroad.

If India can make employment and skill level a priority, India could soon be exporting skilled labour to the world (and not just limiting it to the Gulf and Middle East, as is presently being done), thus filling up the gaps in the world's manpower shortage and become the resource pool of the world. This would in turn generate flows of FOREX back to India and provide gainful employment to the Indian youth. However naysayers strike a note of caution and worry about a generation of unskilled Indian workers left behind if they are not properly skilled. Thus getting India's labour pool ready for export (or for that matter for gainful employment

within the country) will be a complex human resources exercise, which will have major ramifications for not only India but for the whole world.

Way Ahead- Skill Development and Job Creation. If India wishes to harness its demographic dividend, then it is imperative to developing its immense human capital in the coming decade. To give an impetus to manufacturing and make it a genuine engine of growth, the government announced new policies as part of the 12th five-year plan (2012-2017) that aim to create approximately 100 million opportunities for jobs/work by 2022 ; many of these would be in labour-intensive manufacturing sectors such as textiles, gems and footwear. Education is the key to employment and skill development and the government is also working to expand access to education and vocational training for workers in the countryside, including new rural broadband networks that will connect remote areas with educational opportunities.

Technology as an Enabler for Skill Development. Technology is going to play a very critical role in connecting the privileged sections of society and those that till date were deprived from quality education due to lack of access to knowledge resource i.e. the haves and the have-nots. With the right skills and training, workers from India can prosper at home and abroad. As per the statistics given by the United Nations, the working-age population is likely to increase by about 600 million globally in the next decade. Though there is likely to be a decline in the availability of working-age population in developing countries by almost 17 million, yet the global economy as a whole is expected to experience a skilled manpower shortage of 56 million by 2020. Thus by properly leveraging technology, we can make access to online skill development courses and certifications within easy reach of every Indian with a feature phone in his hand and a burning desire in his heart to improve himself/ herself.

Skilled vs Unskilled Labour. During the beginning of the century, while all of East Asia, even China, in the early phases developed using low-skilled, abundant labour, India developed primarily based on skilled services rather than using our abundant pool of unskilled labour [7]. India will be unable to build a manufacturing sector for unskilled labour, as much of manufacturing today is already shifting toward robots,

automation and machines. As the future does not seem to be unskilled-labour intensive, India thus needs to upgrade workers' skills so that as the economy demands more skilled labour, there will be a supply of people to fill those positions. Thus there is an urgent requirement of collaboration between the private sector, primarily backed up by the public sector to meet this challenge to supply the kind of skills in the quantities that the nation needs to progress. Failure to do this will result in a major problem.

The Lurking Danger Ahead. In three years, India will have the world's largest population of working people, about 87 crore in all. Though India had seen high growth after 1991, less than half the population was fully employed. A limited capacity to generate employment is a serious challenge, given the continued expansion of the workforce in India over the next 35 years. [8]. There is also realisation that a very large labour force is moving into an environment which does not have the ability to absorb them. The expectation and anticipation of reaping the benefits of the demographic dividend could easily turn into a grim reapers harvest if challenges are not overcome.

Low End Manufacturing & Slow Down. Traditionally countries have become developed through low-end manufacturing, like garment exports, and then migrating to higher-end work like automobiles, IT and electronics. Though India has all these sectors yet loses out on economies of scale. Bangladesh, Vietnam and Sri Lanka are more efficient and cheaper as regards garments industry. In addition the slowing down of the global economy in last eight years has decreased any external demand of large size that we could capitalise on.

Automation & Competition. Another reason is a lack of qualified manpower as the vast majority of Indians have no access to this education resource and are therefore not equipped to work in the modern economy. At a time when automation is reducing the total number of new jobs every year, countries like the Philippines are eating into India's back-end services jobs.

Unemployment, Unrest & LWE

It is really a challenge to see how India will be able to reap the benefits of a demographic dividend. The youth are looking forward to the dream of a developed nation and have come forward to exercise their mandate and be the prime movers of change. However this unbridled energy of the teeming youth of India needs to be properly and gainfully channelized and soon. The proponents of Left Wing Extremism (LWE) have been trying in vain to establish a "Red Corridor" in India but their efforts have not borne fruit. They merely hold sway over limited parts of the tribal areas, but by and large the youth and the students/ educated intelligentsia (barring a few exceptions) have not lent support to this cause. However god forbidding should India fail to properly utilise the demographic dividend, a period of mass unemployment and social unrest will loom large on the horizon.

The problem then will not be confined to tribal or under-developed areas but would spread to villages, towns, cities and even in metros. This will present a golden opportunity to the proponents of LWE and their ranks will swell and the nation will have a major security problem on its hands. Unless there is a major shift in policies and environment, both internal i.e. within India and external i.e. at the international fora, (which at the moment seems distant), India has a major task in optimally utilising this opportunity and letting it slip from being an opportunity to a challenge. However the changing strategic landscape around India calls for identification of current and future security challenges in totality so that proactive stance can be adopted by the policy makers for countering them.

Conclusion

Erstwhile Union Minister Mr Sarbananda Sonowal had rightly said that the challenge before the country is to empower its huge youth population to bring about transformational changes to ensure progress, prosperity and peace [9]. This would involve providing the right education, the necessary skills to make them employable, developing them as entrepreneurs, making them healthy individuals, and inculcating the right social and moral values. The Government of India currently invests

approximately Rs. 2,710 per young individual per year. However, there is a need for a more focused effort to empower the youth to achieve their potential.

The Hon'ble Prime Minister of India has also recognised the problem and has launched an initiative called Skill India to equip millions of people with basic blue collar skills. However, even here the results will take time because the quality of primary schooling in India leaves much to be desired. The private sector needs to chip in and share the responsibility because such an opportunity comes but once in a century in the life of a nation. It thus remains to be seen as to whether India will be able to reap the benefits of a demographic dividend or will this youth be disillusioned by the lack of adequate employment opportunities and join forces fanning the Left Wing Extremism. I sincerely hope for the former.

BIBLIOGRAPHY/ REFERENCES

1. India's Security Challenges: Perspectives and Prospects; Nancy Jetly, Senior Fellow, IDSA

2. Address by Admiral Sureesh Mehta,(Retd) PVSM,AVSM,ADC, Erstwhile Chairman COSC at India Habitat Centre, New Delhi, on 10 August 2009, courtesy The National Maritime Foundation, New Delhi

3. India's Security Challenges: Perspectives and Prospects-Nancy Jetly, Senior Fellow, IDSA

4. India's Demographic Dividend: Asset or Liability?; Jan 09, 2013- The K@W Network: Wharthon- Unniversity of Pennsylania

5. Asia and the Pacific: Managing Spillovers and Advancing Economic Rebalancing; April 2012 International Monetary Fund (IMF) paper.

6. Article on "The Debate in India on Employability Issue" published in knowledge@wharton high school

7. India's Demographic Dividend: Asset or Liability?; Jan 09, 2013- The K@W Network: Wharthon- Unniversity of Pennsylania

8. Can India benefit from its demographic dividend? By Aakar Patel, Published in The Express Tribune on August 27, 2016.

9. Address by Union Minister Mr Sarbananda Sonowal 'India must make the most of demographic advantage' at two-day Youth Leadership Summit at Chennai: Nov 14, 2015

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

INDIA'S FUTURE SECURITY CHALLENGES FROM THE OUTER SPACE

Gp Capt GD Sharma, VSM (Retd)*

Introduction

In the present times, the global space industry is witnessing a continued expansion of the space-enabled capabilities of the nation-states and the commercial space actors, enabled by increased availability of technology, private-sector investment and falling launch service costs. However, the space presents both opportunities and threats. The opportunities stem from the actual and the potential use of the space for communications, weather forecasting ,remote sensing, global positioning, navigation and many other commercial applications as well as science. The threats would emanate from the weaponisation of the space leading to the arms race in the space. Fortunately; this is not evident as of now mainly due to the implicit moral binding of the States to the United Nations treaties which call for use of outer space for peaceful purposes. The Outer Space treaty of 1967stipulates that "exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind and the States shall not place nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies or station them in outer space in any other manner". The moon agreement of 1979 reaffirms and elaborates on many of the provisions of the Outer Space Treaty as applied to the Moon and other celestial bodies, providing that those bodies should be used exclusively for peaceful purposes.[1]Initially, common interpretation of the term "peaceful" in relation to the outer space was "non-military" However now the term "peaceful uses" is considered to mean "nonaggressive" rather than "non-

1 http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

military". Civilian applications of the space capabilities such as weather, navigation, communication and remote sensing are equally significant for the military purposes. In Gulf War of 1990-91, which came to be known as first space war, the coalition forces were supported by most sophisticated network ever designed. Of particular significance was the role of the US Navigation Satellite Timing and Ranging (NAVSTAR) GPS Satellites which enabled large number of coalition troops to navigate through the featureless Iraqi dessert even in the middle of the sandstorms surprising the Iraqi forces which naturally were expected to have an home advantage on the coalition forces thousands of the miles from their homes in an unfamiliar environment. GPS also guided US air, land and cruise missiles to hit accurately at their targets thousands of miles away. The Gulf War provided an insight in use of the space technology for achieving military effectiveness. Consequent to the Gulf War, today world over, space forms an integral part of military architecture. Net centric operations are reliant on the space to some degree ranging from satellite communication, space derived imagery, navigation and targeting provided by the global positioning system. Hence, their vulnerability is bound to be exploited by a country which feels geopolitically threatened.

The militarization of the outer space is thus already a fact and even weaponisation of the space may emerge as a reality in future particularly as the "peaceful use" of the outer space as permitted by the space treaties do not rule out the future offensive use of the outer space by militaries with conventional weapons or using emerging technologies against a nation state.[2]

The Outer Space Military Threats

Our military space systems are critical to the way we fight war today. Therefore, it is not surprisingly, nations are now actively testing methods to deny continued use of space services during conflict. Every major space-faring nation that can track a satellite and launch a satellite into outer space would have the means to mess up with the satellite," said Michael Krepon, the co-founder of the Stimson Center think tank in

2 Technology and the Law on the use of force :New security Challenges :Jackson Maogoto

Washington, D.C.[3] In that sense, 18 space faring nations as on date, would be able to target the satellites of their opponents. The list does not include a number of private organizations which are also launching space missions, though still largely in the sub-orbital level. Some US companies like Space X and have ventured in the Orbital flights in big way and are often retained by US government for undertaking launches to logistically support International Space station (ISS).

Space weapons could be used to compromise navigation, surveillance, communications and other functions in a wartime scenario or national emergency. Space systems by their nature are vulnerable to the range of threats. These threats include jamming satellite links, blinding satellite sensors, which can be disruptive or temporarily deny access to the space derived products. Anti-satellite weapons whether kinetic, conventional or Electro-Magnetic Pulse (EMP) weapons can irreversibly destroy satellites. Experts believe the biggest threats are not the kinetic threats to the satellites which would give away the identity of the offender but, more serious are the non-kinetic threats such as a subtle cyber-attack on our key space infrastructure that would disable and destroy our satellites in space and; jamming of satellite-based capabilities such as GPS and communications. This threat isn't limited from space-faring countries alone since the satellite jamming technology is relatively in expensive. In fact, there is an evidence to suggest that insurgents in Afghanistan and Iraq also have used jamming.[4]The other non-kinetic threats are from lasers which can blind imagery satellites and high-power microwave guns which could knock out circuitry on targeted satellites. The other development is in realm of offensive microsatellites which could be used for a kamikaze-type mission to ram another satellite or to snoop on it for data collection or jamming. Russia has sent micro-satellites into space and covertly maneuvered a small spacecraft close to commercial satellites. China on the other hand has launched the "Shiyan" -- equipped with a grappling arm that could snatch satellites

3 https://www.cnbc.com/2017/03/29/space-arms-race-as-russia-china-emerge-as-rapidly-growing-threats-to-us.html

4 Ibid

right out of orbit.[5] Russia and China as per the US threat assessment are developing directed energy weapons technologies for the purpose of fielding ASAT systems that could blind or damage sensitive space-based optical sensors.

Finally, Military force can also be employed against the ground relay stations, communication nodes or satellite command and control systems to render space assets useless over extended period of time

It is expected that threats to military, civil and commercial space systems will increase in the coming years. In 2016 worldwide Threat Assessment report of countries by the US Intelligence, opines that, Russia and China are actively developing counter space weapons systems to deny, degrade, or disrupt U.S. space systems. This may be true of Russia and China but, does not acquit US of carrying out a similar activity. As per the report, Russia aims to improve intelligence collection, missile warning, and military communications systems to better support situational awareness and tactical weapons targeting. Russian plans to expand its imagery constellation and double or possibly triple the number of satellites by 2025. Similarly, China is also increasing its space-based military and intelligence capabilities to improve global situational awareness and support complex military operations. This phenomenon is observed worldwide as many countries in the Middle East, Southeast Asia, and South America are purchasing dual-use imaging satellites to support strategic military activities, some as joint development projects.[6] It is believed that Russia and China are conducting sophisticated on-orbit satellite activities, such as rendezvous and proximity operations, which also has inherent dual use in counter space functionality. Similarly, space robotic technology research for satellite servicing and debris-removal might be used to damage satellites. Such missions will pose a particular challenge in the future and characterize the space environment of the future.[7]

5 https://edition.cnn.com/2016/11/28/politics/space-war-us-military-preparations/index.html

6 https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

7 ibid

On 07 may 2017, The U.S. military's experimental X-37B space plane landed on Sunday at NASA's Kennedy Space Center in Florida, completing a classified mission that lasted nearly two years, The unmanned X-37B, which resembles a miniature space shuttle, as per US AF has been designed to test risk reduction, experimentation and concept-of-operations development for reusable space vehicle technologies, maybe is a pointer on future technologies with military implications whose real purpose is still shrouded in mystery.

Space Security Challenges Emanating from India's Neighbourhood

India faces collaborative and collusive threat from Pakistan and China. Kashmir issue with Pakistan and unresolved border issue with China will keep this threat alive till an unforeseen future. The nature of threats faced by India is more complex today than in the past. The convergence of the cyber security and space security domains present a more complex challenge. Pakistan has not let down its support to the terror groups targeting India. The new cadres of terrorists are tech-savvy. The 26/11 Mumbai attacks has already given a preview of the emerging threat.

Pakistan's Space Threat. In the outer space regime, Pakistan is not space faring nation but, it still presents a credible kinetic threat to our satellites independently or with support from China. It has an array of surface to air missiles with maximum estimated range of 2750 km claimed with Shaheen III.As early as March 2001, Dr. Abdul Qadeer Khan in an interview stated that, "Pakistan has robust IRBMs which can launch geostationary satellites and all Pakistan has to do is to erase Delhi or Kolkata from the target and point it towards the sky." While till date Pakistan has not acquired satellite launch capability still Pakistan's threat to our satellites cannot be taken casually and a possibility of Pakistan's ground-based assets being used for targeting of our outer-space assets will always remain as it can also get the required support from China. Pakistan also poses a serious cyber and physical threat to the space infrastructure.

Chinese Space Threat. China has made great strides in both civil and military exploitation of the space. Its satellites have expanded its C4ISR capabilities, as well as ability to achieve space dominance with host of capabilities particularly in Electronic Intelligence (ELINT) , navigation and targeting from its navigation satellites(BeiDou) whose coverage is being expanded from a regional to provide a global with launch of more satellites. Apart from this, its successful foray in the Lunar missions (Change1&2), space stations (Tiangong 1&2) and conduct of five manned missions, showcase Chinese capability in the outer space.[8]When international Space Station (ISS) retires in 2024, China alone will have its space station. The objective of the Chinese space station is not clear but, it could also have long-term military implications. Some analysts estimate that People Liberation Army (PLA) wants to dominate the space high ground from LEO to the moon. In that effort, PLA's future spacelab could play a major role. It will be equipped with space cameras and dispensing payloads, and could be dedicated to space surveillance or combat missions.[9] Some analysts suggest that PLA is also aiming to develop U.S. X37B programme type manned space plane for carrying our passive and active military missions. The statistics show China is closely following American pattern of development in the space and has already overtaken Russia in launch of satellites. All these developments indicate that China will be a formidable space power in future. Chinese space aspiration are explicitly stated in the Chinese white paper titled," China's Space Activities in 2016" which however, focuses on civil space exploits like landing Change-4 lunar probe by 2018, first Mars probe by 2020 and BeiDou network going global by 2020 with 35 Satellites.[10]

China intends to continue increasing its space-based military and intelligence capabilities to improve global situational awareness and support complex military operations. India's concerns are more about the possibility of weaponisation of space by China. China's interests

8 http://www.chinadailyasia.com/chinajourneytospace/2016-10/07/content_15513209.html

9 http://www.strategycenter.net/research/pubID.247/pub_detail.asp

10 Chinese White paper 2016 accessed at www.globalsecurity.org/sp

in ASAT and space weapons are more US-centric than India-centric. However, from India's point of view, the concern is about China's counter-space capability. Eventually, such capability could also offer China an asymmetric advantage against India. Despite overt opposition to the weaponisation of the space, Chinese believes that weaponisation of the space is an inevitable developmental trend and an area for strategic competition. Realizing this, for more than a decade, Chinese military Strategists and aerospace scientists have been quietly designing the blue print for achieving the space dominance. Chinese are engaged in military modernization (especially in defence electronics) and organizational restructuring. In late 2015, China established a new service—the PLA Strategic Support Force—probably to improve oversight and command of Beijing's growing military interests in space and cyberspace. China remains committed to developing capabilities to challenge perceived adversaries in space, especially the United States, while publicly and diplomatically promoting non-weaponization of space and "no first placement" of weapons in space. China has now three priorities: space, nuclear weapons, and new concept weapons. Chinese are developing so called "the new concept weapons"viz; laser, beam, electromagnetic, microwave infrasonic, climatic, genetic, biotechnological and nano-technological weapons. Many of these will find application in space.

Current Status of Chinese Anti Space Capability. US intelligence report released in May2017 assesses that in ten years after China intercepted one of its own satellites in low-Earth orbit (on 11 Jan 2007 China successfully destroyed its own old weather satellite), its ground-launched ASAT missiles might be nearing operational service within the PLA. China is also known to have tested missile launch to 30000Km in the space which hints that China may even be able to target satellites of its adversary at MEO as well as in GSO. Chinese are effectively pursuing their anti-access and anti-denial strategy. It has developed *v*ariety of capabilities to limit or prevent the use of space-based assets by adversaries during a crisis or conflict, including the development of directed-energy weapons and satellite jammers.

Chinese anti-denial and anti-access capability is dependent on its space assets. To bolster its ELINT capability, it has launched a

constellation of 3 satellites in to 1100km, 63.4 degrees inclination orbit. This would enable continuous surveillance of high value targets to PLA.It is also known to making foray in deep space observations which allows it to keep an eye on the satellites of all adversaries including their own.[11]

China also continues to conduct sophisticated on-orbit satellite activities, such as rendezvous and proximity operations, at least some of which are likely intended to test dual-use technologies with inherent counter space functionality. For instance, space robotic technology research for satellite servicing and debris-removal might be used to damage satellites. Very recently, a maneuver made by Chinese satellites (possibly using a mechanical arm on one satellite to grab another satellite) has further increased the suspicion about their possible intent.

The global threat of electronic warfare (EW) attacks against space systems will expand in the coming years both in numbers and types of weapons. Developments will very likely focus on jamming capabilities against dedicated military satellite communications (SATCOM), Synthetic Aperture Radar (SAR) imaging satellites, and navigation satellite systems. Blending of EW and cyber-attack capabilities will likely expand in pursuit of sophisticated means to deny and degrade information networks. Chinese researchers have discussed methods to enhance robust jamming capabilities with new systems to jam commonly used frequencies.[12]

Does India Possess Ability to Counter the Threats to Space Assets? In comparison to China, India too has made great strides in the civil space and in deep space research. The Chandrayaan-1 moon mission launch in 2008, Mars orbital mission launch in end of 2013, Reusable Launch vehicle technology Demonstrator (RLV-TD) all point at tremendous progress made by ISRO in space technology which matches the best in the world but, its progress in the military space is minimal.[13]

---

11 Space, War and Security-A strategy for India .ANIAS publication.

12 https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

13 http://www.isro.gov.in/about-isro/isros-timeline-1960s-to-today#98

India needs to factor in China's investments in counter-space capabilities in its strategic appreciation. Currently, India has 42 operational satellites for different purposes including communication, navigation and research.[14] With the recent launch of the cartosat 2 series of satellite the number of operational satellites has gone to 43 with combined value of more than $40 to $45 billion. Theoretically, there is no protection available for any of India's space assets as on now. Our multi-faced security challenges demand that we should have adequate protection since, these facilities are vital for multifarious growth and lifting the quality of life of populace. Most satellites are dual use and have applications for the military. In coming years, the space technologies will have increasing utility for India's security particularly in the realm of reconnaissance, communications, and navigation assistance which naturally necessitates architecture for defence of our space assets. Presently, ISRO has a evolved a mechanism to safeguard its satellites from the space debris. The agency is a member of Inter-agency Space Debris Coordination Committee (IADC), which makes global effort to reduce man-made and natural space debris. IADC alerts a respective space agency when any satellite of that space agency is in danger due to space debris. ISRO also banks on its sophisticated Multi-Object Tracking Radar (MOTR), which is operational since 2015, to track space debris.[15] But, there is nothing in open domain to suggest that we have credible defence to safeguard our space assets from the inimical forces.

India' Options

Space Policy. To ensure free access to the space, we must develop full range of options to deter and defend against threats to our space infrastructure. Deterrence requires first foremost a clear statement of what interests are of vital national interests. A white paper /policy clearly

14 http://indianexpress.com/article/technology/science/isro-should-double-operational-satellites-to-meet-domestic-tech-knowledge-demands-as-kiran-kumar-4946486/

15 https://timesofindia.indiatimes.com/india/how-isro-is-safeguarding-indias-space-assets-in-orbit/articleshow/59278126.cms

stating this objective is therefore, vital. No nation, non-state actor should remain under any illusion that India will tolerate attack on its national assets in the space.

In order to cater for various existing and emerging space security challenges, two separate space commissions could be put in place: a National Space Commission and a Strategic Space Commission. India's existing Space Commission is tasked to work out a framework of a civilian mandate. The space security perspective should be placed under the preview of a Strategic Space Commission which should spell out a Space Security Policy. Various government organs involved in defence and foreign policy need consider all security issues and formulate policies regarding strategic requirements and issues concerning counter-space capabilities. This could change the nature of outer space dynamics and deal with our security challenges.[16]

Space Command

Threats to our space assets and exercising options to neutralize these threats from part of the military calculus which is beyond the realm of ISRO whose task should be confined for production and launch of the satellites for space scientific research / space exploration, civil and military as per their need. Military should implement the defence policy for the space. For this, we need a credible Tri-service Space organization which has resources and capability to protect the space assets. There have been some media reports regarding the possible formation of a Space Command/Agency as a part of India's security architecture. This agency should work in co-ordination with the Indian armed forces through their space cells which would have a better appreciation regarding to their service present and future needs. Such a structure should also cater to the needs of paramilitary forces which are deployed for border management and internal security tasks. The issues particularly concerning space and cyber activities do have a significant amount of "civil" component to it. Hence, this command/agency must have built-in flexibility in their approach for dealing with civilian government and non-government agencies, industry, and international agencies. The idea of

16 http://www.thespacereview.com/article/2390/1

establishing a Space Command should be on priority taken to its logical conclusion.[17] We need to develop defensive or offensive capability in space to deter and prevent our adversary from acting against our space assets.

Defending the Space Assets

The geostationary satellites and satellites at the medium earth orbit may be presently above the threat regime of ASAT weapons which so far has been tested at the lower earth orbit but, these satellites too are prone to jamming action of an adversary. The electronic attacks will generally take two forms i.e. Up link jamming which targets the radio receiver component of the transponder which will usually require large power. Downlink jamming, on the other hand targets the ground based receivers which are easy to jam and require less power. During the operation of Iraqi Freedom, Saddam Hussein forces employed GPS Jammers against the coalition forces. Although the attempt of the jamming did not succeed, it speaks volumes of the means which adversary could employ.

The other option to deploy hardened and robust satellites The military satellites are “hardened” to protect them against EMP and against collisions with micro-debris, but this adds cost and weight to these spacecraft.[18]

There is a need to encourage commercial space capability. So instead of having a handful of military satellites, there’s now the potential for many more by military teaming up with commercial observation satellite companies. Following this approach, the U.S. Strategic Command — the unified command that deters military attacks on the U.S. and allies — now has agreements with 58 international companies as well as a dozen nations.

Another strategy to reduce vulnerability of some sensitive satellite

17 ibid

18 http://www.nti.org/analysis/articles/future-space-security/

systems is to build more of them "to make the system more resilient and less vulnerable to attack." For example instead of multi-purpose expensive large satellites, we could launch specific task small satellites in large number. Apart from their affordable cost, built in redundancy, proliferation of smaller satellites has made the task of monitoring them much harder for the adversary.

We are not only country with space assets, teaming up with likeminded countries who have shared interests and values can provide a great opportunity to collaborate in Information sharing for mutual benefit in this area.

Protecting the Launch Facilities. Maintaining access to the space requires that all parts of the space complex be protected. The main components are the satellites themselves and ground stations that control them .Probably, the vulnerable part is the network of ground stations which are few in number and relatively soft targets with known locations. Attacks against the ground stations should be expected in the event of war .Hence, these merit grater physical protection.

Protection Through Redundancy. Until very recently, the satellites were fairly large ,very capable but, very expensive. These satellites present a very lucrative targets and even a loss of one would often constitute a dramatic loss of the capability. This particularly true of current generation of reconnaissance satellites as these are very capable but, relatively few in number and are very vulnerable owing to their need to be low earth orbit. One option of mitigating their vulnerability is to deploy in large numbers of less capable satellites. While highest resolution will still require large satellites, a network of small satellites could meet many needs and would provide graceful degradation in the event one is lost. Many countries like Britain, France, and Israel lay stress in deploying micro/mini satellites to bring down the cost as well as the element of threat.

Responsive Space Lift Capability

Another step that can be taken to assure access to space is to develop

responsive space lift capability i.e.to develop the ability to prepare and launch satellite within days to quickly replenish the combat loss. This approach would be more cost effective for small, cheap but not large satellites. ISRO is developing a PSLV launch vehicle exclusively for small satellites that is slated to be launched in early 2019. The small launch vehicle is expected to cost one-tenth of a normal PSLV rocket which costs anywhere between INR 1,500 million and 5,000 million and will be capable of carrying a payload of 700 kg.[19] In February 2017, when ISRO launched record 104 satellites onboard PSLV C37, excluding the Cartosat-2, all the rest were small satellites, including 88 Planet Doves. In Jan2018, once again ISRO launched 31 small satellites their weights ranging from 1 kg to 100 kg along with Cartosat-2 satellite. Hence, ISRO has showcased its ability in small/mini/micro satellites. Defence services too could take advantage of their capacity if needed.

The small satellite industry has witnessed a manifold spike in the last few years and with latest innovations in Nano-technology, the size of the satellites and their costs are expected to further decrease in the future making them highly affordable.[20]

Offensive Counter Space

This covers kinetic and non-kinetic means. The kinetic means relate to direct ascent weapons like ASAT or directed energy weapons and co orbital ASAT.

Kinetic. To deter an adversary from committing the space misadventure, acquiring of ASAT capability for India is often recommended by the strategists. Weaponisation of space however, is not an option for responsible space faring state and should be avoided at higher altitudes due to creation of space debris. However, what is important for India is to

19 https://www.geospatialworld.net/blogs/isro-market-satellite-launch-vehicle/

20 http://www.thehindu.com/sci-tech/science/isro-developing-a-compact-launcher-for-small-satellites/article21420644.ece

build and showcase its technological capabilities. India should build and display *debris-free* ASAT competence at about 150 to 250 kilometers above the earth's surface. This should adequately deter our adversaries.

Non-Kinetic /Soft kill - Jamming/Cyber, Wresting Control of the Enemy Satellites. It provides suitable and equally effective alternative to the hard kill option and should be explored by India especially due our acclaimed reputation of being an IT capable state.

Enhancement of Surveillance Capability. India has so far does not have a credible ELINT for monitoring electronic signals of military facilities of our adversaries especially over the ocean areas. This is a major gap that needs to be addressed if an operational ISR capability has to be created. Similarly, deep space observation is necessary to keep eye on satellite environment for an effective offensive counter space action.

Recommendations

No other space faring nation except India has shown antipathy towards military use of the space. As we move forward towards 21stcentury, it is inevitable that space becomes another medium of warfare. China near home is rapidly emerging as a space power and its capabilities may also be placed at the disposal of other countries for strategic and commercial reasons. Exploitation of the space would be great advantage against non-space capable nations such as enjoyed by Allied Forces in Iraq war and Afghanistan campaign but, advantage would be nullified against a space capable nation. In such a scenario, the favourable space control (similar to a favourable air situation in context to the air space) is feasible only if we retain our capability to use space assets while denying their offensive use to the adversary. This would mean that we develop ability to degrade the performance of enemy satellites. In this context, India needs to address the role of space in our defence and national security. Towards this, the setting up of Strategic Space Commission for holistic appraisal of the space security needs of the country similar to the Space Commission for the civil needs be established. All stakeholders from

defence, paramilitary, industry and scientific community could be part of this body for holistic review of the needs. This could be followed in a white paper /policy statement clearly stating the defence objectives. The establishment of Space Command /Agency should be taken to a logical conclusion to implement the programmes with co-operative participation of individual service space cells including that of Para- military forces. We also need bolster our ELINT capability by launching a constellation of satellites for continuous surveillance of high value targets on land and sea and create capacity for deep space observation to keep eye on satellites (own and adversary's satellites) to avoid surprises in conflict situations.[21] Small satellites could provide an answer to the need of military for redundancy and high cost involved in addition to dual use of the civil satellites for the military.

***Gp Capt GD Sharma, VSM (Retd)** is a Senior Fellow CENJOWS, New Delhi

21 http://isssp.in/wp-content/uploads/2016/03/Space-War-and-Security-_A-Strategy-for-India.pdf

THE MULTI DOMAIN BATTLE CONCEPT : A PRELIMINARY ASSESSMENT

Dr Manabrata Guha*

Preface

This paper, which is part of a larger and more detailed ongoing research project on the subject of Multi Domain Battle (MDB), is a preliminary and tentative presentation of the background and core elements of this "new" battle concept. As such, it will confine itself to (1) providing a brief context-setting account within which the MDB concept may be situated, and (2) the rationale and design-intent of the MDB concept, particularly in the context of Anti-Access/ Area Denial (A2AD) architectures and systems.

The Context: The "Modern Battlespace" and "The Modern System" of Warfare

To recognize and appreciate the evolutionary imperative that underwrites the MDB concept, it is necessary to first take a step back and pay attention to its antecedents. While the available literature does not overtly mention it, the MDB concept can be said to be grounded within a concrete reality, which Stephen Biddle refers to as the "modern system" of warfare. Biddle describes the "modern system" of warfare as being "a tightly interrelated complex of cover, concealment, dispersion, suppression, small-unit independent maneuver, and combined arms at the tactical level, and depth, reserves, and differential concentration at the operational level of war".[1] It is important to bear in mind that this "modern system" of warfare emerged within the context of a "modern battlespace" that was, and continues to be, marked by an intensity of firepower – direct and indirect – that is growing exponentially.[2] Biddle provides us with some

stark examples. He observes that "both speed and apparent lethality have increased dramatically since 1900, and are continuing to do so…"[3] Using an impressive set of data, Biddle demonstrates that

> the maximum tank speeds for designs fielded between 1916 and 1991…shows an average increase of 0.5 m.p.h (miles per hour) per year, or a more than tenfold improvement across the interval as a whole; with the increasing use of helicopters on the battlefield after the 1960s, the effective increase in the speed of the most mobile ground forces is arguably at least fiftyfold since 1916.[4]

His observations regarding the exponential growth of the range of the lethality of weapons-systems are equally enlightening. His analysis of the relevant data-sets suggests that ground and air weapon systems have seen improvements

> …from a maximum range of less than 100 meters for 200mm armour penetration by direct antitank weapons in the 1930s to more than 6000 meters by 1980; from less than 10 kilometers for tube artillery in 1900 to more than 250 kilometers for missile artillery in the 1990s; and from an unrefueled combat radius of under 500 kilometers for ground attack aircraft in the 1920s to more than 2000 kilometers today.[5]

Given this, it is not surprising that "[s]uch tremendous growth in speed and lethality creates a powerful incentive to find ways of limiting one's vulnerability to such weapons."[6] Interestingly, Biddle's evidence further shows that the emergence of this "modern system" of warfare can be said to have first become evident during the First World War where the freedom, indeed possibility, to maneuver was increasingly curtailed by the intensity of direct and indirect artillery firepower leading to the infamous "trench warfare" conditions that marked the better part of that war.[7]

Max Weber, in his landmark study, The Protestant Ethic and the Spirit of Capitalism[8], used a curious phrase, stahlhartes Gehäuse, which Talcott Parsons famously translated as "the iron cage" - though recently his translation been challenged and the phrase "shell as hard as steel"

has been offered as being a more accurate representation of Weber's original phrase.[9] Either way, in the context of this essay, Weber's term, used metaphorically, represents a condition of existence wherein freedom of action is restricted or constrained by the enforcement of rational-efficiency. Considered in this way, it could be said that "the modern battlespace" is akin to a "steel cage", within which military operations and, in an extended sense, military affairs - since 1918 - have unfolded. The growing intensity of firepower is, in a way, "rationalizing" the battlespace by imposing a set of constraints that restrict freedom of action at the tactical, operational and strategic levels. This has led, as Biddle points out, to an increased focus on "force employment" and, consequently, on doctrine and training.[10] It is also worth bearing in mind that "the modern battlespace", in addition to the growing intensity and lethality of firepower, is also being increasingly draped with dense meshes of communication and surveillance networks, which aim to "illuminate" the battlespace thereby making the task of, in Biddle's words, "limiting one's vulnerability" to the intensity of firepower and the growing coverage, accuracy and depth of the mesh of surveillance networks a highly problematic one.

One can see the evolution of this "steel cage" over approximately the last one hundred years. As mentioned above, the first evidence of the material reality of the "steel cage" can be said to have emerged during the First World War. The freedom to manoeuvre that military forces had enjoyed from the time of the Napoleonic Wars to the Franco-Prussian War of 1870 was severely constricted when faced with the growing role of the artillery.[11] But this state of affairs did not halt efforts to break out of this "steel cage". As the imperatives of the emergent battlespace imposed themselves on the combatants of the First World War, simultaneously, efforts were being made to identify optimal ways and means to "break-out" from within the growing constraints that "the modern battlespace" was imposing.[12] Most famous of these were the German efforts, commonly known as 'infiltration tactics' or von Hutier tactics, which later informed the peculiar (for the time) style of the Wehrmacht's military operations as evidenced especially in the early years of the Second World War.[13] Additionally, though originally initiated

by the British, the fundamentals of tank/ mechanized warfare were also being explored by the major European powers, which also count as efforts being made to recover the element of mobility that was deemed to have been lost since the emergence of the "steel cage" of modern warfare.[14]

A closer analysis of the innovations in small-unit infantry tactics and of the nascent efforts to think through the use of tanks in combat operations in the interwar period (1918-1938) suggests that at least two of the key "concepts" underlying the attempt to "break-through" the constraints of the "steel cage" were "dispersion" and "surprise". We can see these concepts being further developed as the Wehrmacht undertook Fall Gelb in May 1940, which lead to the defeat of France – tactically, operationally, and strategically. But aside from acknowledging the brilliant use of the concepts of dispersion and surprise by the Wehrmacht, there are two points which are of relevance to us and, as such, must be noted. First, the Wehrmacht's operational aim, as is well-known, sought to solve the problem imposed by concentrated and overpowering defensive artillery firepower and an entrenched defensive system by seeking ways and means to recover and exploit the freedom to manuever. This was in keeping with the German tradition of designing manoeuvre-centric operations in a bid to defeat an adversary by attacking and overwhelming his flanks and rear.[15] Also of critical importance for the German military-operational designs of the time was the element of surprise, rapid concentration at the point of attack, and an equally rapid dispersal approximating what Liddell-Hart described as "the expanding torrent".[16] In this connection, it is important to note that in some quarters of the German General Staff and military establishment, the Manstein version of the German military plan for Fall Gelb was not expected to succeed. Indeed, as the operations unfolded the initial atmosphere within the German High Command was one of extreme anxiety.[17] Thus, some of Hitler's directives to his commanders during the preparatory phase of Fall Gelb were clear in its insistence on avoiding getting into a situation where the German Armed Forces could get bogged down in a bloody and brutal stalemated situation reminiscent of World War I. Indeed, such directives went further to state that preparations should

also be made for addressing precisely such an eventuality. This suggests that the collective experience of most of the German commanders – including, in part, that of Hitler – remained powerfully impacted by their experiences on the battlefields of the First World War.[18] Equally, if one looks at the French military doctrine of the time, one notices a disproportionate emphasis being laid on fixed defensive systems. And, while the "cult of the offensive" remained an important element of French military doctrine in the 1920-1940 timeframe, the French strategic-military posture remained defensive in nature.[19] Leaving aside other factors, it could be said that, at least one of the primary reasons as to why French military planners and strategists chose to remain on the strategic-defensive was because of their experience, like their German counterparts, of the bloody stalemate battles of the First World War. In other words, despite impressive advances made by the French in terms of tank designs, among other things, the French strategic-posture relied on the "steel cage" of the "modern battlespace" represented by, among other things, fixed defences (the Maginot Line), weight of artillery firepower (including the revised and improved doctrine for its use[20]), aerial surveillance, which were geared to deter and thwart any offensive movement. While rational analysis would suggest that this reliance was, in essence, not misplaced (relative to the times), the evidence from history is otherwise.[21] In approximately six weeks, a Wehrmacht, still equipped with a relatively underpowered and under-gunned tank fleet, an artillery park that was, on average, of a lower calibre than what was needed to penetrate the armour of the majority of French and British tanks, with a doctrine that was still in the process of being fleshed out, and led by commanders who brought to a combined arms battlespace their default tendency to apply "infiltration tactics" and, at the operational level, strategies of "expanding torrents", defeated the combined might of the Anglo-French forces. As impressive as these victories may appear, it is important to also recognize that while the Wehrmacht's innovations in force-employment achieved a "break-through", which led to the defeat of a feared adversary, the final outcome of the operation was unexpected - both by the Allied and German military high commands.[22]

The second point of interest is related to the first and, for our purposes, has greater significance. As noted, the French laid emphasis on the primary characteristics of the "modern battlespace" – intensity of firepower and a deep defensive system - by means of which she hoped to deter and contain any aggressive movement by her primary adversary, Nazi Germany.[23] We also noted that German innovations in the area of force employment relating to infantry tactics, battlespace management, armoured and combined arms warfare "cracked" the constraints imposed by the "modern battlespace". Given our specific interest relating to the evolution of the MDB concept, it is important to recognize what may be considered to be an "organizing principle" that appears to have underwritten the German military operations in May 1940. Most overtly, of course, the Whermacht's operations ensured the defeat and surrender of a feared adversary. More importantly, however, they also give us an insight into the advantages that accrue when considering an adversary in "systemic terms", and in the designing of military operations that take into account a systemic view of an adversary's strategic-military's war-waging potential. When considered in this light, the Wehrmacht's offensive operations – though they were never overtly assigned this objective – may be said to have provoked a systemic paralysis, which broke the coherence of the French military command thereby triggering the collapse of the French ability to wage war.

Interestingly, Soviet military theorists, particularly Isserson, Tuchachevsky, Triandafillov, among others, were already working – even in the late 1920s and early 1930s - on a military-operational model that took into account – albeit vaguely at the outset – a systemic consideration of an adversary.[24] This was reflected with increasing sophistication in various subsequent versions of the Soviet theory of "deep battle" wherein the aim was (and remains) to target what are deemed to be critical nodes of an adversary's defensive system in a bid to bring about the collapse of his war-waging abilities. Considered in the context of the first two decades of the 20th Century, this was a highly advanced concept and one which underwrites the early discussions on "revolutions in military affairs" in the late 20th and early 21st Centuries. Our interest, however, is restricted to the perception of an adversary's

offensive and defensive capabilities in systemic terms for it is in this specific context that the MDB concept assumes its real significance. Considering an adversary's offensive and defensive capabilities from a systemic point of view enabled Soviet military theorists to refine and evolve the basic concepts underlying the German offensive operations, which they used to great effect in the latter stages of the Second World War. Nevertheless, the overhang of the "modern battlespace" remained.[25]

As the Second World War drew to a close, it was evident that while the "cracking" of the "modern battlespace" was already a military-operational imperative, the German model had lost much of its innovativeness, but not its relevance. The blunting of the edge of innovativeness was not because of some weakness of the model, but because, for the most part, virtually all the antagonists in the war had - to some degree or another – adapted to it and had employed it under combat conditions.[26] In other words, "blitzkrieg", by May 1945, was not so much a "German thing". It was employed as much by the Germans as it was by the Allies.[27] Moreover, the "modern battlespace" had also evolved in the interim. As the world segued into the phase of the Cold War and with the dawn of the nuclear age, in the context of conventional inter-state warfare, the "steel cage" of the "modern battlespace" continued to make its presence felt. While the quantum and intensity of firepower increased, so did increasingly sophisticated networks of command, control, communications and surveillance. With the rapidly increasing range of weapon-systems, coupled with emergent advanced capabilities like beyond-visual-range attack capabilities, sophisticated battlespace management systems, the growing ability to leverage the domains of space and sea, the concept of an "extended battlespace" began to make its appearance.[28] Marked by precision-guided weapons, and overwhelming intensities of targeted firepower, the military-operational aim was not so much to deter or defeat masses of an adversary's field formations, but to target key links and nodes of his military-operational systems thereby engineering a military-operational collapse and, by extension, a strategic-political defeat. Such an aim also brought in its wake the need for an "integrated" effort given that, in the interim, "the extended battlespace" was expanding to include the Space,

Electro-magnetic, and undersea domains, which had begun to acquire increasing importance.

Much of this was observed and commented on by Soviet military theorists in the 1970s and early 1980s who referred to this transformation of the battlespace in terms of a military-technical revolution.[29] Indeed, their model of the Recon-Strike-Complex may be said to be a consequence of such emergent capabilities, which they perceived in, among other things, the Assault Breaker program of the U.S. military.[30] Soviet theorists understood the nature and import of the transformation that was taking place in "the modern battlespace" wherein massed firepower was (and continues to be) replaced by firepower of equal intensity, but delivered precisely. They recognized the fearsome effects of integrated firepower – across domains – that could be brought to bear on an adversary within an "extended battlespace" thereby constraining – to the extreme – his operational flexibility. Such assessments appear to validate Biddle's emphasis on the criticality of "force employment" – both as a tool with which to assess military capabilities and effectiveness of adversaries, and as a sphere of activity that demands constant training, doctrinal development and innovation – in the context of "the modern battlespace".

These assessments, of course, form the bedrock of the intense debates on revolutions in military affairs, Information-Age Warfare and Network-centric War. Critically, the common thread that runs through these debates is an appreciation – overt and implied – of the harsh and uncompromising nature of "the modern battlespace". Thus, it is within this context that the MDB concept must be considered and its significance assessed.

The Multi-Domain Battle Concept: A Brief Overview

The Multi-Domain Battle (MDB) concept - as championed by the U.S. Armed Forces, particularly the U.S. Army - aims to supplant the Air-Land and Air-Sea Battle concepts.[31] This aim is underwritten by a growing appreciation of the fact that

> [c]ontemporary and emerging threats seek to gain control of contested spaces not only in the air and on land but [also] at sea, in space and cyberspace as well as the electromagnetic spectrum and the cognitive dimension of human perception. Thus, the increasing number of adversaries who learned to attack the air, maritime, space and cyberspace domain superiority premises of current [U.S.] Army and joint doctrine challenge the U.S. military's ability to achieve military and political objectives[32]

Further, it has been assessed that "separatist forces [are] able to gain air superiority via the land, without even an air force….[they are] able to take down large land forces with a combination of electronic warfare, cyber, autonomous systems, drones, et cetera – not with a close-in battle."[33] In short, the conclusion is that the U.S. strategic-military establishment requires "urgently" – depending on who is asked – "a very difficult-to-fracture concept."[34]

By positioning the MDB concept as a successor to the Air Land (and Air Sea) Battle concept, while the U.S. strategic-military establishment appears to be in the process of designing a "new" battle concept, it is also - at least implicitly - acknowledging that either (1) the previous two concepts have been 'fractured' or run the imminent danger of being so, and/ or (2) they are now being rendered increasingly obsolete/ irrelevant given the technological and operational solutions/ counter-measures that 'near-peer competitors, but also separatists and other lower-end threats', are developing, adapting to, and deploying. The MDB concept is thus envisioned as 'a more complex concept' that will expand the operational scope and reach of the US strategic-military establishment thereby potentially thwarting the operational parity that near-peer competitors and other lower-end threats are alleged to be acquiring with growing alacrity.[35]

Clausewitz had observed that while everything in war may appear to be simple, but the simplest thing often ends up being the most difficult to accomplish. In a similar sense, while the MDB concept may yet prove to be difficult to actualize, as a concept, however, it is relatively simple to grasp. For our purposes, it is enough to say that the basic idea is to

"synchronize cross-domain fires and manoeuvre in all the domains to achieve physical, temporal and positional advantages."[36] This requires "mov[ing] beyond the mere synchronization of joint capabilities to the complete integration of capabilities", which will allow, for example, "anti-air capabilities…coming from a … submarine or anti-ship cruise missiles…coming from an Army unit on the ground."[37] But, as the concept's proponents hasten to clarify, "the multi-domain battle concept isn't just about better integrating the operations of the services…It also requires each individual service to expand its areas of responsibility." The security environment, it is claimed, "will require all the services to exert influence in non-traditional domains."[38] Consequently, it is argued, the MDB concept will require the U.S. Defense Department to rethink how its forces are organized, trained and equipped.[39]

Why is this necessary? Because, "[w]e're not organized that way, we don't necessarily train that way…Our equipment doesn't necessarily operate that way."[40] The proponents of this concept offer some illustrative examples of how they envision the concept playing out under combat conditions. Thus, for example, they assert, "[the] Army has got to be able to sink ships, neutralize satellites, shoot down missiles, and hack or… [damage] the enemy's ability to command and control its forces."[41] Such a posture, it is claimed, will allow for a re-imagining of the battlespace, which may be somewhat colourfully described – particularly when referring to an Anti-Access/ Area-Denial (A2AD) complex – as "a block of Swiss cheese", which will allow for seeking out gaps in the defensive designs of an adversary and attempting to trigger a systemic collapse of the adversarial defensive system by unleashing a lethal symphony of firepower and other non-contact, but equally disruptive, means.[42] While the design-intent of this concept of battle is interesting and, in some ways, may even be innovative, however, some questions remain. Thus, for example, it could be asked can the MDB concept be considered "new" or even "different" when considered in the context of the concepts that it seeks to replace (Air-Land and Air-Sea Battle)? Indeed, in the case of the Air-Land Battle concept, can it not be said that the forces of the "air domain" impact directly on land-centric operations? The Wehrmacht's offensive operations in May 1940 integrated – at least to some degree – forward air controllers who directed the "air artillery". Notice how in this

formulation, a weapon-system generally associated with “land power” – artillery – is conjoined with a domain – “air” - in and to which it has no direct correlation except perhaps when it is being transported. Yet, the Stuka bombers, in close air support operations, using innovative tactics, effectively played the role that ground-based artillery would have played had it the range. And, while the arsenals used by the Stukas were primitive in comparison to what is available now, the parallels are striking where the Air Land Battle concept is concerned. Another example, at the level of a specific weapon-system is that of the German 88mm Anti-Aircraft gun, which was originally designed for ground-based air defence systems. On the battlefield, however, increasingly German commanders could be noticed using it as a highly accurate and very effective anti-tank weapon, which proved its worth in, among other places, North Africa and on the Eastern Front, especially in the post 1942 phase. Of course, it needs to be mentioned that, strictly speaking, the gun crews of the 88mm in land warfare roles were from the Army and not from the Luftwaffe which controlled the Air Defence functions.

The Multi Domain Battle concept, however, appears to claim a fundamental and critical difference. In effect, the difference lies in the “nature” of the “intervention/ participation” of capabilities and weapon-systems across “domains”. The U.S. Army claims that the aim is to be able to orient ground forces to intervene in, say, a sea battle with the use of weapon-systems that usually are not within the arsenal of ground forces like, for example, anti-ship missiles. Alternately, ground forces with offensive cyber warfare capabilities, if positioned appropriately, may be able to play a pathfinder’s role by targeting and neutralizing information systems that control enemy air defense systems thereby allowing the air force to conduct air strikes with relative impunity. Note also that considering the source of the MDB concept – i.e., the U.S. Army - the emphasis of the literature released thus far suggests that it appears to be almost a plea for the U.S. Army’s continuing relevance. This is made more than obvious if we consider the following statement: “…the Army has got to be able to sink ships, neutralize satellites, shoot down missiles, and hack or… [damage] the enemy’s ability to command and control its forces.”[43]

In this context there is another point to consider, which is perhaps one of the most interesting elements of the MDB concept because it gives us an insight into the "vision of the battlespace" that underwrites the concept. Recall here Admiral Owens' "system of system" concept.[44] It is worthwhile to remind ourselves that the Admiral was well versed in the Soviet theorization of the Recon-Strike-Complex which, as we have noted previously, was a distillation of what in its originary form was the Soviet theory of deep-strike operations of Georgi Isserson and Mikhail Tukhachevskii. While the basic tenet of the Soviet theory was maneuver warfare (with a growingly important and refined role being accorded to Operational Maneuver Groups (OMGs)), the conceptual premise, however, was grounded in "systems theory" which, in turn, was based on the "scientific materialism" of Marxist-Leninist theory. Roughly speaking, this was based on the understanding and rendition of an adversary in terms of "systems of capabilities" consisting of nodes and links. The basic aim of such a theory was principally to attack and neutralize (and/ or destroy) selected nodes and links of such an adversarial system thereby triggering a breakdown of the feedback and control loops that maintained and fostered the consistency of the system. This would, or so it was conjectured, lead to the eventual "stretching" of the enemy system leading to a systemic collapse.

The key point here is to recognize the unmistakable presence of the Soviet "systems theoretical" approach to assessing and engaging with an adversary's military and combat capabilities within the MDB concept. It could be said that the MDB concept implicitly presumes a confrontation – spread out across multiple domains - against "a system" comprising of nodes and links under combat conditions. Consideration of an enemy's capabilities in this way allows for a macroscopic understanding of the comprehensive combat capability of the adversary. Simultaneously, it also allows for the identification and targeting of not simply nodes and links, but also "pathways" that lead deeper into the adversarial system to expose and target deep vulnerabilities. It is important to recognize that the visualization of the adversary and of the battlespace is multi-dimensional in nature, which is evident in how an Anti-Access/ Area Denial (A2AD) system – with specific reference to the Chinese Anti-

Ship Ballistic Missile (ASBM) project - is described: as a "block of Swiss cheese" with holes rather than as a iron dome.[45]

Thus, for example, an A2AD complex may be considered to be an assemblage of a set of "zones" and "experiential conditions" wherein adversarial combatants experience calibrated levels of deterrence. These levels of deterrence, which culminate in a kill-zone, are contingent on not only the capabilities of the weapon-systems that constitute the A2AD assemblage, they also depend to a very large extent on how these capabilities are integrated and employed. In effect, an A2AD system aims to present an asymmetric counter to the potential of a concerted offensive assault. This asymmetry is expressed by designing concept-technology pairings which aim to subvert the critical capabilities of the offensive weapon-systems that underwrite the offensive assault. Given this, it would appear that the MDB concept is designed to degrade the A2AD's "deterrent potential" and to render ineffective its "kill-box". While the conventional approach would be to overwhelm a defender's A2AD system, the MDB concept seeks to selectively target in a bid to degrade and/ or destroy key capabilities of the A2AD system. Such efforts would include, among other things, the selective targeting of the satellite constellations that coordinate and "integrate" such systems; corrupting or otherwise distorting the critical data links that provide terminal guidance to the key weapon-payloads; targeting ground-based radar systems and interfering with the electro-magnetic spectrum etc. When considered in this way, it may not be amiss to say that the MDB concept serves as the emergent counter-part of the A2AD concept. Put differently, it could be said that if we consider Biddle's "modern system" to be Janus-faced, then the MD and the A2AD concepts represent the two "most modern" antagonistic faces of "the modern system" of warfare.[46]

Concluding Observations

It is tempting to understand the MDB concept as being an expression of "maneuver warfare theory" in the context of an informationalized and networked battlespace. However, when observed keenly, it becomes apparent that what the MDB concept appeals to is "maneuver-ism" and not necessarily "maneuver warfare theory" given that the latter is

beholden to the interplay between the dimensions of time and space while being, for the most part, restricted to a single domain (land). "Maneuverism" – in the context of the MDB concept - may be understood as being a military-theoretical framework that privileges movement/ mobility as against the physical notion of maneuver (which, being a land warfare concept, is domain-specific). Given this, it may be more appropriate to speak in terms of "agility" in the MDB context rather than in terms of "maneuver" though both these terms share a familial relation with the notion of "maneuverism".[47] It warrants mentioning that there are at least three kinds of agility that are invoked in the MDB concept: (1) agility of the "sense and response" function; (2) agility of the command and control function, and (3) agility in the production and delivery of targeted effects on adversarial strategic-military systems. Agility, thus, while assuming a critical role in the MDB concept, also highlights the recognition that the "the steel cage" of "the modern battlespace" is not as precise (or set-piece) as earlier. Today, the battlespace both expands and contracts, which contributes to the exponential growth of complexity in the battlespace. The MDB concept is, thus, being offered as being one way by which to "sense and respond" to the vagaries of an "elastic battlespace" and as a means by which to operate within highly complex operational conditions.

Given the above, it is perhaps obvious that within "the extended battlespace" of the 21st Century, to be able to create, sustain and expand a Multi Domain combat capability in any meaningful manner will necessitate building up of cutting edge capabilities, particularly in the cyber and Artificial Intelligence (AI) domains. This is because, particularly where the cyber domain is concerned, it is increasingly being viewed as the critical "connective tissue" that "integrates" cross-arm efforts to create and deliver what may be referred to as a "composite effect" on an adversary across multiple domains, while AI would facilitate the acquisition, and analysis of data and as a tool to facilitate decision-making in addition to, eventually, being integrated into weapon-systems and platforms. In the process, data and information fusion will become increasingly important given that the "fusion" process latter breaks down silos in which information is usually stored, which is a necessary pre-

requisite for the development of a truly seamless multi-domain capability. It thus follows that if the cyber domain is considered to be "the connective tissue" in the context of not only a multi-domain capability, but also in the context of an informationalized "modern (extended) battlespace", then it is likely that in the future it may become the primary site wherein the outcome of a battle or an operation or even a campaign will be decided. Further, the focus on delivering precise and targeted, but overwhelming firepower, is contingent on the development of weapon systems and platforms that are designed from ground-up with such capabilities in mind. Thus, as the MDB concept matures, it is to be expected that the design and development of weapon-systems will also undergo a change. Increasingly weapon-systems would be designed to be able to operate seamlessly across domains with a likely emphasis being put on unmanned and autonomous systems like drones and cruise missiles that can carry and deliver heavier and a more varied payload.

The MDB concept is being offered as an organizing principle of military operations that will combine "informationalized warfare with the accuracy and relative low cost of guided munitions…[and]…the victors on the next battlefield will fix and fracture their adversary with quick, decisive, and lethal effects across the entirety of the battlespace and immediately consolidate gains to make any military response politically unpalatable."[48] To this end, it is asserted that "[w]hat we require today are truly integrated, resilient, and rapidly deployable military capabilities designed to achieve cross-domain maneuver and fires, capable of working together in a convergence that goes beyond synchronization. This is the idea behind Multi-Domain Battle."[49]

ENDNOTES

1. Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle, (Princeton: Princeton Univ. Press, 2006), p 3

2. See, for example, Jonathan B. A. Bailey, "The First World War and the birth of modern warfare" in The Dynamics of Military Revolution, 1300–2050, Ed. Knox and Murray, (Cambridge: Canbridge Univ. Press,

2001), pp 132-153. See also his Field Artillery And Fire Power, (Oxford: Taylor and Frances, 2009, e-version). Note also, the notion of a "modern battlespace" has been defined by the U.S. Army's FM 1005, Operations, June 1993 in the following terms: "[1] Battle space is a physical volume that expands or contracts in relation to the ability to acquire and engage the enemy and [2] Components [are] determined by the maximum capabilities of a unit to acquire and dominate the enemy; [it] includes areas beyond the AO [area of operations]; it varies over time according to how the commander positions his assets. See Robert J. Bunker, "Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI" in Parameters, Autum 1996, pp. 108-120. Available at http://ssi.armywarcollege.edu/pubs/parameters/articles/96autumn/bunker.htm

3. Stephen Biddle, "The past as prologue: Assessing theories of future warfare", in Security Studies, Vol. 8, 1998, p 13

4. Ibid., p 13

5. Biddle, "Past as Prologue", p 13

6. Biddle, Ibid., p 14

7. The Battle of Somme is said to epitomize the massacres involved with saturation-level artillery fire that reduced the battle to a bloody stalemate and which powerfully reinforced the critical role the artillery was to henceforth play in military operations with consequence impacts at the strategic-operational and even strategic-political levels. See, for example, Peter Hart, The Somme: The Darkest Hour on the Western Front, (New York: Pegasus Books, 2016).

8. Max Weber, The Protestant Ethic and the Spirit of Capitalism, transl. Talcott Parsons, with a foreword by R.H. Tawney. (London: G. Allen & Unwin, Ltd., 1930), p 181

9. For a discussion of the appropriateness of Parson's translation and of its suggested replacement, see Peter Baehr, The "Iron Cage" and the "Shell as Hard as Steel": Parsons, Weber, and the Stahlhartes Gehäuse Metaphor in the Protestant Ethic and the Spirit of Capitalism, History and Theory, Volume 40, Issue 2, pages 153–169, May 2001.

10. Again, looking back at World War 1, it is instructive to see how armies adapted to such emergent conditions. For an interesting account of the

Canadian experience, see Bill Rawling, Surviving Trench Warfare: Technology and the Canadian Corps, 1914-1918, 2nd Revised Ed., (Toronto: Univ. of Toronto Press, August 15, 1992)

11. For an excellent account of the role of the artillery and the influence it is deemed to have had on the revolution in military affairs in the 1920-30s see Jonathan B. A. Bailey, Field Artillery And Fire Power, (Oxford: Taylor and Frances, 2009, e-version)

12. In Biddle's terms, these efforts may be understood as finding ways and means to innovate and to refine "force employment". See his Military Power: Explaining Victory and Defeat in Modern Battle, (Princeton: Princeton Univ. Press, 2006)

13. For an excellent account of German "infiltration tactics" see Bruce I. Gudmundsson, Stormtroop Tactics: The Innovation in the German Army, 1914-1918, (Westport: Praeger Publishers, 1989)

14. Williamson Murray, "Armoured warfare: The British, French, and German experiences" in Murray & Williamson, Ed. Military Innovation in the Interwar Period, (New York: Cambridge Univ. Press, 2009), pp 6-49

15. Trevor N. Dupuy, A Genius for War: The German Army and General Staff, 1807-1945, (London: Endeavour Press, 2013)

16. Captain B.H. Lidell-Hart, "The "Man-in-the-Dark" Theory of Infantry Tactics and the "Expanding Torrent" System of Attack", November 3rd, 1920. Talk delivered and published in the Journal of The Royal United Service Institution; February, 1921. Available at http://regimentalrogue.com/misc/liddell-hart_man_in_the_dark.html

17. Karl-Heinz Frieser, The Blitzkrieg Legend: The 1940 Campaign in the West, (Annapolis: The Naval Institute Press, 2012), p 290. One illustrative example, as Frieser reports, is of Hitler admonishing Rommel's "unauthorized push at Avesnes" by saying, "Your raid cost me a sleepless night".

18. Ibid, p86

19. There are multiple reasons for the adoption of a "defensive posture" by France of which only a few are purely military in nature. Other reasons

include a dropping population rate, a fractious internal political climate, and the deleterious impact of the costs of the First World War, not simply financially and economically, but also socially. For a classic account of the fall of France, see Alistair Horne, To Lose a Battle: France 1940, Repreint Ed., (London: Penguin, 2007).

20. The use of Bruckmuller's tactics. See David T. Zabecki, Steel Wind: Colonel Georg Bruchmuller and the Birth of Modern Artillery, (New York: Praeger, 1994)

21. "Just how sure of victory the French felt behind their Maginot Line was expressed by their Supreme Commander, General [Maurice] Gamelin. In January 1940 he said that "he would be ready to give a billion to the Germans, provided they would do him the favor of taking the initiative in the attack." Frieser, p 26.

22. Frieser, pp 27-29

23. This was, of course, in addition to her strategic alliances with Great Britain and other European powers.

24. One of the reasons suggested for this is because of the underlying Marxist-Leninist philosophy that underwrote the Soviet State which, among other things, privileged a "scientific" view of the world and of its affairs of which military affairs is but a subset.

25. One only needs consider the sheer weight of firepower that the Soviet formations brought to bear on the German defenders in the last stages of the Second World War, particularly in the opening stages of the Battle for Berlin and, more specifically, to the Battle of Seelow Heights. It has been reported that the Soviets unleashed a military force comprising of over half-million soldiers, 3000 tanks and approximately 17,000 artillery pieces. Notice the high number of artillery pieces which suggest the volume and intensity of the firepower that was brought down up on the German Ninth Army, which boasted of approx. 125,000 soldiers, 512 tanks, 584 artillery guns and more than 300 anti-aircraft guns (serving in an anti tank role). For accounts of the Battle for Seelow Heights, see Max Hastings, Armageddon: The Battle for Germany, 1944-45, (New York: Vintage, 2005); Tony Le Tisser, Zhukov of the Order, (New York: Praeger Press, 1996); Earl F. Ziemke, The Battle for Berlin: End of the Third Reich, (New York: Ballantine Books, 1968).

26. For an account of how this process of diffusion of idea, concepts and technologies in the strategic-military context takes place, see Emily O. Goldman &‍ Leslie C. Eliason, Ed., The Diffusion of Military Technology and Ideas, (CT: Stanford Univ. Press, 2003).

27. One way to think of this would be, as the Chinese theorists put it in their discussions on war and its conduct in the Information Age – Information Age Warfare with Chinese characteristics. Here Information Warfare is a thematic which, regardless of its source of origin, remains amenable to being "localized", which is what the phrase "with Chinese characteristics" seems to imply. Similarly, while the moniker of "blitzkrieg" is most commonly applied to German tank and combined-arms warfare, in effect, however, as the war progressed wr find "blitzkrieg" with American characteristics, with British characteristics, with Soviet/ Russian characteristics and so on. Indeed, one often refers to Israeli tank operations during the Arab-Israeli Wars as being "blitzkrieg" with Israeli characteristics.

28. Bunker, "Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI", 1996. Available at http://ssi.armywarcollege.edu/pubs/parameters/articles/96autumn/bunker.htm

29. Andrew F. Krepinevich, Jr., The Military-Technical Revolution: A Preliminary Assessment, (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2002)

30. Robert Tomes, "The Cold War Offset Strategy: Assault Breaker and the Beginning of the RSTA Revolution" in War on the Rocks, Nov. 20, 2014. Available at https://warontherocks.com/2014/11/the-cold-war-offset-strategy-assault-breaker-and-the-beginning-of-the-rsta-revolution/. See also Thomas G. Mahnken, Technology and the American Way of War, (New York: Columbia Univ. Press, 2008), p 130

31. Gen. David G. Perkins, U.S. Army, "Multi-Domain Battle: Driving Change to Win in the Future", in Military Review, July-Aug., 2017. Available at http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2017/Perkins-Multi-Domain-Battle/. See also Sydney J. Freedberg, Jr., "A Wider War: Army Revises Multi-Domain Battle With Air Force Help" in Breaking Defence, Oct. 12, 2017. Available at https://breakingdefense.com/2017/10/a-wider-war-army-revises-multi-domain-battle-after-air-force-input/.

32. Gen. David G. Perkins, Multi-Domain Battle: Joint Combined Arms Concept for the 21st Century, at Association of the United States Army, Nov. 14. 2016. Available at https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms-21st-century

33. Megan Eckstein, "'Multi-Domain Battle' Concept To Increase Integration Across Services, Domains", in USNI News, Oct. 04, 2016. The comment is attributed to Army Gen. David Perkins, commanding general of the U.S. Army Training and Doctrine Command (TRADOC). Available at https://news.usni.org/2016/10/04/multi-domain-battle-concept-increase-integration-across-services-domains

34. Sean D. Carberry, "Officials: DOD must adapt to multi-domain warfare model", in FCW, Oct. 04, 2016. Available at https://fcw.com/articles/2016/10/04/multi-domain-warfare.aspx.

35. It is interesting to note the use of the term "a more complex concept". In some ways it reflects on how the US strategic-military establishment understands its adversary. In other words, there appears to be an underlying assumption that the more complex a concept is, the more difficult it would be for an adversary to fracture or "crack it". In turn, this suggests that those who would think in such terms assume that their adversaries are not necessarily intellectually or even perhaps cognitively equipped to "deconstruct" a complex battle concept.

36. Deputy Secretary of Defense Bob Work, Remarks to the Association of the U.S. Army Annual Convention, Oct. 04, 2016, Washington, DC.

37. Ibid

38. Admiral Harry B. Harris, Jr., Commander, U.S. Pacific Command, "Role of Land Forces In Ensuring Access To Shared Domains", Institute of Land Warfare (ILW) LANPAC Symposium, Sheraton, Waikiki, May 25, 2016. Available at http://www.pacom.mil/Media/Speeches-Testimony/Article/781889/lanpac-symposium-2016-role-of-land-forces-in-ensuring-access-to-shared-domains/. My emphases.

39. Sean D. Carberry, "Officials: DOD must adapt to multi-domain warfare model", in FCW, Oct. 04, 2016. Available at https://fcw.com/articles/2016/10/04/multi-domain-warfare.aspx

40. Ibid. Quote attributed to Gen. David G. Perkins, U.S. Army

41. Jon Harper, "Pentagon Pushing 'Multi-Domain Battle' Concept," National Defense, October

42. 4, 2016, p. 2. Available at http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=2319

43. Considered in operational-tactical terms, my reference to "defensive designs" and "defensive systems" refers to the "battle networks" by means of which a military force engages in combat. As is well-known, such Battle Networks act as the critical infrastructure that sustains and nourishes the conduct of battle. Equally, it is also a critical node by means of which information is transacted along and across the strategic-military establishment.

44. Whyatt Olsen, "PACOM chief urges Pacific Army to master cross-domain warfare" in Stars and Stripes, May 26, 2016. Available at https://www.stripes.com/news/pacific/pacom-chief-urges-pacific-army-to-master-cross-domain-warfare-1.411491. Comment attributed to Adm. Harry Harris (USN), Speech at the Association of the U.S. Army, Honolulu, Hawaii,

45. For a clear and detailed exposition of the "systems of systems" concept see William A. Owens, Lifting the Fog of War, (Boston: Johns Hopkins University Press, 2001).

46. Admiral Samuel J. Locklear III, commander, US Pacific Command, remarks to the National Defense Industrial Association conference, BreakingDefence.com, Nov. 4. Admiral's comment in full was: ""We need to look at it [China's anti-access defense] not as an iron dome but as a block of Swiss cheese that gets more dense as you get closer to the center. ... The way you deal with it is you find the holes in the Swiss cheese and widen them. Those holes in the Swiss cheese ... that's where our ... money ought to go. You've got to buy the things that increase our asymmetric advantage, and we have many, many, many of them. [Everything else], let it go, because we're just throwing money into places that aren't going to make a difference." Available at http://www.airforcemag.com/MagazineArchive/Pages/2013/December%202013/1213verb.aspx See also Steven Stashwick, "The US Army's Answer for an A2/AD Shield in Asia" in The Diplomat, Oct. 15, 2016. Available at https://thediplomat.com/2016/10/the-us-armys-answer-for-an-a2ad-shield-in-asia/

47. Janus is an Ancient Roman god of beginnings, gates, transitions, time, duality, doorways, passages, and endings. He is usually depicted as having two faces, since he looks to the future and to the past. See Varro apud Augustine, De Civitate Dei, VII 9 and 3; Servius Aen. I 449

48. David S. Alberts, The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavours, (Washington, DC: DoD Command and Control Research Program, 2011)

49. Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story", Modern War Institute at West Point, Oct. 27, 2017. Available at https://mwi.usma.edu/road-multi-domain-battle-origin-story/

50. Ibid. My emphasis

***Dr Manabrata Guha** is a distinguished Fellow of the CENJOWS, New Delhi

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: http:// www.cenjows.gov.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/Annualmember 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/ PAN Card/ Iden 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 ……..…….

Place: New Delhi

Date:.....…….....

Director CENJOWS

Note:-

1. Life membership is open for all serving and retired personnel of the Armed Forces, Government Ministries, Academia, members of other think tanks and others interested in studying defence and military strategy.

2. Membership Fees:-

(a)	Life Membership	-	Rs 1500/-
(b)	Annual Membership	-	Rs 300/-

CENJOWS PUBLICATIONS

S No	Title	Author
	Monographs	
1.	Reforming and Restructuring : Higher Defence Organization of India.	Brig (Dr) RK Bhutani (Retd)
2.	Pakistan's Defence Industrial Base: An Overview	Shri R Chandrashekhar
3.	Defence Diplomacy and International Military Co-operation	Lt Gen Vinod Bhatia (Retd) R Adm VS Chaudhari (Retd) Brig Ranjit Singh
4.	J&K Imbroglio: A Comprehensive Approach to Normalcy & Strategy to Deal with Pakistan	Brig Ranjit Singh
5.	Understanding Special Forces, Special Operations, It's Structure & Organisational Imperatives for India's Special Forces in the 21st Century	Col Arvind Sharma
6.	India's Foreign Policy Panchseel to Panchmrit: Changing Paradigms	Col Laxman Singh
7.	Social Media and the Armed Forces	Brig Deepak Malhotra
8.	Gilgit and Baltistan Regions of Jammu and Kashmir State	Shri R Chandrashekhar
9.	The Tibet Autonomous Region	Shri R Chandrashekhar

S No	Title	Author
	Issue Brief	
1.	Pragmatic Approach to Command of Unit.	Brig Ranjit Singh
2.	Exploiting Indian Military Capacity in Outer Space	Gp Capt GD Sharna, VSM (Retd)
3.	Whose Life is it Anyway?	Lt Gen Gautham Moorthy, PVSM, AVSM, VSM (Retd)
4.	Harnessing Social Media by the Indian Armed Forces.	Brig Deepak Malhotra
5.	Countering the Emerging Civil Drone Threat	Gp Capt GD Sharma, VSM (Retd)
6.	Strategic Partnerships-Strengthening India's Defence Manufacturing Base	Shri R Chadnrashekhar
7.	Operationalisation of India's Ballistic Missile Defence	Brig (Dr) Rajeev Kumar Bhutani (Rd)
8.	China Pakistan Economic Corridor: Furthering the Initiative and Progress on Projects	Shri R Chadnrashekhar

S No	Title	Author
	Synodos Paper	
1.	Review of Policy Issues and Organisational Structures: Imperative for Enhancing Defence Cooperation	Brig Ranjit Singh
2.	Should Unorthodox Measures in Counter Terrorist Environment be Allowed to Trump Rules of Engagement?	Lt Gen Gautham Moorthy, PVSM, AVSM, VSM (Retd)
3.	India: A Global Military Training Hub	Brig Ranjit Singh
4.	Aslant Hat: Hitting Below the Belt	Brig Rajiv Kumar Bhutani (Retd)
5.	Defence Reforms-Transforming Indian Military Force to Military Power-Occasional Paper	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
6.	US's Latest South Asia Policy May Not Succeed	Maj Gen Harsha Kakar (Retd)
7.	Looking Beyond Doklam: Is the Army Future Ready?	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
8.	China's Military Reforms & Implications for India	Col C Madhwal
9.	Exploiting Special Operation Forces-Beyond the Surgical Strikes	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
10.	Social Media & the Indian Armed Forces	Maj Gen Bipin Bakshi, VSM
11.	Revisiting India's Afghanistan Policy	Col Laxman Singh
12	Sagarmala-A Game Changer	Capt (IN) Ranjit Seth
13.	Status & Honour Civil-Military Status Equivalence and Pay-Parity Need for Urgent Intervention-Occasional Paper	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
14.	India-Japan: Forging Strategic Partnership	Lt Col Nikhil Kapoor
15.	Chinese Armed Forces: Down five Decades	Pinaki Bhattacharya
16.	Operation Cactus Maldives(Occasional Paper)	Brig SC Joshi, YSM, VSM (Retd)
17.	Quantum Computing and Likely Defence Application	Air Cmde T Chand
18.	Can India Learn from the US National Security Strategy	Maj Gen Harsha Kakar (Retd)
19.	Revisiting Maldives_ India's Military Intervention	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)
20.	CPEC: Fundamental Negative Paradigms	Lt Gen Rameshwar Yadav, PVSM, AVSM, VSM (Retd)