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@cenjows.gov.in

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.

Note : *Views that are recorded are the individual opinions of the writers. CENJOWS doesn't take any responsibility for them.*

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$**

MP BIRLA GROUP
Ghar Banao
Perfect
MP BIRLA GROUP
IS 1489
ISI
(Part I)
MP BIRLA CEMENT
PERFECT
PLUS
ADDITIVES FOR EXTRA STRENGTH
PORTLAND POZZOLANA CEMENT
(Fly ash based)
NET QUANTITY: 50 kg
BIRLA CORPORATION LIMITED
PERFECT PLUS

पिछले पांच दशकों से निरंतर कार्य करते हुए, लाखों लोगों के जीवन को और बेहतर बनाने तथा विद्युत क्षेत्र की संपूर्ण वेल्यू चेन में एक अग्रणी वित्तीय सेवा प्रदाता होने के कारण, हम विद्युत और प्रगति के पर्याय के रूप में, एक ब्रांड बनकर उभरे हैं। वित्तीय वर्ष 2019 की दूसरी तिमाही में हमारा वित्तीय प्रदर्शन हमारी सफलता का प्रमाण है जहां हमने अब तक का सर्वाधिक ₹ 1764 करोड़ का तिमाही लाभ अर्जित किया है। ₹ 32,000 करोड़, से अधिक निवल मूल्य के साथ हम देश-भर में स्थित अपने 25 कार्यालयों द्वारा ग्राहकों के लिए आसान पहुंच सुनिश्चत करते हैं तथा हम अपनी असाधारण सफलता के लिए अपने ग्राहकों तथा देश के लोगों द्वारा दर्शाए गए विश्वास के लिए इनके ऋणी हैं।

आरईसी
REC
असीमित ऊर्जा, अनन्त संभावनाएं
Endless energy. Infinite possibilities.

पूरे भारत में विद्युत उत्पादन, पारेषण और वितरण परियोजनाओं के वित्तपोषण में भागीदार

•फॉर्च्यून इंडिया 58 •गोल्डन पीकॉक अवार्ड •डन एंड ब्रैडस्ट्रीट पीएसयू अवार्ड •सीआईएमएसएमई अवार्ड
•दैनिक जागरण इंडिया प्राइड अवार्ड •एनएसई मार्केट अचीवर अवार्ड

@OfficialREC @reclimited REC Limited पर फॉलो करें

MULTI DOMAIN WARFARE IN THE INDIAN CONTEXT

QMAX
BEYOND QMAX; BEYOND TEST
TRUST THAT
PROTECTS A NATION.

इकाECIL

Self-Reliance in Strategic Electronics

A multi-technology company that provides

Systems and Solutions to Atomic Energy, Defence, Aerospace, Security, Telecommunications IT & e-Governance Sectors

Portfolio

- ❖ Radiation Detectors, Control and Instrumentation Systems, SCADA Systems and Power Electronics Equipment.

- ❖ Electronic Surveillance and Warfare Systems, Command and Control Systems, Radio Communication Equipment and Electronic Fuzes.

- ❖ Antenna Systems, V-SAT Networks, Cockpit Voice Recorders, Inertial sensors and Actuators.

- ❖ Integrated Security Systems, Electronics Jammers and Encryption equipment.

- ❖ Telecommunication equipment, IT and e-Governance solutions.

इलेक्ट्रॉनिक्स कॉरपोरेशन ऑफ इंडिया लिमिटेड
Electronics Corporation of India Limited
A Government of India (Department of Atomic Energy) Enterprise
Hyderabad - 500 062, Telangana

CIN No: U32100TG1967GOI001149
E-mail: cbdgoffice@ecil.co.in
www.ecil.co.in
Telefax: +91 40 27120671

CONTENTS

FOREWORD

Indian Armed Forces have successfully fought well coordinated wars in the past involving the then existing domains. Due to the changing nature of warfare, the dimension and complexities of war fighting domains is now all encompassing. Multi Domain Warfare (MDW) impacts the geostrategic geo-economics and geopolitical spaces as well as geo-technologies. In addition to Land, Sea and Air, domains such as cyber, space, special operations, informational warfare, psychological operations, legal, electromagnetic, hybrid, asymmetric, water, energy and autonomous weapons would also form part of MDW. Ground forces equipped with long range missiles, helicopters, UAVs, electronic warfare systems, cyber capabilities and Special Forces can operate and support operations in other domains. The Armed Forces will continue to remain central to the emerging MDW.

The study of MDW in the Indian Context is relevant and essential and has the potential to closely integrate all elements of India's comprehensive national power. Almost all aspects of the MDW including niche technologies have been studied in detail by subject matter experts and included as articles in this issue. There will be a challenge for commanders who have to handle inter service and multi domain assets and operations These commanders need to be trained over the years by exposure to inter service organisations and specialized weapon systems across domains. Integration and jointness will be imperative while reforms at the higher defence organization and restructuring would be necessary to be operationally effective in MDW.

The MDW concept therefore calls for further introspection and scrutiny. The new Army War Doctrine amplifies this concept, while other Forces too are likely to adopt this. CENJOWS recently published a well researched monograph on MDW and has now dedicated the Feb 2019 issue of the Synergy Journal to this theme. I am sure CENJOWS will usher in a new era of debates and discussions on this important subject leading to greater understanding of the concepts of emerging warfare.

(PS Rajeshwar)
Lt Gen
CISC & Chairman CENJOWS

EDITOR's NOTE

Defence Forces across the world have fought battles in all domains in the past. Due to changing nature of warfare, the numbers and complexities of the war fighting domains is steadily increasing. The necessity of reinventing the concepts of Multi Domain Battle in the present avatar was felt by the US Army for replacing the Air Land and Air Sea Battle concepts. The Multi Domain Warfare (MDW) concept on the other hand is much broader and could be likened to Chinese concept of unrestricted warfare. MDW concept could serve as a broader concept of warfare within which new concepts of employment of weapons would come up. Also newer concepts of design of weapons are likely to evolve to address the threats that conditions of unrestricted warfare may throw up

It is important and relevant to explore the potential and applicability of the MDW concepts in the Indian context. The whole of nation approach would be needed for implementing the concepts as entities under various ministries and departments would be the stake holders. The higher defence organisation needed for the MDW would also be much broad based. The Navy will have its own perspective for the MDW. Similarly the Air Force will reappraise the Air Land and Air Sea battle concept applicability to the MDW. Implementation of this concept would need the study of the role and relevance of special operations. The cyber warfare and information warfare will also play an important role. Space will be a major facilitator of the MDW and its capabilities will need deeper understanding. All these aspects have been amply addressed in this issue of the journal.

Happy Reading

(T Chand)
Air Cmde (Retd)
Senior Fellow & Editor

MULTI-DOMAIN WARFARE: WAGING UNRESTRICTED WARFARE

Dr Manbrata Guha*

Introduction

In 2016, the United States Army initiated the development of the "multi-domain battle" (MBD) concept. While critics and cynics have argued that it is a desperate attempt by the U.S. Army to find relevance for itself in the battlespaces of the Information Age, it has now been progressively adopted by almost all arms of the U.S. military establishment.

While this battle concept was offered as a "difficult to fracture" concept and signaled the gradual demise of the AirLand and AirSea battle concepts, it is, in conceptual terms, not difficult to understand. As has been reported elsewhere, the basic idea is to "synchronize cross-domain fires and manoeuvre in all the domains to achieve physical, temporal and positional advantages."[1] 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."[2] Leaving aside the critical and cynical points of view, the rationale offered is that "[p]otential adversaries are closing the technology gap with the United States and developing strategies to

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

[2] Ibid.

keep U.S. forces at bay."[3] 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."[4]These developments suggest that the key element underwriting the development and adoption of the MDB concept is the conceptualization and design of weapon-systems and capabilities that are unrestricted by the limitations of domains here understood as land, air, sea, and outer space. While this is not a "new" idea *per se*, the novelty of this development should not be lost on us which, counter-intuitively, lies not simply in the projected cross-domain capabilities that are being expounded; rather, the novelty – indeed the uniqueness – lies in the nature of the battlespace that is being presumed that requires such cross-domain capabilities.

In the short essay that follows I will engage with this theme thereby attempting to draw attention to the transformation that is taking place in how we conceptualize the emergent battlespace and some of the implications of the same. I will conclude with some observations on how this impacts the Indian strategic-military architecture and will recommend some ways by which it may adjust to these changing realities.

The Nature of the Emergent Battlespace

If a multi-domain capability is what is being called for, then it is necessary for us to ask: what are the conditions that require such capabilities? In other words, what are the strategic-military conditions that necessitate our thinking in terms of developing a multi-domain capability?

[3] Jon Harper, "Pentagon Pushing 'Multi-Domain Battle' Concept – Blog", Oct. 05, 2016. Available at http://newsmilitary.com/pages/81623199-pentagon-pushing-multi-domain-battle-concept-blog

[4] 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

Publications issued by the U.S. Department of Defence, specifically, from the U.S. Army, suggest a number of points of interest. Thus, for example, it has been asserted that the MDB concept seeks to replace the twin concepts of AirLand and AirSea Battle. This leads us to ask why these latter concepts are now considered defunct and in need of replacement? What changes have occurred in the global strategic commons that renders these twin concepts either obsolete and/ or less-than-optimal? Before we address these questions, it is important to recognize that these two concepts – the AirLand and, to a lesser degree, the AirSea battle concepts - have a lineage that can be verifiably traced to the theories of Maneuver Warfare and to its exhibition during the Second World War.[5] With the advent of the Cold War, however, U.S. and NATO forces found themselves confronting a well-equipped and heavily mechanized Soviet Armed Force in Central Europe, which led to the creation and adoption of the AirLandbattle concept. The AirLand battle concept was specifically designed, in part, to attack and interdict the heavy tank and mechanized armies that the Soviets were expected to field in the event of a massed Soviet attempt to dominate and wrest control of Western Europe. The basic objective, put simply, was to achieve a high degree of co-ordination between the Air and Land Forces, not simply in tactical terms – as the German armies had demonstrated, particularly in the initial stages of the Second World War – but also at the operational level thereby thwarting and negating the heavy asymmetry in terms of numbers and firepower that the Soviet forces at the time

[5] Note that the AirSea battle concept emerged in the 2009-2010 timeframe and was more geared to address the U.S. strategic-military posture in the Western Pacific theatre. See Jan van Tol, Mark Gunzinger, Andrew F. Krepinevich, Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept*, Future Warfare and Concepts, CSBA Online, Available at https://csbaonline.org/research/publications/airsea-battle-concept/. The rationale for pairing the AirSea battle concept with the AirLand battle concept is because the former concept takes the "design principles" of the latter concept and applies it to the Western Pacific theatre with specific reference to particular scenarios, for example, the defence of Taiwan and addressing the Anti-Access/ Area Denial strategy that China is said to be constructing.

were deemed to have enjoyed over their NATO counterparts.

Much, however, has changed in the intervening years. With the collapse of the Soviet Union in 1989, and with the failure to reap the benefits of the so-called "peace-dividend" and the "swords to ploughshares" paradigms, the world, in the interim, has segued into a condition marked by the sudden and unexpected eruption of violent insurgencies which are not simply local in nature, but which are also often planetary in scale.[6] In addition to this, regional powers have begun to flex their muscles and have made concerted attempts to modernize and upgrade their conventional forces and to acquire weapons of mass destruction, which has also led to the fracturing of what was once proclaimed as "the New World Order". Further, the Age of Information has rendered the borders of nation-states more porous than ever before. Ideas and technologies have begun to virally proliferate empowering individuals and groups regardless of the limitations of time and space, and of national borders. Indeed, in some quarters, there are growing concerns that the very concept of the nation-state is under threat.[7]When coupled with a seemingly unending series of major and minor economic shocks that have wracked the world-at-large, and unprecedented movements of populations driven from their homelands by either devastating climatic changes or instances of extremely violent ethnic

[6] As the USSR collapsed, this assessment was also made by the CIA though the extent and the significance of this recognition may not have been widely appreciated at the time. As James Woolsey, President Clinton's nominee for the CIA Directorship, in his Senate confirmation hearing said: "Yes, we have slain a dragon…but now we live in a jungle filled with poisonous snakes. And in many ways, the dragon was easier to keep track of." See Neil A. Lewis, "Bigger Battle Expected on Spy Budget," *The New York Times*, Feb 01, 1993.

[7] See, for example, R. Rotberg, "The Failure and Collapse of Nation-States: Breakdown, Prevention, and Repair", in *When States Fail: Causes and Consequences*, (Princeton: Princeton University Press, 2003)ch. 1. See also, Rana Dasgupta, The demise of the nation state, in The Guardian, April 05, 2018. Available at https://www.theguardian.com/news/2018/apr/05/demise-of-the-nation-state-rana-dasgupta

actions, it would not be incorrect to suggest that traditional strategic-military paradigms are in dire need of a critical re-evaluation. It is in this context that the MDB concept assumes importance and assertions that concepts like the AirLand and AirSea battle may have passed their prime appear increasingly plausible.

The emergence of the MDB concept signals that such changes are being recognized and are being taken very seriously by the U.S. strategic-military establishment. It is also indicative of how the U.S. strategic-military establishment is re-evaluating the nature of "the emergent adversary". Thus, as noted earlier, it has been observed 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."[8] This is an intriguing observation and warrants our attention.

In the first instance, this observation suggests that the traditional advantages that the world's foremost military has enjoyed, namely, the leveraging of high-technology, superiority of firepower, and well-trained combat personnel, particularly in the context of a close-in battle, and the ability to wage war, if required, beyond visual range are being gradually eroded as the emergent adversary seeks battle at flexible ranges of its own choosing. Secondly, it has also been observed that "separatist forces [are gaining] air superiority via the land, without even an air force…" This suggests, among other things, that the emergent adversary is becoming increasingly proficient in leveraging what are often "commercially-off-the-shelf" (COTS) technologies to achieve effects that are disproportionate to their size and capability. Thirdly, it has been asserted that the AirLand

[8] 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

(and, by extension, the AirSea) battle concept has lost its lustre. This is obliquely indicated by the observation that the need of the hour is to develop a "difficult to fracture" battle concept. In other words, it is being asserted that the AirLand (and the AirSea) battle concept is now in danger of "being fractured". But what leads to this assertion? In light of the gradual transformations that are taking place within the global strategic commons, it would not be incorrect to conclude that the utility of the weapon-systems that have thus far constituted the major portion of the arsenals of the major global powers are finding themselves falling short. From this it follows, and it would not be unwarranted to conclude - even if provisionally – that the battle concepts crafted on and around the capabilities of such weapon-systems are consequently falling short and, in some cases, are even being rendered obsolete. Thus, despite the apparently dazzling victories achieved by the Allied Forces in the Gulf War of 1990-91 and the Iraq War of 2003 wherein, allegedly, the AirLand Battle concept was employed with success, there is a growing assessment that traditional weapon-systems and the doctrines associated with their use are being undermined by the advent of what some have referred to as "the wars of the small and the many".[9] One stark instance of this was the so-called First Battle of Mogadishu (Oct 3-4, 1993), where a Somalian militia group fought an elite U.S. force comprising of Rangers and Special Forces and compelled them to withdraw after inflicting significant damage. Of course, subsequent to those events, the world has also witnessed a rash of hyper-violent attacks on not only the U.S but also other nation-states such as India, the UK, among others, which have been launched by small bands of highly motivated individuals – acting either singly and/ or in concert - across time and space, which have rendered the complex high-technology defensive systems of

[9] See, for example, T.X. Hammes, "The Future of Warfare: Small, Many, Smart vs. Few & Exquisite?", *War on the Rocks*, Texas National Security Network, Univ. of Texas, July 16, 2014. Available at https://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite/

these nation-states helpless to thwart such attacks.[10]And, last but not the least, it has also been assessed – and with good reason – that emergent adversarial forces have begun to acquire a growing expertise to adopt and employ cyber-centric weapons. These "new age" weapons are not necessarily destructive, though under some circumstances – particularly when targeting sensitive civilian infrastructure – they can be so; rather, the most effective use of these emergent weapon-systems and capabilities is to inflict a debilitating effect by impacting the cognitive capability of the target and its home population.[11]While one of the more conventional examples, as the documentation on the MDB concept itself suggests, is "to gain air superiority via the land, without even an air force", another, more insidious, example is the alleged Russian cyber offensive conducted against the U.S. in 2016-17. It has been argued that this concerted Russian offensive, which was launched mainly through online means, has given rise to a sense of uncertainty within the U.S. "homeland" by propounding the notion of "fake news" and which, allegedly, played a major role during the 2016 U.S. Presidential elections.[12]It may have

[10] I am, of course referring to the September 11, 2001 attacks on the World Trade Center in New York City and the November 26, 2008 attacks in Mumbai which left thousands dead and injured. It has become fashionable in some quarters to consider such attacks as being "one-off" events. Such a perspective tragically misunderstands the nature of such attacks and the emergent form of warfare that they herald. One of the most under-appreciated consequences of such attacks is that they have been able to transform the "security-climate" of nation-states, which has resulted in the creation and institution of security protocols which, some allege, undermine the very foundations of free and democratic societies. In this sense, these and similar attacks may be considered to be highly effective "effects-based operations"!

[11] See footnote 10.

[12] See, for example, Ewen MacAskill, "US and UK blame Russia for 'malicious' cyber-offensive", in *The Guardian*, April 17, 2018. Available at https://www.theguardian.com/technology/2018/apr/16/us-and-uk-blame-russia-for-malicious-cyber-offensive. It should be noted that this is not a one-sided affair. Equally, the U.S. has retaliated by launching its own offensive. See, for example, Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections", in *The New York Times*, Oct. 23, 2018. Available at https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

also served as a feint to distract attention from Russian intentions in the Ukraine and in the Black Sea Basin.[13]It is easy to dismiss these operations as being simply instances of "cyber-centric" operations. To do so, however, would be to not only underestimate the import of such operations, but also to misunderstand the larger strategic-level concept of multi-domain warfare, which subsumes the MDB concept.

Assessments like these have led the U.S. strategic-military establishment to conclude that the emergent security environment"*will require all the services to exert influence in non-traditional domains*."[14] Consequently, it is argued that "the multi-domain battle construct will require the U.S. Defense Department to rethink how its forces are organized, trained and equipped."[15]

None of the above, however, should suggest that future wars will only be fought between nation-states and non-state actors and that inter-state wars will not take place. Instead, what we have alluded to above only serves to expand the envelope of future forms of war in which inter-state wars will constitute only one part of the full spectrum of war. Indeed, it may also be the case that nation-states, when faced with adversaries who bring to battle an overwhelming war-waging capability in terms of firepower, technology and quality of fighting forces, may

[13] For an overview of Russian strategic moves in the Black Sea Region see "Black Sea's Back, Alright? A New Special Series", Available at War on the Rocks, Texas National Security Network, Univ. of Texas, July 26, 2018. Available at https://warontherocks.com/2018/07/black-seas-back-alright-a-new-special-series/

[14] 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 emphasis.

[15] 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

disperse their own more modest combat elements and masquerade as an unstructured fighting force, and will employ any and all means to wage war. It is in this context that it is necessary for us to revisit the concept of “unrestricted warfare”, which was first articulated – allegedly unofficially – by two Chinese military officers.[16]

In their curiously titled publication, “Unrestricted Warfare”, the two Chinese officers assert that “…war itself has now been changed…it can no longer be carried out in the ways with which we are familiar…war will no longer be what it was originally…the metamorphosis of warfare will have a more complex backdrop.”[17]Thus, they claim

> *Warfare which transcends all boundaries and limits, [is], in short: unrestricted warfare…*this kind of war means that all means will be in readiness, that information will be omnipresent, and *the battlefield will be everywhere*. It means that *all weapons and technologies can be superimposed at will*, it means that all boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed and *it also means that many of the current principles of combat will be modified, and even that the rules of war may need to be rewritten*.[18]

Aside from observing the uncanny overlap of these postulations, which were made in 1999, with the core tenets of the MDB concept, we should also pay careful attention to the assertion that “all weapons and technologies can be superimposed at will” and, further, to the conclusion that the authors draw, which leads them to state that “the rules of war

[16] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization*, [Chaoxianzhan - dui quanqiuhuashidaizhanzhengyuzhanfa de xiangding], (Beijing: Peoples Liberation Army Arts Publishers, Feb., 1999). For a brief background to this text, see https://fas.org/nuke/guide/china/doctrine/unresw1.htm.Various translations and publications of this text has been made over the years including that by the US FBIS, which is available at http://www.c4i.org/unrestricted.pdf

[17] *Unrestricted Warfare*, p 4-6

[18] Ibid., p 12. Emphasis mine.

may need to be rewritten". When considered in this light, the MDB concept may be considered to be, at best, a tentative first step in the process by which "the rules of war" are being rewritten. But this revision is happening in a specific manner. Again, the two Chinese authors give us some additional hints. For example, they state that there are "two broad types of combat conditions, which they list as "Fighting the Fight that Fits One's Weapons" and "Making Weapons to Fit the Fight".[19] This distinction, according to the authors, "reflects the involuntary or passive adaptation of the relationship between man to weapons and tactics."[20] What the authors are attempting to draw our attention to is the important fact that "only after one first has a weapon does one begin to formulate tactics to match it. With weapons coming first, followed by tactics, the evolution of weapons has a decisive constraining effect on the evolution of tactics."[21] One can immediate see how this strain of thought may be co-related to the strategic intent of the MDB concept. Thus, for example, as we have seen above, the aim driving the MDB concept is to "move beyond the mere synchronization of joint capabilities to the complete integration of capabilities", which will allow, for example, "anti-air capabilities…coming froma… submarine or anti-ship cruise missiles might be coming from an Army unit on the ground."Thus, as my co-author and I have observed elsewhere,

> When considered in the context of the MDB concept, we can see how an attempt is currently being made to break out of this bind… particularly with reference to the efforts of the U.S. Army, there is a growing intent to take weapon-systems out of their traditional and domain-specific operational contexts and to employ them in innovative and, potentially, unexpected ways.[22]

[19] Ibid., p 19. See also Manabrata Guha & David Galbreath, *The Multi-Domain Battle Concept: A Preliminary Assessment*, CENJOWS Research Monograph, Center for Joint Warfare Studies, HQ IDS, New Delhi, India, Oct. 2018, p 30

[20] Ibid

[21] Ibid.

[22] Manabrata Guha & David Galbreath, *The Multi-Domain Battle Concept: A Preliminary Assessment*, CENJOWS Research Monograph, Center for Joint Warfare Studies, HQ IDS, New Delhi, India, Oct. 2018, p30

Nevertheless, it is also important to be sensitive to the fact that such efforts still “remain ensconced within a cognitive framework that is heavily dominated by individual weapon-systems which guide tactical and operational considerations.”[23] But it also behoves us to recognize that this trajectory can only move in a direction that leads to a blurring of the link between “man to weapons and tactics” thereby enabling, in time, the transcending of the limitations that individual weapon-systems have traditionally imposed on tactics and doctrines. This, in turn, will lead to conditions wherein, in the words of the two Chinese military officers, “everything that can benefit mankind can also harm him. This is to say that *there is nothing in the world today that cannot become a weapon*, and this requires that our understanding of weapons must have an awareness that breaks through all boundaries.”[24] In the more immediate context of the MDB concept, it is important to note that the underlying intent is to, in the words of the authors of “Unrestricted Warfare”, eventually “mak[e] Weapons to Fit the Fight”. In other words, the MDB concept may be considered to be a pathway by which combat forces of the future will weaponize themselves relative to the contingency that they are tasked to address rather than attempting to address the contingency with the arms at their disposal.

It would, therefore, not be incorrect to suggest that with the introduction of the MDB concept, what we are witnessing is nothing less than the initial and exploratory efforts by which the current generation of weapon-systems and capabilities are being reconfigured and, in some instances, being reimagined to be used in contexts for they have not been originally designed. The next most likely stage of this development process will involve the design of weapon-systems and capabilities that have a multi-domain use, that is to say, newer generations of weapon-systems will be flexible enough - and modular in nature - such that they can be used across domains (namely, land, air, sea, space,

[23] Ibid.

[24] Ibid. p31;*Unrestricted Warfare*, p 25

the electro-magnetic spectrum and cyberspace). As this development process further unfolds, we can also expect to see transformations in the evolution of tactics, strategies and of doctrines. Indeed, we can also expect that such transformations will also trigger radically different processes by which combat personnel are recruited and trained.

In effect, therefore, the MDB concept may be considered to be not simply an innovation in the design and operationalization of weapon-systems and of related capabilities; it may also be considered to be a signature of the transformation of war.

The MDB concept: Considerations for India

In many ways - though the fact remains under-recognized and under-appreciated - India has been at the forefront of contending with the transformation of war. In addition to being faced with two geo-strategic threats across her western and northern borders, the Indian strategic-security establishment has had to – since 1947 – deal with fissiparous elements, armed insurgencies and terrorism that have threatened to fracture and disintegrate the Indian Union. Till date, the Indian strategic-security establishment has been able to address these challenges though often the cost to security personnel and civilians has been high. However, if we are to take the prognosis of the two Chinese military officers referenced above seriously, then there is a growing imperative to think in terms of an “age of unrestricted warfare” wherein the need to design and develop multi-domain combat capabilities becomes an urgent necessity.

India’s strategic-security imperative demands that it maintains a sizeable conventional armed force in addition to a credible nuclear deterrent force, including a robust second-strike capability. This is necessary to present conventionally-oriented would-be aggressors from across her western and northern borders with a sufficiently effective deterrent force. But, at the same time, to assume that these threats will culminate in only a conventional battle would be a strategic error. Indeed, there is a plausible argument to be made that in the event of intensive and extended hostilities breaking out over and across India's western and/ or northern borders, the battlespace will not remain conventional.[25] India's adversaries can be expected to employ any and all means possible to disadvantage India tactically, operationally, and strategically.[26] Thus, it is likely – even probable – that the emergent battlespaces that the Indian Armed Forces will find itself involved in going forward will not be simply conventional (including the potential use of WMD) in nature and character. When considered in this light, it evident that to prepare for such an eventuality, the conventional (including nuclear) elements, which currently constitute a major proportion of India's defensive capability, will form only one part of the comprehensive Indian strategic-military profile. Thus, an urgent reconfiguration is necessary and the first steps must involve experimenting with the development of weapon-systems – kinetic and non-kinetic - that can target and/ or interdict adversarial systems across domains.

There are at least two benefits that will accrue if such a course of action is undertaken. First, it will hasten the integration of different elements of the Indian Armed Forces. Already such moves are afoot with the gradual creation of Integrated Battle Groups, which aim to bring together all arms of the Indian Armed Forces into a tightly knit combat force that is capable of presenting an aggressor with a comprehensive

[25] My use of the word "conventional" here includes the possession and use of weapons of mass destruction.

[26] Take, for example, the Kargil War (1999) and the Mumbai Attacks of 2008. While these two events are commonly seen as independent events, consider, however, a scenario wherein these two events could have been subsets of a comprehensive campaign to destabilize the Indian defensive posture as a prelude for a concerted offensive across either of the Indian fronts (northern and western). Additionally, also consider the possibility that preparatory attacks launched through a well thought out cyber campaign could serve to not simply interdict India's military and civilian infrastructure, but also to – in a manner similar to the alleged Russian campaign unleashed against the U.S. in 2016 – undermine public confidence in both the government and the military.

combat challenge. Care, however, must be taken that the notion of “integration” is not misinterpreted in terms of a “combined arms” combat capability. True integration requires a multi-domain capability exercised by all components of the envisaged Battle Group. This requires, at the minimum, that the service-centric identities of the elements that comprise such Integrated Battle Groups be subsumed (but not effaced) within such fighting units. This will require not simply a high degree of co-ordination between the elements comprising such battle groups, it will also require innovative training and doctrinal models whereby the constituents of such battle groups are melded into a full-spectrum war-fighting entity. It should also be mentioned that such capabilities should not be limited to the use of kinetic weapon-systems; they should also include the ability to leverage the cyber and electromagnetic domains. The key objective of developing such a capability will be to leverage the advantages that these specific domains offer and the ways by which they can augment the more traditional kinetic weapon-systems. Indeed, it can be argued with some justification that future design of such weapon-systems should have such exploitative capabilities built into them natively.

The second advantage that will accrue to such an initiative will be in the arena of defence R&D and production. If weapon-systems are designed and manufactured to operate across domains then, while the initial R&D costs may appear high, the consequent payoffs may be realized in their cross-spectrum use. In other words, unlike how weapon-systems, which cater to specific service requirements, are designed and operated today, multi-domain weapon-systems can be (rather, should be) usable by any element of the Indian Armed Forces. This will bring about a reduction in problems associated with logistics and, given the training and doctrinal convergence that will be necessary to effectively operate such systems, it would also bring about a more deep-rooted integration than before. In this context, an additional underlying advantage will accrue if this path is chosen. For emergent weapon-systems to be truly multi-domain in nature, the concept and design phase of such weapon-systems will necessarily have to include multiple cross-domain operational and tactical inputs, which can be engineered not post-factum, but in the R&D phase itself. As a consequence, frontline combat elements will be able to design operations and tactics with much greater freedom than is the case under current conditions wherein operations and tactics are bound, in a manner of speaking, to the physics and chemistry of the weapon-systems. In this way, the Indian Armed Forces will be able enjoy the benefits of employing "Weapons [that] Fit the Fight" rather than "Fighting the Fight that Fits One's Weapons".

Additionally, it is vitally important to keep in mind that the notion of a multi-domain capability cannot be only restricted to the conventional battlespace. As we have seen, if it is indeed the case that we are segueing into an age of what the two Chinese military officers referenced above referred to as "unrestricted warfare", then it would not be misplaced to assume that "the battlefield will be everywhere". The implication of this is immense. It suggests that "all boundaries lying between the two worlds of war and non-war, of military and non-military, will be totally destroyed." And, if this is indeed the direction that the global strategic common is hurtling towards, then it becomes a strategic-security imperative for Indian strategy planners and managers to prepare the grounds from which such a state of affairs may be addressed. The Indian strategic-security establishment will have to begin thinking in radically different terms and not be held hostage by either a traditionally-crafted notion of the conventional battlespace or by the dictates of geography or, indeed, of specific domains. Indeed, they must look to identify ways and means by which they can leverage every possible means to enhance the Indian strategic capability across domains.[27] Above all, planners and managers of the Indian strategic-security establishment must recognize that even more vital than the commonplace notion of the battlespace is the cognitive battlespace, which is where - as history has repeatedly shown us - battles and wars are won and lost. Waging war in the cognitive

[27] By "domains" here I am implicating the geographical and non-geographical domains which include cyberspace, the electro-magnetic spectrum *and* the bio-neurological domains.

battlespace may, at first glance, appear to be a jargon-ridden formulation. If understood in this way, the disservice to the Indian polity would be grave for waging war in the cognitive battlespace involves nothing less than the manipulation of "truth" and the distortion of the perceptive/ cognitive capabilities of an adversary. As can be imagined, the level of effort and co-ordination required to develop and refine such capabilities will be immense. This is not simply a case of undermining the will and morale of an adversary. Rather, it involves provoking an adversary to construe reality in a way that is conducive to Indian strategic-security purposes. This applies as much at the strategic level as it does at the operational and tactical levels. This calls for a fundamental re-adjustment of how we think about war and about the domains within which war has been traditionally conceptualized and waged. It also calls for a revamping of the modes of defence production as it will involve planners and tacticians to be intimately involved in the defence R&D and production process.

Conclusion

If viewed in this way, the MDB concept appears to be much more than simply a fad or a buzzword. It is a signature of a radical transformation underway in Western, primarily U.S., military circles and represents a serious effort to come to grips with a shifting strategic landscape. As we have seen, it is a concerted move to change how we think about war by blurring the service-specific lines that demarcate the traditional arms of a fighting force. Of course, it goes without saying that such an exercise is fraught with danger. This is not only because what is being proposed – at least conceptually – is a radical rethinking of how future combat forces will wage war, it also implicates the very structure of the strategic-military establishment. In this sense, the conceptualization and operationalization of the MDB concept is a dangerous affair, but it is one that is fast becoming an unavoidable imperative.

For India, without the deep technological and financial advantages enjoyed by the U.S. strategic-military establishment, and given her existent strategic-military imperatives – both external and internal – the matter is an even more delicate one. However, as in the case of the U.S., it is also a strategic imperative for the Indian strategic-military establishment to be acutely responsive to these developments. The need of the hour is not simply to copy the developments in the U.S. Instead, Indian strategic planners need to take the core ideas underwriting emergent concepts like the MBD concept and to rethink them in a manner that is relevant and applicable to India. To not do so would be, in the estimation of this author, a grave error. Indian strategic planners must exercise their creativity and local insights and refashion the ways and means by which Indian strategic interests are best served and extended in an age of unrestricted warfare.

***Dr Manbrata Guha** is a Distinguished Fellow of the CENJOWS and Research Associate, Univ. of New South Wales @ the Australian Defence Forces Academy, Canberra, Australia

MULTI-DOMAIN WARFARE IN INDIAN CONTEXT: A FEW THOUGHTS

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

"Future conflicts will be characterised by operating in a zone of ambiguity where nations are neither at peace nor at war a 'Grey Zone' which makes our task more complex. Wars will be Hybrid in nature, a blend of conventional and unconventional, with the focus increasingly shifting to multi domain Warfare varying from non-contact to contact warfare."-Indian Army Land Warfare Doctrine 2018.

India Tryst with Multi-Domain Warfare

On 13 June 1971, an article in the UK's Sunday Times exposed the brutality of Pakistan's suppression of the Bangladeshi uprising. It changed history. Anthony Mascaren has, a Goa born Pakistani reporter exposed for the first time the scale of the Pakistan army's brutal campaign to suppress its breakaway Eastern province in 1971. Prime Minister Indira Gandhi told the then editor of the Sunday Times, Harold Evans, that the article had shocked her so deeply it had set her "on a campaign of personal diplomacy in the European capitals and Moscow to prepare the ground for India's armed intervention,"[1]Preparing favourable international public opinion and explaining India's position was the aim of tours. Signing of 'Treaty of Peace, Friendship and Co-operation'

[1] https://www.bbc.com/news/world-asia-16207201 Bangladesh war: The article that changed historyBy Mark Dummett, BBC News 16 December 2011 accessed on December 22, 2018.

on August 09, 1971 between India and Soviet Union were a part of well-orchestrated multi-domain efforts that eventually led to creation of Republic of Bangladesh after a military victory. A lesser talked about feature of the military victory was the synergy achieved between the Mukti Bahini operating in the lower spectrum and the conventional ground, maritime and air forces.

"You can do a lot with diplomacy but of course, you can do a lot more with diplomacy backed up with firmness and force" said Kofi Annan on July 26, 1999, the day successful completion of Operation Vijay was declared, India's fourth war with Pakistan. Operation Vijay was a perfect blend of strong and determined political, military and diplomatic actions which enabled us to transform an adverse situation into a military and diplomatic victory.[2]Electronic intercepts of conversation between Pakistani COAS visiting Beijing and his CGS in Islamabad unfolded a well-choreographed media campaign and virtually brought war to the living rooms. Interacting political, diplomatic, ground and air forces brought to fore maturity of India's strategic scheming.

Portending Future Conflicts

Multi Domain Warfare (MDW) is essentially all encompassing and impacts the geostrategic, geo-economics and geopolitical space. In brief, the essential components are cyber, space and outer space, special operations, informational warfare, psychological operations, legal, electronic, electromagnetic, hybrid, asymmetric, water, energy, autonomous weapons and vehicles including drones, fuelling unrest.[3]Conflicts in the coming years are most likely to witness all elements of national power being brought into effect to achieve political objectives by the adversaries. The militaries in the neighbourhood are already focussed on developing strategic systems, conventional capacity and asymmetric capabilities.

[2] https://mea.gov.in/articles-in-indian-media.htm?dtl/14821/Kargil+where+defence+met+diplomacy Kargil: where defence met diplomacy By V P Malik July 25, 2002 accessed on December 22, 2018

[3] CEJOWS Concept Note: Multi Domain Warfare in the Indian Context

PLA is engaged in forging the ‘Assassin’s Mace’ (Shashoujian) through unique weapons to defeat a stronger enemy and informationisation.[4]Their doctrinal orientation is to employ combat disruptive technologies and exploit the information domain. Information dominance is likely to be achieved through a combination of space, network and electronic ascendency as a precursor or in tandem with military operations. ‘Three Warfares’ strategy of shaping the public opinion, conducting psychological and legal warfare is likely to be prosecuted with finesse. Noted academic Michael Clarke, of the Australian National University has identified the elements of ‘Three Warfare’ thus, “Psychological warfare centred on ‘disseminating particular information via various channels’ to influence or disrupt an adversary’s decision-making capacities and foster doubt about capabilities in such a way that will to act is degraded. Public opinion warfare is geared to influence both domestic and international public opinion to support Chinese objectives and dissuade adversaries from pursuing contrary actions. Legal warfare involves the exploitation of international and domestic legal systems to claim the legal high ground, assert the legitimacy of Chinese claims and constrain an adversary’s operational freedom.”[5]The PLA has existing computer and network attack missions which has been combined with Electronic Warfare into an Integrated Network Electronic Warfare (INEW) activity. Specialised IW militia have also been organised to support operational activity. The Strategic Support Force is expected to further consolidate PLA’s cyber, information as well as possibly support the ‘Three Warfares Strategy’. The Sustained surveillance along all the borders, creating depth through anti access and area denial capabilities along with projecting power in shallow depths both on land and maritime frontiers are the essential elements of their thought process.

[4] Assassin’s Mace: A Chinese Game Changer. Col Saif Ul Islam Khan. Vij Books India Pvt Ltd. New Delhi 2015. P 12.

[5] Michael Clarke, ANU. ‘China’s ‘Three Warfares’ in Xinjiang’. Available at http://www.eastasiaforum.org/2017/11/27/chinas-three-warfares-in-xinjiang/ Accessed on 21 December 2018.

Pakistan has demonstrated through the history that it has employed ‘Limited Aims or Fait Accompli’ strategy to achieve her political and military objectives while waging conventional war against India. This has been in line with hypothesis of TV Paul in his book, “Asymmetric Conflicts: War Initiation by Weaker Powers”.[6] Prosecution of War including Proxy War by Pakistan follows the broad contours of ‘Total Strategy that demands preparation and application of total National power and military instrument is one of its instruments’.[7]Total war or ‘Jehad’ is waged at political, economic, social, psychological, domestic, moral and spiritual levels to achieve objects of policy.

A concerted effort is being made by our adversaries to shrink the space for conventional wars, through prosecution of unconventional operations at the lower end of the spectrum and threats of early and irrational use of nuclear weapons at the other.[8]

The advancement in technology in space, electronic, electromagnetic and cyber domains has some defining features. First, technology is becoming cheaper and its transference is comparatively easier than yesteryears. The internet including the darknet abets espionage and transference. Second, the competence in new age cyber skills is unrestricted across geographies, cultures and economies. Analysis of cyber-attacks brings out that their origin and targets are transnational without prejudice to state of development or progress of the countries. It has been taken advantage of by non-state actors, proxies of big powers and Corporations. Third, social media, mobile, analytics, cloud computing and internet of things (SMACT) has made spreading disinformation or hoaxes easy. The world is grappling with the challenge of ‘Fake News’ on the one hand and manipulation of perceptions on the other using Social Media. Fourth, availability of access to systems and

[6] T V Paul, Asymmetric Conflicts: War initiation by Weaker Powers, (London, Cambridge University Press)pp 35

[7] Brig SK Malik, Quarinc Concept of War, (Adam Publishers and Distributors, Shandar Market, Chitli Qabar, Delhi 110006) pp 54

[8] Indian Army Land Warfare Doctrine-2018

technologies are being offered as a package by big powers to those who join their efforts to spread their influence and reach. A case in point is Pakistan being granted access to Beidou satellite system allowing precise guidance to missiles, ships and aircrafts. Joint development of JF -17 aircraft, its radar, navigation systems portents and substantiates that state of art technologies will be available to Pakistan for doing Beijing's beckoning.[9] Fifth, the economic integration and interdependence while bringing mutually beneficial prosperity also carries the dangers of trade wars and economic manipulation. Sixth, powers transferring highly sophisticated equipment and technologies have the ability to manipulate, alter or restrict the capabilities of systems in a crisis depending upon their orientation and national aims. World over, fears are expressed about electronic systems produced in China and deployed elsewhere being manipulated by them in a crisis situation.

It would thus be inferred that peer competition is getting complex. It may be imprudent to assume that technological edge enjoyed by one cannot be matched by the adversary. It can be acquired through alliances or as quid pro quo for economic concessions. The world has seen asymmetry being used by a lesser adversary as an instrument to win as much as by the superior having a distinct edge in technology and systems. 'Multi-Domain Battles assumes that any superiority will only be temporary and short lived. The term often used to describe this situation is "windows of superiority" and the assumption is that these windows might be abruptly shut by the enemy at any minute. However, in today's context, it is an important observation and might need to be restated after all these years of counter-insurgency warfare.'[10]

[9] https://economictimes.indiatimes.com/news/defence/chinas-belt-and-road-plan-in-pakistan-takes-a-military-turn/articleshow/67173327.cms Chinas' Belt and Road plan in Pakistan Takes a Military Turn, Economic Times December 21, 2018

[10] https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/Commentary: Multi-Domain Battle: AirLand Battle, Once More, with FeelingShmuel ShmuelJune 20, 2017

Strategizing Application of Comprehensive National Power

Kautilya advocated convergence between diplomacy and warfare and use of all means of political influence (four upayas)-*sama* (conciliation or diplomacy, *dama* (economic gratification), *danda* (use of force) and *bheda* (dissension or information operations) to achieve the end state resonates with use of all elements of national power.[11]

Application of power across two or more domains makes a conflict multi-domain. A States' actions in terms of means employed can be differentiated by classifying these as 'Kinetic' or 'Non-Kinetic.' Kinetic component would include spectrum ranging from space weapons, nuclear, biological, chemical options, land, maritime, air or special forces, irregulars carrying out sabotage and other violent actions. Non-Kinetic would incorporate political and diplomatic actions; information operations including shaping of opinions and disruption of critical infrastructure; economic war in all its dimensions, ideological and all such actions which are non-violent.[12]

Russians have been particularly successful in converging different elements of national power in their pursuit of objectives in Estonia, Georgia and Ukraine. Estonia was a case where political, diplomatic and cyber domains were brought into effect to convey message not to cross the 'red lines.' In Georgia, proxies were used to prepare ground for short and sharp military action to bring it firmly under Russian influence. In both cases minimum condemnations by international community were voiced.[13] Russia's mastery of the cyber domain and aptness to exploit internal fissures backed where required with precise application of kinetic forces in quick time has made the world take notice of General Gerasimov's non-linear war.

[11] 'Contextualising Hybrid Warfare' byVikrant Deshpande and Shibani Mehta, Hybrid Warfare- The Changing Character of Conflict, Ed Vikrant Deshpande, IDSA, Pentagon Press pp33

[12] Op cite

[13] Russia and Hybrid Warfare- Aman Saberwal, Hybrid Warfare- The Changing Character of Conflict, Ed Vikrant Deshpande, IDSA, Pentagon Press pp70

Closer home, Pakistan having failed time and again to achieve its objectives through conventional wars has resorted to sub-conventional operations first in Punjab and later in J &K. She has resorted to pan India terror strikes when opportunity presented itself. With change in political and international climate the colour of operations in J & K has also changed. Proxy war has been pursued relentless with means varying from economic (hawala funding, circulation of fake currency, subverting border trade), to kinetic means by employing terrorists and through information operations to shape the public opinion at home, in J & K and of international community. Diplomatic manoeuvring has been the corner stone which has seen a few successes. To combat the same India too has acted in various domains namely, political, diplomatic, economic, information and military. The last one has received prominence but closer look reveals the work in progress in other domains as well.

Military Dimension of Multi-Domain Warfare

The Armed Forces individually and collectively operate across domains even now. Army operates primarily on the ground but flies' helicopters and UAVs. It has airborne and heliborne forces that use aerial medium to undertake operations on ground. The Air Force operates in air but bases its aircraft, air defence assets, command centres and other facilities on ground. The Navy operates at sea having three-dimensional capability of undersea, surface and aerial operations with its own aircraft and UAVs. Its amphibious force is trained to operate at land from ships. All three services draw intelligence inputs from space-based satellites, exploit electronic spectrum and are taking first steps in the cyber domain to further operations. Collaboration across domains within a service is the norm and intrinsic to warfighting. Collaborative operations amongst services across domains is possible like an Army Aviation helicopter directing an airstrike by AF aircrafts against a threat or similar collaboration at sea between Naval and AF assets. There is no single domain force and the domains of warfare (air, land, sea, space, and cyberspace) are not new. The challenge is to exploit the opportunities through joint and integrated conduct of operations to achieve military and political victory.

The US thought on multi-domain warfare advocates integrating and synchronizing joint capabilities to create temporary windows of superiority across multiple domains and throughout the depth of the battlefield to seize, retain, and exploit the initiative and achieve military objectives.[14] This should be the aim though may not be possible in the present Indian context to be fully executed.

Ground forces with inventory of long-range missiles that can be employed against aerial and land targets, helicopters, UAVs, Electronic Warfare systems, cyber capabilities and highly trained Special Forces can operate and support operations in other domains. These capabilities transform Army into active partner in the multi-domain battles. With support from other interacting domains ground forces will have greater capability of manoeuvre across terrains.

Crystal ball gazing the likely threat scenarios in the future in India's context, throws up possible use of high-tech weapons, exploitation of electronic spectrum, space-based systems and use of cyber domain. These are likely to be inter-woven into a web that either presents a fait-accompli situation through rapid and unexpected manoeuvre where objectives are achieved before the defenders' plan can unfold and take effect. Alternatively, to thwart offensive designs construct anti-access and or area-denial network employing high-tech kinetic/non-kinetic systems across domains and forces.

To achieve break-through forces employed for operations for ground, maritime, air and special operations along with elements engaged in intelligence, space, electronic and cyber domains will have to harmonise manoeuvres and operations. The broad concept would be to synchronise simultaneous or sequential operations across services and domains to either enhance the culmination point of the domain or force, or to achieve break-throughs by hastening adversary's culmination point of the force and or the domain.

[14] https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/ Commentary: Multi-Domain Battle: AirLand Battle, Once More, with Feeling Shmuel Shmuel June 20, 2017

The operational battle field will have to be crafted masterfully understanding the complexities of operations, according priorities to domains of forces or both at different stages or during ‘widows of opportunity’. In order to accentuate the atrophy of decision making of the adversary, operational manoeuvres supported by operational fires and offensive employment of Special Forces, electronic, space and cyber elements will have to be schemed. For prosecuting war, leading role of force or domain will have to switch back and forth between domains and or forces with all elements having real time understanding of emerging situation and role expected of them. To that end, use of predictive algorithms, artificial intelligence and other emerging technologies will be essential to aid decision making. Secure communication systems providing data and voice facilities with layers of back-ups will form the scaffolding on which the entire concept would be casted.

Command and control of such forces at the operational and strategic levels will require focussed thought. It is not being dwelled further here. New structures, methods, facilities, protocols, practices and culture will have to be put in place. Joint doctrine would need recasting to guide operations, training, force structuring and development of systems. Logistics and other administrative support will have to cater for the demands of inter-acting domains and forces and would require added emphasis on flexibility and survivability.

In summary, the multi-domain force will be capable of operating in an environment contested by different forces and from other domains. It will be capable of defending itself against threats from all domains through employment of joint capabilities across domains and forces. The force will also have the ability to create break-throughs and present stratagems for restoring manoeuvre through forces and systems employed across domain(s).

Capability Development

Indian Army Land Warfare Doctrine 2018 enunciates the way ahead in terms of capability development by stating, “The Indian Army will enhance capabilities to address the challenges of non-contact domains of conflict viz cyber, space and information as a component of our National strategy for noncontact warfare to cause unaffordable losses to potential adversaries.”

Sanction of Space, Cyber and Special operations Cells under HQ IDS are the harbingers of future force development perspectives. These cells will have to be upgraded in time. For that resources and long-term plans will have to be put in place. Doctrinal shift to make multi-domain fighting strategy will usher disruptions and challenge existing warfighting notions and force structures. Reorienting human approach to operate in joint, integrated, inter-acting domains and forces will require great deal of doing. The challenge to build on existing anew! Involvement of academia, industry, free lancing cyber hackers and specialists from other domains will have to be incorporated to maximise utilisation of skills within the country in a cost-effective manner.

The role of military will vary from lead, to support to net provider of violence for coercion to its role as understood now or something not yet defined. More research and debate on the subject to translate the concept into warfighting is required.

In Conclusion, would be appropriate to end with a clear resolve enunciated in the Indian Army Land Doctrine 2018, “Due to increased threat of hybrid warfare, the Indian Army will prosecute operations with designated forces, equipped and mandated to effect attacks/ retaliation in the Information Warfare (IW) domain. Adequate capabilities will be developed to dominate the hybrid warfare environment, both along our Northern and Western borders and in dealing with internal security, in coordination with earmarked services and agencies.”

***Maj Gen Umong Sethi, AVSM, VSM (Retd)** is a renowned Delhi based Defence Analyst and a Distinguished Fellow, CENJOWS, New Delhi

MULTI DOMAIN WARFARE: EVOLVING HIGHER DEFENCE ORGANISATION IN THE INDIAN CONTEXT

Lt Gen Anil Ahuja, PVSM, UYSM, AVSM, SM, VSM** (Retd)*

Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win Sun Tzu

Introduction

Multi Domain Warfare (MDW) is a concept of fighting future wars which is still under evolution with the United States Army and the Marine Corps. The draft concept, aimed at creating capabilities to overcome new challenges in more innovative ways, is still in the realms of discussion and salient aspects are being deliberated in various writings available in public domain.

This paper aims at briefly describing the battlefield environment and the concept of MDW, as being evolved by the US, to set the backdrop for subsequent deliberations relating it to Indian operational environment, for which Higher defence and security organisations is sought to be evolved. The terminology used in the US context has been retained. The co- relation and applicability to Indian environment is included in explanatory notes. A suggested organisational structure applicable for policy planning and for operational execution of MDW in Indian context has also been put forth.

Battlefield Environment for which Concept of MDW is Being Evolved

The concept is being evolved for the US ground forces, operating as part of joint, inter organizational and multinational teams, on the premise that they are currently not sufficiently trained, organized, equipped or postured to deter or defeat capable peer competitor adversaries (`Revisionist' China& Russia and `Rogue' Iran& North Korea), in high intensity conflict, to win future wars. These countries have developed substantial force structures for physical combat as well as capabilities in virtual domain (e.g. cyber, information, cognitive…). There also exists a threat of non- state actors/ insurgents/ terrorists / criminals embedded in own and friendly countries. It is perceived that countering multi-dimensional threats in these domains necessitates creation of ground forces capable of projecting combat power from land into other domains to seize positions of relative advantage and control key terrain[1]. It entails integration and synchronization of joint, inter – organizational and multinational capabilities for conduct of warfare.

The visualised multi-dimensional operational environment, immensely enlarged in time and space, is illustrated in the table below, extracted from "Multi-Domain Battle: Evolution of Combined Arms For the 21st Century 2025- 2040[2]".

OWN SIDE ENEMY SIDE

Strategic Support Areas	Operational Support Areas	Tactical Support Areas	Close Areas	Deep Manoeuvre Areas	Operational Deep Fire Areas	Strategic Deep Fire Areas

CONTINUM OF GEOGRAPHIC SPACE

In the MDW, the `battle space' for conducting joint operations extends well beyond the commonly perceived battle space normally referred to as Tactical Battle Area (TBA). This vastly extended area encompasses all domains of warfare including space, cyber, electromagnetic, information warfare and also entails employment of non- state actors and other tools of punitive action against the adversary. Capabilities available to both sides, with co – related actions and counter measures taken over a period of time produce tactical, operational and strategic results. Manifestation of these `abstract elements' creates a hugely complex battlefield environment, where distinction of war and peace, front line and rear areas and military and civilian targets gets severely blurred. US armed forces visualise applicability of this concept in the global construct.

Amplification of different battle areas illustrated in the figure above is given in succeeding paragraphs.

The `Deep Fire Areas (Strategic and Operational)'. These areas lie deep within enemy territory. They are either beyond the range of physical deployment of conventional manoeuvre forces or access to these is prohibited by policy (being across borders, in a country with which there are no open hostilities). These areas therefore would need to be addressed by : joint fires (missiles / Remotely Piloted Aircraft), Special forces, Information Warfare or by use of virtual capability[3].In interpretation, these `fires' need not be in real sense of term and may actually be `delivered' in form of influence operation, deep into the heart of potential adversary(s), even during periods of peace.

Deep Manoeuvre Area. In a simplistic manner, this is the `depth area' of the battlefield where most `Operational level' objectives would lie. It is contiguous to the battle space (Close Areas) but is less intense in comparison. Combat elements of the attacker can operate in this area more extensively than in `Deep Fire Areas'. In a joint operations environment, coordinated fires, from weapon systems across all domains can be brought to bear in this area to influence actual battle. The analogy, in the context of land warfare, can be of conducting `degradation operations in depth areas' by bringing down coordinated fire from land based long range weapon systems and air or by employing special forces.

Close Areas. This is the area of actual `contact battle' on land, sea and air space. Operations in this area are characterised by manoeuvre, concentrated application of fire power and physical combat (employing Infantry, combat aircraft, battle ships). Operations in this area pose challenge of cross domain integration of weapon systems of various services due to proximity of contesting forces (safety considerations) and time criticality of orchestrating coordination functions. This in turn necessitates creation of capabilities organic to particular service (integral missiles, UAVs, attack helicopters, electronic warfare capabilities etc.), which would be available to the commander for employment, readily.

Support Areas. These areas, on friendly side of the battlefield, constitute the space through which own combat forces are mobilised, deployed and launched. Included herein are the lines of communication (air, sea and land) over which the forces are transported to their designated areas of employment; locations of nuclear, space, cyber and other strategic assets; logistic bases and HQs. In the US context, considering long distances from mainland to global deployment locations, the areas are categorised as: Strategic, Operational and Tactical support areas. Strategic support areas lie across the geographic boundaries of Combatant commands and include sea and air lines of communication over which the deploying forces are mobilised across the globe.` Operational support areas' encompass the command and control HQs, deployment areas of long range vectors, missiles, air and other fire support elements. These may also contain operational air bases or deployment areas of aircraft carriers for providing support in TBA if overseas operations are launched by expeditionary forces. In this eventuality, operational support areas may even be located in other nations, close to the area of operations. The `tactical support areas' would be much closer to the area of actual combat and would provide launch pads for combat/manoeuvre elements.

In the Indian context, the `support areas' could be viewed from two perspectives: in defensive role and in the role of a regional net security provider. Territorial defence operations would primarily be land centric, for which, support areas would lie within the geographic space of the country and distances would be substantially telescoped.

Strategic support areas would include areas in depth from / through which mobilisation takes place by rail, road or air and these may lie across geographic boundaries of Commands and Areas (static formation HQs), particularly for deployments / re deployments between Southern, Eastern, Western and Northern Theatres (Commands). Operational and tactical support areas would also be considerably closer and include `Rail/ air heads', `Concentration Areas', `Assembly and Forward Assembly Areas', Forward Air Bases, deployment areas of long range strategic assets and logistic support areas.

A different model would however be applicable while performing the role of a Net Security Provider in the Indo – Pacific Region. The Strategic support areas, in this case would include sea lanes of communication (SLOCs). Operational and Tactical support areas may lie in the Island territories (Andaman & Nicobar and Lakshadweep Islands) or in friendly neighbouring countries. A detailed concept for this is needed to be evolved.

Each of these areas would be susceptible to different nature of threats, kinetic and non – kinetic and would require building up of different capabilities for defence and counter measures. Orchestrating operations through these areas would entail institutionalised coordination between various organisations, departments and security agencies with a clear perspective that these areas also constitute a `battle space' vulnerable to potential enemy threat in a MDW environment.

Salient Features of MDW

It would be evident from above that there is blurring distinction between war and peace and between battle space, rear areas, hinterland and homeland/ heartland. MDW entails near simultaneous conduct of battle from tactical level to strategic level; creating ability to contest high end threats to hybrid threats below threshold of war; employing forces operating across all domains of Cyber, Space, Information Warfare (IW), legal warfare…It also entails factoring political shaping and economic influence, over a period of time, to achieve strategic ends, which may be to avoid war or to wage it, using lethal and/or non-lethal means. While in previous wars it may have been possible for global powers to achieve `continued superiority' on the immediate battlefield, MDW would entail creating `window of temporary superiority 'in highly contested battle space, across multiple domains, which may even be from strategic and operational distances. Organisations at the national level and for the armed forces would need to be re structured to meet challenges of this changed nature of warfare.

Considerations for Structuring Organisation for Conduct of MDW

There are primarily two approaches to evolving organisations and command and control structures suited to operate in the MDW environment: One is to equip a particular service with most `multi domain assets and capabilities', while the other is to create organisations to integrate multi domain capabilities, which rest with various services / organisations[4]. In the former option, Army and the Marine Corps (for whom MDW capability is being contemplated in the US) would need to be equipped with: missiles (SSM, SAM, anti – ship), unmanned vehicles (ground, aerial), electronic, cyber and IW capabilities. The rationale for this being that ground forces with such multi domain assets would be able to seize and hold objectives, shape the battlefield in anti-access and anti-denial environment (A2AD) and influence other domains, enabling other services to achieve at least temporary superiority. Eg. Ground forces suppressing/ physically neutralising enemy's air defence system to facilitate air force achieving favourable air situation.

In the Indian context, application of the concept of MDW is still at a nascent stage. Armed forces continue to operate in an environment of inadequate `Jointness' have acute capability voids and contend with limited budgetary support for capability enhancement. Under these circumstances it would be inconceivable to adopt the first option of equipping land forces (or any other service) with dedicated (integral) multi domain assets. Eg. Comprehensive cyber, space, IW offensive and defensive capability, all categories of armed / unarmed UAVs, helicopters, missiles etc. Besides the complexity of apportioning meagre resources, there is also the challenge of non-availability of commanders trained to handle inter service and multi domain assets/ operations. Such commanders need to be trained over years by exposure to inter service organisations and specialised weapon systems across domains. There also exist challenges of `span of command and control', which is a function of: complexity of operational environment, type of forces placed under command, proficiency of subordinate commanders and staff, terrain, infrastructure, technology etc. This in turn limits the number of units, formations and weapon systems that can be placed under command, at a particular level. In MDW, where jointness is sought to be `pushed down' from operational to tactical level, adoption of this course of action, in the Indian context, seems impractical, for now.

Indian operational needs for MDW can best be fulfilled by adopting the second option of creating appropriate organisational structure for coordination and integration of resources available with different services and with other agencies within the country. Following basic aspects merit consideration for evolving this construct:

- Integration of services is a *sine qua non* for future battles because there is no such thing as a single service or single domain warfare.
- The battle field of tomorrow will not remain confined to close area' (as indicated in the figure above) or so called TBA.
- It will extend to `Deep Strategic' and `Operational Fire Areas' into enemy territory. Likewise, on own side, it will extend into depth areas, to include `Strategic and Operational Support Areas', in the heartland or where the industrial base is located.
- The future commanders need to take the battle deep into enemy territory, across all domains and also plan defensive measures well inside own country.

- The MDW is not confined to periods of imminent or active hostilities but would be an on-going and continuous process where, even during no war conditions, thoughts, opinions and environment are shaped, economy, infrastructure and technological assets targeted and own `assets' created across domains (*Intelligence sources, opinion makers, political activists, academia, think tanks, ethnic communities et*c).

- MDW is thus a combined national effort where besides the armed forces, other Security/ Para military forces, Police, government and non-governmental civil organisations/ departments have a role which needs to be assigned and whose implementation needs to be ensured, as part of overall `war waging effort'.

- Armed forces need to play a` lead role' not only in execution of actual operations but also in planning and coordination of these activities at the national level because they possess the capability to view each of the relevant domains (cyber, space, social media, information space, cognitive domain and rear areas) from the `perspective of warfare'.

- A renewed national perspective of `all of a nation effort' to conduct this nature of warfare needs to be evolved where various departments and agencies work `independently in their own space' as well as `work together', concurrently. This distinction would be most pronounced while formulating policy, organisations and concept of operations for Cyber, Space and cognitive domains and while planning `depth area operations' (rear area security, mobilisation, counter intelligence, counter radicalisation, counter subversion etc.)

National Level Policy Planning for MDW

Organisation for national level policy planning for MDW would be most optimally created on existing national security structures. In this domain we have the: National Security Council (NSC) along with its secretariat (NSCS) and the Strategic Policy Group (SPG) -the principal inter-ministerial coordination mechanism, in place since 1999. Hitherto it was chaired by the Cabinet Secretary. Since September 2018 however, it is chaired by the National Security Advisor (NSA), who heads the mechanism to strategize on matters dealing with security: external, internal and economic security. SPG comprises of Vice Chairman of NITI Ayog, Cabinet Secretary, three services chiefs, RBI Governor, Secretaries of External Affairs, Home, Defence, Finance, Defence Production, Revenue, Atomic Energy, Space, Scientific Advisor to Defence Minister, Secretary (R) in Cabinet Secretariat and the Intelligence Bureau chief. Representatives of other Ministries and departments are invited to SPG meetings as and when considered necessary. The Cabinet Secretary is now responsible for ensuring implementation of SPG decisions by the Union Ministries, departments and State governments.

The basic National policy on conduct of MDW and allocation of responsibilities to various agencies of the Union and States must emanate from the National Security Council (with approval and directions of Cabinet Committee on Security - CCS). This necessitates creating a more expansive NSCS with a robust military component to enable it to review the operating environment, analyse and strategise activities in various domains, from a perspective of `warfare'. A similar structure would also be required to be created in the Cabinet Secretariat to assist the Cabinet Secretary in implementation of the decisions of the SPG, across different ministries and with different states. The Union War Book would need to be updated to redefine the combat zones, assign responsibilities as well as to coordinate activities, across different domains of the MDW. The entire concept of `mobilisation' and `declaration of state of conflict/ war' would also need to be reviewed. The activities at this level would however remain primarily in the policy formulation, planning and macro level coordination domain. It is imperative that the armed forces are thoroughly integrated in Policy planning since they would be at the core for operational execution of the MDW, two being linked inextricably.

Organisation for Operational Implementation

Jointness and integration of the Armed forces is essential for conduct of protracted MDW activities, where distinction between peace and war time operations gets blurred. A robust HQ Integrated Defence Staff (IDS) under an empowered Chief of Defence Staff (CDS)should be responsible for synergised execution of operations by services under their respective Chiefs. A four star CDS, at par with the Service Chiefs, would after all only be coordinating implementation, albeit robustly, of the decisions taken in a forum of which all Chiefs would have been a part. He would also be better placed to plan and execute integrated capability development to fulfil operational requirements and be the primary interface with NSCS, SPG and other relevant agencies and States.

It would also be prudent, for now, to keep creation of the post of CDS independent of creation of Theatre commands (*which, in effect entails equipping single formation with all multi domain assets*). This is because the current state of resources and largely single service centric training and career progression profiles of senior military leadership do not lend themselves to creation of Integrated Theatre commands, yet. These drawbacks need to be acknowledged and progressively addressed over a period of time. Sheer reduction in number of Command HQs is a superficial `look good factor' for the academia, for which the country and the armed forces are not prepared yet. Raising Theatre commands, adequately equipped for MDW, is an expensive proposition for which the current defence budgets are inadequate. The overriding priority should be to address the challenges of changing nature of warfare, within available resources, than to merely optimise a few hundred men!

Organising Armed Forces for Specialised Domains – A Cyber Domain Illustration

In the context of MDW, Cyber is one of the most significant domains, in which warfare is being conducted already between countries across the globe. Realising the significance and cross domain implications of this dimension of warfare, the Government of India has recently approved raising of a Defence Cyber Agency (besides the Defence Space Agency and a Special Operations Division)[5]. A review of the possible role and organisational interface of this Defence Agency with other national organisations in this domain would provide guidelines for evolving similar organisations for other domains: space, information warfare, economic warfare. This aspect is being discussed in details in succeeding paragraphs.

At the outset it is essential to identify the characteristics of the particular domain for which the organisation is sought to be evolved. A few salient characteristics of warfare in the cyber domain are: asymmetric nature of warfare (*can be launched by much weaker adversary (militarily, technologically and economically) or even by non – state actors at a negligible co*st); near anonymity enjoyed by the attacker ; involvement, even involuntary, of a neutral (or Innocent) third Country ; ambiguity in defining what constitutes a cyber-attack; absence of objectives/ targets for retaliation; cross domain linkage where cyber-attacks in a particular sector (military or civil) may result in cross sectoral disruptions and may result in retaliation in cyber, nuclear , conventional and/or other domains.

For optimum resource allocation across multiple domains it would be essential to carry out an analysis of most suitable/ critical targets susceptible to particular dimension of warfare. In cyber domain, these could be:

- C4 ISR L Networks. (Command, control, communication, computer, intelligence, surveillance, reconnaissance and logistics networks).
- Critical information storage systems, which may contain classified operational plans, intelligence data, critical technology and weapon control data.
- Platform centric networks
- Decision support and Fire control systems.

- Navigation and guidance systems of aircraft, ships, missiles and precision guided munitions.

From the foregoing analysis, it is likely to emerge that in asymmetric warfare domain, targets are spread across military and various civil domains. It would be impractical for the armed forces to assume responsibility of addressing such diverse threats, without active indulgence of all stake holders. An integrated organisational structure would therefore have to be created.

A workable organisational structure could be evolved, for Cyber domain, with following considerations:

- All cyber users (*banking, financial sector, power, transport, communications, individual services etc.*) remain responsible for creating their own robust and secure system, within the guidelines contained in the National Cyber Security Policy – 2013 and the Data Protection Law (*Similar national policy and legal framework would be available for other domains, for similar consideration*)

- The overall organisational structure for managing cyber security at the national level should remain under the oversight of the National leadership, through the National Security Adviser.

- An empowered Chief Cyber Executive (appropriately designated) with a robust secretariat be appointed at the national level for management of all aspects of cyber space (These tasks are presently being performed, in a rudimentary manner, by the National Cyber Security Coordinator).

- Primary functions of managing protection and resilience of nation's critical Information Infrastructure should continue to be performed by established national agencies: Indian Computer Emergency Response Team (CERT-IN) , National Critical Information Infrastructure Protection Centre (NCIIPC) and National Technical Research Organisation (NTRO). These agencies should also be responsible for obtaining strategic information regarding MDW threats to ICT infrastructure and for evolving crisis management mechanism.

- Defence Cyber Agency (or Command at a later stage), though a dedicated, trained and equipped military formation should work within the overall national cyber security architecture and in concert with cyber organisations of each individual sector / department, including the three services.
- A robust legal component would need to be built into ensure that operations are conducted in accordance with the rules of engagement that comply with international and domestic laws and that enough legal justification exists for transcending to physical conflict (Kinetic offensive action), should it become necessary.
- Authority for conduct of offensive cyber operations, as part of MDW should however rest only with the Defence Cyber Agency (or Command) due to the criticality of retaining control at the national leadership level.

Organisational structure for warfare in other domains can be evolved by similar considerations. This can therefore be considered as a representative case study.

Since most of these areas would have substantial civil – military overlap and boundaries between operational and peace time activities are likely to be blurred, the concerned agencies may be empowered to selectively outsource their operations. Alternatively, selected personnel may be temporarily embodied (akin to Territorial Army (TA) battalions). This would enable regular induction of contemporary technology and provide benefit of deniability (anonymity).

Conclusion

The concept of Multi Domain Warfare (MDW) is being evolved by the US Army and Marine Corps to meet emerging challenges from: `revisionist powers', `rogue states', `rapid technological advancements' and `changing character of warfare', for which, they perceive that they are not adequately prepared. The merits of projecting combat power from land to other domains are still being debated and the outcome is awaited.

This concept however presents a different perspective in the Indian context. It is a stark reminder (yet again!) of the fact that there are no single service, single domain operations on the battlefields of tomorrow. Cyber, Space, electromagnetic, information and legal warfare… all contribute to shaping the battlefield which extends well beyond the TBA. Also, there is blurring distinction between war and peace, between battle space and heart land, between military and civilian targets and that targeting of minds, opinions and economy is as potent a weapon as rockets and missiles.

The nation's security establishment and the armed forces need to review their organisational structure to bring to bear `all of nation effort' to wage and combat MDW threats. This paper is aimed at suggesting an approach to evolving such a construct in policy planning and operational implementation domain.

***Lt Gen Anil Ahuja, PVSM, UYSM, AVSM, SM, VSM** (Retd)** is a former Deputy Chief of Integrated defence Staff (Policy Planning and Force Development). He has also commanded a Corps and a Division along Northern borders in Arunachal Pradesh and Assam.

Endnote

[1] ShmuelShmuel. “Multi Domain Battle: Airland Battle, once More, With Feeling”. War on the Rocks. June 20, 2017.

[2]“Multi-Domain Battle : Evolution Of Combined Arms For The 21st Century 2025- 2040” by THEATRUM BELLI : BibliothèqueDéfense et Sécurité

Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0 October 2017 DISTRIBUTION RESTRICTION: DRAFT - NOT FOR IMPLEMENTATION. Approved for public release. The material in this publication is still under development. It is not an approved concept. Fig 2.Pg 9.

https://en.calameo.com/books/0000097798a77b76a3dc1

[3] ibid.

[4] Op.cit. Shmuel.

[5] SenSudhiRanjan. India to set up 3 new agencies, including cyber and space, to boost defence capabilities.Hindustan Times, New Delhi. October 16, 2018.https://www.hindustantimes.com/india-news/india-to-set-up-3-new-agencies-including-cyber-and-space-to-boost-defence-capabilities/story-umuS4UOsDavc0MhHkUjuWN.html

STRATEGIC AND OPERATIONAL DETERRENCE IN INDIAN CONTEXT : MULTI DOMAIN WARFARE

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

"When you talk about peace through strength, what you're talking about is the concept of deterrence" *Chris Gibson*

Introduction

It is rather ironic that while change is inevitable it is generally always resisted as it moves Nations and individuals out of their comfort zone and is initially chaotic. And if change is at a global level as is happening today, and driven by geo-strategic and geo-political considerations, economics, resources and technology, and is multi layered, multi-dimensional, cross-impacting and affecting nations, allies and adversaries, corporates, terrorist organisations to individuals we are looking at a turbulent, insecure international security environment leading to global **'**Competition[1] 24X7**'.** Why club everybody? because,

[1] A important activity/word in multi domain warfare - In competition, the adversary takes multi domain actions 24X7 (political, economic, military, diplomatic, information, cyber, space etc) to achieve objectives below the level of armed conflict, as well as to posture forces to support the escalation of activity into armed conflict. His primary aim is to separate or isolate friendly forces politically, limiting a coordinated allied response and destabilising target states internally to attain its objectives below the threshold for armed conflict. The adversary in competition may consider themself already engaged in national conflict and, therefore, employ all elements of

the 'World is getting Flatter' as glimpsed by Thomas L Friedman[2] in his seminal book on globalisation, digitisation and trade, and the very scope, spread and implications on security has 'compressed, enlarged and converged in time and space' and impacts all of us, directly or indirectly, sooner or later. Incidentally the heading of the book is attributed to our very own Mr Nandan Nilekani when he briefed the author at Infosys HQ in Bangalore during mid 2000's.In today's world of real politik, strategic balancing and engaging in Competition (also cooperation and confrontation when required) by Nations is in itself 'a form of engaging in deterrence operations'. This also validates the popular quote 'there are no permanent friends or enemies, only permanent interests[3]'.

The rapidity of change accelerated ever since 9/11 and GWOT. Diminishing comprehensive national power (CNP) and power projection capabilities of USA starting the slide to a multi polar world, emergence of China as a superpower; resurgence of Russia under President Putin; state controlled narratives leading to signs of ultra-nationalism; authoritarian Governments like Philippines, North Korea, Syria, Turkmenistan; emerging powers with regional aspirations like Iran, Saudi Arabia, South Africa, Nigeria, Turkey, India; rise of religious Islamic fundamentalism with a twist of occupying territory and establishing a caliphate like the ISIL; global warming and climate change indicators; transnational MNCs with their own agendas, drug cartels and international crime syndicates

its national power with few procedural limitations in a coordinated approach before own elements/forces receives authorization to respond. The adversary also positions systems to fragment own force capabilities and make a potential response costly and ineffective in the event of escalation. Essence taken from Para 2-4(a) of Draft Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0 October 2017

[2] 'The World Is Flat: A Brief History of the Twenty-first Century' by Thomas L Friedman, published by Farrar, Straus and Giroux, 05 Apr 2005

[3] The original of this pragmatism is generally conceded to Lord Palmerston (John Henry Temple) of Great Britain, but most world leaders have invoked it at one time or another to justify their policies and actions

have changed the world scape. There is a renewed political, ideological, economic and military competition due to globalisation which brought many good practices and developmental growth, but is a major driver of instability and conflict. While threat of full-scale conventional wars has gone down, correspondingly the span of conflict, its complexity, unpredictability, lethality, accuracy, reach and manifesting into many domains have emerged. The physical and nonphysical domains including the cognitive have expanded. There are no front, rear and flanks and there is no place to hide. Many new types of warfare have also emerged/ emerging like hybrid, media, cyber, information, electromagnetic spectrum, asymmetric, digital, waged either singularly or cross domains both in peace, no war no peace, or war! Nations have their National Vision and aspirations and want to find their legitimate place amongst the comity of Nations. India the ancient, proud civilization with a glorious history too aspires for the same and we are destined by our geography, size, population, resources and history to be a great power in the World Order.

While deterrence has always played its part as evident through military history and statecraft, the increasingly complex technological security environment, with nuclear weapons, hi-tech modern conventional weapon systems like hypersonic-weapons and low-end high impact easily available disruptive systems, which can carry out major devastation, alongwith the rapid mushrooming of terrorist organisations has raised questions on the current relevance, role and impact of Deterrence. As we will see, deterrence by itself has got multi-dimensional to address various facets of multi domain. This short paper provides an overview of the emerging security landscape of Multi Domain War (MDW)/Competition in brief and goes onto discuss Deterrence as applicable in the strategic and operational domain of MDW and in the Indian context. Obviously, it is pitched at India’s rising stature as a regional power with ever expanding sphere of influence and interest with matching aspirations as a key global balancing power in Asia (Century of Asia) and the World.

An Overview of MDW/Competition in Relation to Deterrence

The concept of MDW was formally introduced by the US Army quickly followed by the Marines sometime in 2017[4]. Essentially the concept is meant to counter the technological leap in military and non-military domains taken by adversaries which will adversely impact the security of USA and its allies, during the two decades of US focus on combating rogue Nations, in support of Western liberal democratic ideology and GWOT. While the US was busy, the US Armed Forces believe that its main adversaries Russia and China and others, have observed the methodology of US war fighting and its capacities and capabilities, and after detailed analysis identified its vulnerabilities and weaknesses and are building own capabilities to exploit them whenever a situation or contingency arises. The trigger has undeniably been the concept of A2/AD (anti access/area denial) actively being pursued by China, Russia and even Iran and North Korea. In future, no one power (including USA) can dominate one or multiple domains forever. MDW calls for a change of thought process, 'a transformation and not just modernisation[5]'. Visualization of battle spaces, cross domain operational capabilities and capacity in the military and non-military fields in war and peace, goes beyond the current jointmanship and synchronization of operations. Multi-domain means creating an effect in one domain that produces an effect in other. Multi domain-specific capabilities can be leveraged to defeat a capable foe in another domain. The resources must be capable of cross domain operations and fires, must be robust, deployable, low

[4] 'The Road to Multi-Domain Battle: An Origin Story' by Kelly McCoy | 27 Oct 17. Origins of Multi-Domain Battle can be traced back to 08 Apr 15 at the US Army War College, where then Deputy Secretary of Defense Bob Work charged the US Army to get after Air Land Battle 2.0. "Multi-Domain Battle" made its first appearance in Army doctrine with the release in Oct 17 of the updated Field Manual 3-0: Operations and as a draft operational concept, document that provide insight into how the army sees itself fighting tonight, tomorrow, and in the future

[5] 'Multi Domain Warfare in the Indian Context' by Lt Gen PR Kumar, 36th USI National Strategic Paper, 2018

maintenance and manoeuvrable[6]. Simply put, MDW envisions the military and non-military; everything from fighters to destroyers, space shuttle to submarine, cyber to satellites, tanks to attack helicopters, electromagnetic to electronic, media to information influence operations, munition factory worker to hacks— working together intrinsically as ONE, to overwhelm the enemy with attacks from all domains: land, sea (including sub surface), air, space, cyberspace, media and electronic. The span of operations addressed simultaneously is from the political, national, strategic, operational to the tactical domain. Traditional turf and domains are shed as it's everybody's domain and whoever is more effective more lethal, faster acts and reacts. Both adapting to and driving change in the operating environment, adversaries continue to alter the battlespace in terms of time, geography, and domains and by blurring the distinctions between peace and war. Battle space has expanded, converged and compressed all at once during competition and actual conflict; tactically, by bringing kinetic and non-kinetic effects to bear from any place in the world and, strategically, by being able to challenge the deployment and echeloning of forces into the fight at all places simultaneously. The first diagram (Fig 1) below illustrates the multi domain operational framework[8] with expanded battle spaces in terms of geography, space, time and domains in the future battlefield. It also illustrates the fires being executed from various domains ranging from the strategic support areas to close battle to deep manoeuvre area. Point to note that these areas are not strictly compartmentalized and are dynamic based on domain application. For example, in the cyber domain the strategic support area can be adjacent to the close support area. The 24X7 competition (below the actual conflict phase) being

[6] ibid

[7] Draft 'Multi Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040 Version 1.0', October 2017

[8] Ibid. Deterrence as a component of the operational environment has been added.

prosecuted is shown in the next diagram[9] .

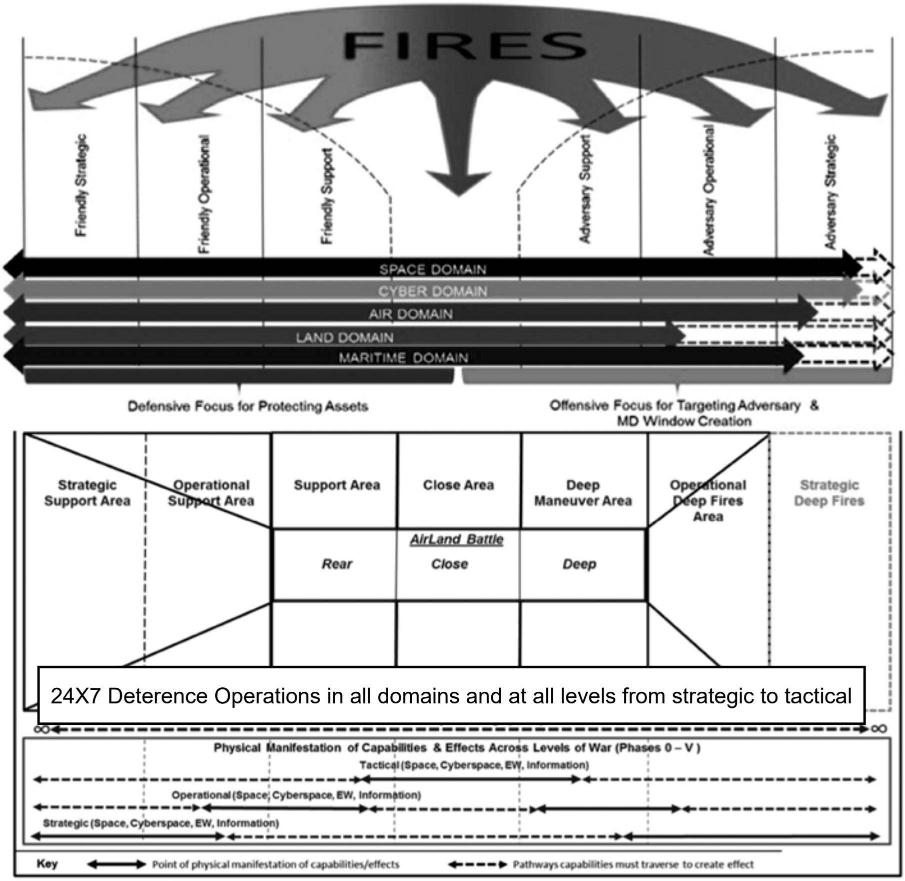
FIRES
Friendly Strategic
Friendly Operational
Friendly Support
Adversary Support
Adversary Operational
Adversary Strategic
SPACE DOMAIN
CYBER DOMAIN
AIR DOMAIN
LAND DOMAIN
MARITIME DOMAIN
Defensive Focus for Protecting Assets
Offensive Focus for Targeting Adversary & MD Window Creation
Strategic Support Area
Operational Support Area
Support Area
Close Area
Deep Maneuver Area
Operational Deep Fires Area
Strategic Deep Fires
AirLand Battle
Rear
Close
Deep
24X7 Deterence Operations in all domains and at all levels from strategic to tactical
∞
∞
Physical Manifestation of Capabilities & Effects Across Levels of War (Phases 0 – V)
Tactical (Space, Cyberspace, EW, Information)
Operational (Space, Cyberspace, EW, Information)
Strategic (Space, Cyberspace, EW, Information)
Key
Point of physical manifestation of capabilities/effects
Pathways capabilities must traverse to create effect

Fig 1: The Multi Domain Battle Operational Framework

[9] ‘A Wider War: Army Revises Multi-Domain Batle With Air Force Help’ By Sydney J. Freedberg Jr on October 12, 2017 and ‘Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040’; Version 1.0 October 2017. Deterrence operations as important ingredient of competition has been added.

[10] Numerous international open source official publications on deterrence including nuclear deterrence of various countries, newspaper/defence magazines have been perused. The similarities on the basic approach towards ‘Deterrence’ are strikingly similar including the Rand Corporation publication ‘China’s Evolving Approach to “Integrated Strategic Deterrence” by Michael S. Chase, Arthur Chan of 2016. Attribution specified where necessary

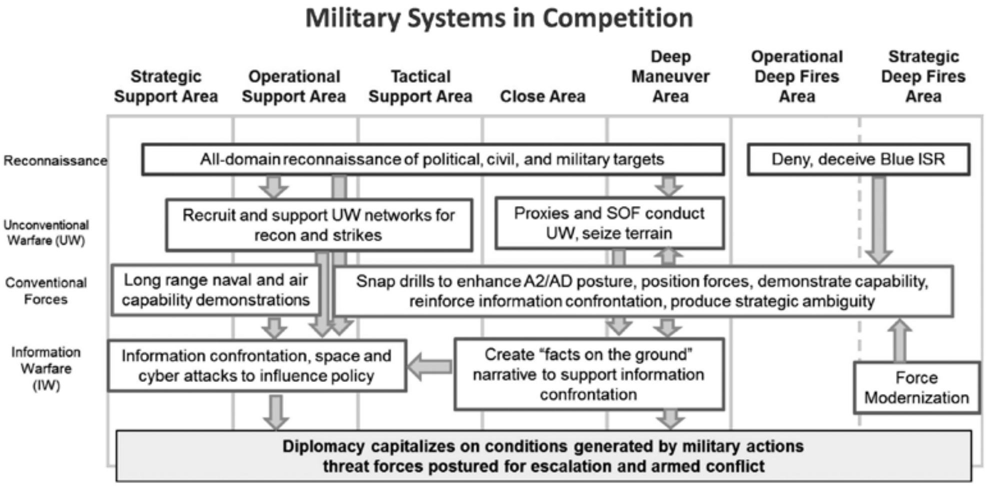
Military Systems in Competition
Strategic Support Area
Operational Support Area
Tactical Support Area
Close Area
Deep Maneuver Area
Operational Deep Fires Area
Strategic Deep Fires Area
Reconnaissance
Unconventional Warfare (UW)
Conventional Forces
Information Warfare (IW)
All-domain reconnaissance of political, civil, and military targets
Deny, deceive Blue ISR
Recruit and support UW networks for recon and strikes
Proxies and SOF conduct UW, seize terrain
Long range naval and air capability demonstrations
Snap drills to enhance A2/AD posture, position forces, demonstrate capability, reinforce information confrontation, produce strategic ambiguity
Information confrontation, space and cyber attacks to influence policy
Create "facts on the ground" narrative to support information confrontation
Force Modernization
Diplomacy capitalizes on conditions generated by military actions threat forces postured for escalation and armed conflict

Fig 2

Deterrence In Indian Context[10]

Just as management of public perception is an essential part of counter insurgency campaign, deterrence operations form an integral part of competition and conflict in ALL domains. While obvious, it is wise to benchmark the dictionary definition of deterrence and compellence. Oxford dictionary defines deterrence as 'the action of discouraging an action or event through instilling doubt or fear of the consequences', and compellence as a 'direct action that persuades an opponent to give up something that is desired[11]'. It is an obvious byproduct of the world of 'competition'.As a regional power dominating South Asia, India needs to forge strategic alliances, ensure neutrality of some and keep adversaries at bay by strategic balancing (internal, external, and soft power balancing) and deterrence. India has bilateral strategic partnerships including Security Agreements with USA, Japan, Bhutan and forged alliances in multi-national alliances/groupings like ASEAN, SCO, BIMSTEC, QUAD, BRIC to name a few. India also needs to prosecute 'Competition' operations in all domains as also develop deterrence tools and capabilities, to act/prohibit/restrain/react to

[11]Coined by Thomas C Schelling the Nobel Price Winner in Economics in 2005 in his book *Arms and Influence* (1966)

other Nations from degrading our CNP. To illustrate, ability to protect our networks and carry out cyber warfare, protect our space assets, our economic and trade pathways, defend and prosecute influence information operations down to the basic essentials of protecting India's sovereignty and integrity in all domains including IOR. We must be absolutely clear that ALL countries are in competition with us including even our strategic partners, especially our known collusive adversaries China and Pakistan and immediate neighbours. While the superpower USA and possibly China possess compellence capabilities (even they cannot dominate all domains), all nations especially the weaker need to create/develop deterrence capabilities in multi domains for obvious strategic reasons both during peace and war.

Deterrence is enhanced through security cooperation and military integration and interoperability with own security and intelligence agencies, allied forces and partner nations and building trust and confidence between partners. The deterrent impact of such cooperation and integration is both political and military in nature. The political impacts are primarily derived from the effects that coalition-based responses have on adversary decision-makers' perception of India's and allied political will; the potentially long-lasting, harmful post- conflict political and economic effects of taking on India. Allied and partner contributions to the joint fight are significant. For example, they can provide host nation security, fly additional combat and support sorties, supplement naval presence, provide additional manoeuver forces, supplement ISR inputs, to name just a few. They could stay short of providing 'kinetic support' also. These actions contribute significantly to deterrence, force protection and overall operational success. While military intervention of any of our strategic partners including USA is very tenuous at best, we must realise the unique potency of US Global Strike capabilities: their nuclear and armed forces contribute uniquely and fundamentally to deterrence[12], through their ability to threaten to impose costs and deny

[12] US Field Manual: Deterrence Operations Joint Operating Concept, Version 2.0, Dec 2006

benefits to an adversary in an exceedingly rapid and devastating manner (practice of imposing trade sanctions if adversary does not cooperate is a deterrent operation). It must be noted that China and Russia too possess such strike capabilities and even USA feels threatened and insecure. Knowing our main adversaries, they can and will operate with and through proxies, and attempt to achieve their strategic and operational goals below the threshold of armed conflict. Terrorism, proxy insurgency, information and unconventional warfare (UW) are inherently difficult to attribute and subsequently to punish the originator, and, therefore, difficult to deter. Armed Forces do not possess the capabilities to carry out deterrence operations/deter in all domains especially non-military.

Deterrence requires a national strategy that integrates diplomatic, informational, military, and economic powers. We must develop strategies, plans and operations that are tailored to the perceptions, values, and interests of specific adversaries. Deterrence strategies and actions must span daily operations and must be developed for all phases of competition and conflict planning. Deterrence operations convince adversaries not to take actions that threaten India's vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome. Deterrence operations must therefore be planned and executed across all domains in concert with other elements of national and international power in order to achieve strategic objectives. Till we fine-tune our international security alliances and are fairly confident of their direct military and non-military participation, India must plan and prepare to go it alone. This paper, however, does allude to the multi nation cooperation to India to assist domain competition and even in case of actual military conflict, given that with time and India's own rise of CNP (especially economic and military including power projection capabilities and domination of IOR), our allies will respond as much as they would expect us to respond. In the MDW operating environment, deterrence must address a broader range of potential adversaries and situations than previously envisaged. Deterrence operations are dependent on the ability of our Armed Forces to manage perceptions and act directly and discriminately through multiple domains on the decision-making calculus of adversaries. A crucial aspect is that successful deterrence is knowledge-dependent and requires the ability to establish and secure communication access to adversaries in order to generate the desired decision outcomes. The strategic implication of India's multi-national security alliances in today's multi polar world is a complex subject by itself and outside the scope of this paper.

HUMINT naturally is essential in seeking to understand an adversary's values, culture, decision calculus, risk propensity, and capacity for situational awareness as well as obtaining other information required for effective deterrence. HUMINT reporting must be integrated into situational awareness displays that provide our Armed Forces with battle space visualization. Interagency and multinational cooperation is key to achieving success in these efforts. It requires creation of a collaborative environment that incorporates intelligence community, diplomatic, law enforcement, military, and multinational inputs to achieve true situational awareness for deterrence. Our military capabilities and potential must be visible and known to all as it's a pivotal ingredient of deterrence. Effective deterrence combines military and non-military means. In some cases, military capabilities may not be an effective tool to deter a particular adversary's action, making other instruments of power the primary deterrent. Additionally, coalition support should be integrated to enhance deterrence credibility, but deterrence also must be viable as unilateral strategy. Our deterrence will obviously be challenged by other affected Nations. Just as a defender need not gather superior multi domain strength/capabilities to stave off an attacker by projecting unacceptable losses if attacked by adversary, similarly deterrence does not necessarily need overwhelming superiority but credible/deterrent capability. Military options/actions will always remain the final pivotal option to achieve national objectives both proactive and reactive. The Indian political and military leadership does carry out net assessment exercises regarding potential adversaries and needs to constantly review the deterrent capability which needs to be put in place against potential adversaries specially against a probably two and a half front threat against a collusive China-Pakistan. For India, to list some of the main military deterrents would be a credible nuclear triad with second strike capability[13] (China has it and Pakistan claims full spectrum capability to justify their tactical nuclear weapons[14,15]), capabilities of conventional ICBM/IRBM missile and rocket artillery, strategic lift, robust C5I2SRT (command, control, communications, computers, cyber, intelligence and information, reconnaissance and targeting), BMD (ballistic missile defence), dominate IOR, strategic offensive capabilities military and multi domain to provide credible deterrence and punitive deterrence against China and Pakistan respectively.

In relation to Pakistan, we face a peculiar problem of whom to deter! If he suffers significant conventional losses or loss of territory, he may assess that escalating the conflict by employing weapons of mass destruction, effect, or disruption could recapture the initiative or drive policymakers to the negotiation table to end the conflict on more favourable terms. Pakistan may also use tactical nuclear weapons if presented an appropriate target contributing to the attainment of op or strategic objectives. This brings us to the strategic nuclear dilemma (faced by the major powers against each other like US, China and Russia) that India should not risk escalation for Pakistan to reach a perceived "use it or lose it" situation, especially if he perceives backing by USA. If and when India prosecutes offensive operations we must conduct a

[13] 'Modi hails 'India's successful establishment of Nuclear Triad', The Dawn, 05 Nov 2018

[14] 'Pakistan completes nuclear triad' by Kinza Asif, Foreign Policy News, 16 Jan 2017

[15] Pakistani nuclear forces, 2018, Hans M. Kristensen, Robert S. Norris & Julia Diamond, pgs 348-358| published online: 31 Aug 2018, 'Bulletin of the Atomic Scientists', Volume 74, 2018

very effective Influence Operations against Pakistan and to the World too about the dangers of employing WMD, minimize vulnerabilities, and demonstrate the ability to continue operations if attacked. If deterrence fails to preclude a tactical weapon of mass destruction or disruption attack, our influence operations must ensure isolation of Pakistan internationally and regionally. The option of exercising our stated nuclear policy is a constant. When it comes to non-state actors and terrorist organisations, it's a different ball game. They differ in their susceptibility to our efforts to credibly threaten cost imposition. They have different goals/objectives, different values, and they employ different means to achieve them. Since India does not believe in using a hammer to kill a fly which is why planning and preparing for deterrence operations against specific targets (nation, non-state actors like corporates, agencies, terrorist organisations or even individuals) is important.

China is a past master and strong advocate of 'unrestricted warfare' in which deterrence forms a key component. Her rapid growth of CNP with a focus on military modernisation (A2/AD), niche technologies (cyber, space and information warfare capabilities coupled with development at par if not superior capabilities in niche tech like AI, robotics, swarm, drones, EW, hypervelocity systems etc) poses multiple challenges even to USA, and she is currently engaging India in competition 24X7 to ensure our CNP, strategic growth and space remains confined and restricted. In addition, China is increasingly discarding the rules based international system, and conventional defined norms of international behaviour and its opaque strategic thinking and decision making makes deterrence more difficult. Recently President Xi asked the PLA to prepare for war[16]. Speaking at the US Naval War College Prof James Holmes quoted Clausewitz "it's wise to pick a fight with a stronger power today if you see the trendlines running against you," and further elaborated that "You might get part or all of what you want today, but not tomorrow, next year,

[16] 'Prepare for War' President Xi Jingping tells military region that monitors South China Sea and Taiwan, South China Morning Post, 20 Nov 2018

[17] Political newspaper 'The Hill' dated 30 Oct 2018, published in Washington by Capitol Hill Publishing

or a decade from now. If China sees its rise plateauing or starting to decline, it might strike rather than wait[17]." These proclamations should be taken very seriously by our leaders, and deterrence measures must be planned and put in place both military and non-military. Recent Chinese publications have increasingly spoken of strategic deterrence. While focussing on China and Pakistan we must not ignore other adversaries, or conclude that the multi domain lessons learnt can be commonly applied, as every competitor is different. Naturally, India has to address non-state actors on equal priority.

As its already a pre-requisite for combating MDW, knowing and understanding the adversary is the bedrock of deterrence and requires enhanced ISR (intelligence, surveillance and reconnaissance) and operational intelligence gathering capacity and capability including hi-tech mechanisms to understand adversary's perceptions, assets, capabilities, vulnerabilities, his decision making hierarchy, procedure and structure, non-state actors sponsored by him, in short a holistic situational awareness of all. We must develop cogent plans to identify and defeat his military and non-military plans during and after 'Competition', and create a proper military and non-military target list which we keep reviewing. What cannot be understated for above capability is our understanding of our own capabilities including allies, limitations, and real time situational awareness. Such understanding is achieved only by total synergy amongst all players involved in deterrence operations. Highly networked forces which are integrated and interoperable will increase the commander's flexibility to choose from widely varying types of capabilities to achieve the desired deterrence effect.

Current Ground Realities Regarding Deterrence

The cold war deterrence (mainly nuclear) has given way today, leading to a lot of cynicism about the relevance and even effectiveness of deterrence especially on illiberal nations and terrorist organisations. Even given the tremendous CNP of USA, increasingly many minor nations from Iran, North Korea, Venezuela, Philippines, and Pakistan etc are thumbing their noses at USA with impunity[18]. Deterrence effect finds it difficult to prevent strategic competition which fall beneath the threshold of traditional military force (military dimension less than armed conflict), allowing these adversaries to make operational gains without tripping the 'go-to-war' calculus of the adversary. Russia demonstrated some of these capabilities as part of its operations into Georgia, Crimea, and the Ukraine. North Korea demonstrated its advanced cyber capabilities in November 2014 when they launched a cyber attack on Sony Pictures, and China has built artificial islands in the South China Sea to advance its sovereignty claims on vital international waterways that are part of the busiest maritime trade routes in the world, and closer home, the proxy war being waged by Pakistan against India.

The Complex Deterrence Theory, General Deterrence Theory[19] (Immediate Deterrence Theory as applicable between USA and Russia during Cold War period) and a lot of papers have emerged on Deterrence in recent years. Complex Deterrence Theory recognizes that the credibility of the deterrence threat has been increasingly compromised due to the ambiguity and fluidity of the international system[20]. As a similar perspective to this, it is being pointed out that the growing complexity of international nuclear order has played a part in exacerbating the uncertainty of nuclear deterrence[21]. Emanuel Adler reasons that the asymmetrical power relationship between or among

[18] James J. Wirtz, "Conclusions," Complex Deterrence, pp.322-328, pp.322-323. The outbreak of the Bosnia-Herzegovina conflict in 1992 and the Rwanda genocide of 1994 can be cited as examples of this.

[19] Patrick M. Morgan, Deterrence: A Conceptual Analysis (Beverly Hills: Sage Publications, 1977), pp.28, 31-43.

[20] **"**Beyong the Nuclear Umbrella: Re-Thinking the Theory and Practice of Nuclear Extended Deterrence in East Asia and the Pacific**"**, byHayes and Tanter,Nautilus Institute for Security and Sustainability, 2011

[21] House of Commons Defence Committee, Deterrence in the twenty-first century: *Eleventh Report of Session 2013-14, Volume II* (London: Stationery Office, 2014), p.Ev w32, http://www.publications.parliament.uk/pa/ cm201314/cmselect/cmdfence/1066/1066vw.pdf.

actors in the international political arena following the Cold War has given rise to the so-called deterrence trap[22]. A deterrence trap refers to a situation, in which a major power is unable to deter the actions of a relatively weaker actor no matter whether the major power threatens the weaker actor with retaliation, or abstains from threatening and appeases the weaker actor. For example, even if America threatens to use force in order to deter Iran from nuclear development, there is a possibility Iran will turn America's threat against it in order to fortify its position on its nuclear development plan.

Coming to deterrence against terrorist organisations, YairNaveh of the Israel Defence Forces says that we need to hit their assets which they rely on for survival. He identifies them as the organization's leadership strata and commander; its military capability for carrying out terrorist attacks; its economic and financial support base; and the network of alliances with other organizations and states that provide support in the form of arms and financing. It is possible to achieve deterrence by demonstrating the will to use military force to inflict damage on these assets.[23] We can proudly say that our Army has identified the same but been only somewhat successful in following this deterrence concept in entirety, specially hitting their support bases across our borders.

Cyber deterrence based on traditional deterrence theories is difficult, and deterrence by retaliation, in particular, has been thought of as unworkable. However, recently cyber deterrent forces are being

[22]**"**Unconventional Deterrence: How the Weak Deter the Strong**"** by Ivan Arreguin-Toft. Citing Israel's retaliatory attack against Hezbollah in 2006 as an example, Adler argues that although Israel's use of military force was aimed at deterring any further terrorist attacks from Hezbollah, it instead resulted in a bolstering of Hezbollah's international standing, thus putting Israel in a deterrence trap.

[23]"Deterrence against Non-State Actors: Thoughts following Operation Protective Edge**"**, by YairNaveh, *The Institute for National Security Studies (INSS) Insight, no*. 663, February 11, 2015, http://www.inss.org.il/index. aspx?id=4538&articleid=8720.

[24]"Cyberwar and the Nuclear Option," byElbridge Colby, The National Interest, June

established, including ones that identify the sources of cyber-attacks and threaten to retaliate against such attacks. There is even talk that nuclear weapons should be used as a means of retaliation[24]. However, I feel that it will not be a credible threat if announced by India or any Nation. Some defence experts and Think Tanks feel that unless nations can deter cyber-attacks, the appeal of cyber-weapons to hostile forces will increase and the credibility of extended deterrence, including the nuclear deterrent, is likely to be undermined[25]. Chinese cyber intervention is a known practice and they are targeting India, and we need to protect ourselves against all adversaries, and create robust and real time counter cyber warfare capabilities. New niche technologies and even low end and low-cost technologies employed enmasse will certainly impact deterrence capabilities of every nation and even individuals and organisations with many such gadgets/systems available commercially off the shelf (COTS). High end Conventional Prompt Global Strike (CPGS) system being developed by America is one such example. CPGS is based on a leading-edge military technology said to make it possible to accurately destroy any target on earth using a non-nuclear warhead that is carried by a strategic missile such as an ICBM before detaching at a near-space altitude and then accelerating to fly at hypersonic speeds of Mach 5 or faster. While US is planning to only arm conventional weapons, it is rumoured that China will deploy even nuclear warheads on it (on the new Wu 14 missile)[26]. This will further exacerbate the deterrence relationship between nations (mainly major powers) but also initiate a new arms race (which has already commenced in the nuclear and niche tech domain of AI, robotics, space etc).

24, 2013, http://nationalinterest. org/commentary/cyberwar-the-nuclear-option-8638.

[25] Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspaceby Brian M. Mazanec and Bradley A. Thayer, Houndmills: Palgrave Macmillan, 2015, p.32

"Prompt Global Strike: China and the Spear,"by Lora Saalman, APCSS, April 2014, http://apcss.org/wp-content/ uploads/2014/04/APCSS_Saalman_PGS_China_Apr2014.pdf.

Conclusion

Frankly, similar to the important factor of 'Surprise and Deception' in warfighting/competition, Deterrence Operations too has generally appeared as an abstract operation for most ground soldiers even at the theatre level, but its impact, generates/prevents/initiates defensive or offensive action by the adversary. We have now entered the complex world of multi and cross domain competition which needs to be synergised at the apex level; PMO- CCS – NSA – Ministries – COSC and concerned agencies involved. At the military sphere, once the political directive (hopefully in the form a National Security Strategy) has been promulgated, strategic military deterrence will be planned and coordinated by the COSC and executed by the Services while operational deterrence is executed by Theatre Commanders. Currently it is happening automatically and intrinsically (raising of new mountain Corps for China; strategic command assets and deployment; induction of nuclear submarines, aircraft carriers and modern fighter squadrons- all have deterrent constituent) by all domain holders but it needs to get institutionalised, specially the non military domains. When US intervention and multi-national activities to protect a liberal rules based world order is not considered hegemonistic, India needs to think, prepare, plan and execute strategy to dominate its area of influence and interest. A collusive China-Pakistan in our immediate neighbourhood, rising trend of ultra nationalism infecting our immediate neighbours and contested strategic space of Asia, dictates that India needs to get its act together, continue building its CNP, militarily transform into a MDW capable Armed Force and gets its multi domain deterrence capabilities in place.

***Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)** is a renowned Defence Analyst

MULTI DOMAIN WARFARE IN THE INDIAN CONTEXT-NAVAL PERSPECTIVE

Vice Adm HCS Bisht, PVSM, AVSM, NM (Retd)*

Introduction

Wars over the years have evolved with capability enhancements, involving technology. The concept of Multi Domain Warfare has existed for decades, in its basic form, however with galloping advances in technology and the advent of new and powerful domains like cyber and space, the concept of Multi Domain Warfare has to further evolve. The components of cyber, space and networks have enhanced warfighting capabilities tremendously. The first version of a cyber enabled war and network centric war were seen during the first Gulf war between US and Iraq in 1991, where the war was co-ordinated across continents and by use of satellites and literally brought to our bed rooms. The second Gulf war of 2003 saw even greater application of technology. It is thus evident that future wars will be fought in a multi domain format, which is likely to encompass the geo strategic, geo economic and geo political contours of nations involved, as well as involving the domains of cyber, space, information warfare, psy ops, electromagnetics, lasers, artificial intelligence, robotics, autonomous weapons, special operations, drones etc.

Multi-Domain Warfare (MDW), in simple terms, can be described as actions in and across land, air, sea, space and cyber domains, harnessing individual service capabilities and technology to achieve desired military effects with an element of surprise. Due to its wide-ranging geographic and conceptual dimensions, all of which are divided amongst multiple military services, the key to this kind of warfare is increased integration of capabilities, developed and managed by individual services i.e. the Army, Navy and the Air Force. MDW as a concept is apparently being steered by the US Army, however it has relevance across the board since the future wars are likely to entail aspects like Artificial Intelligence, lasers, robotics, UAVs etc. One such type of operations, which combines the individual capabilities of all services are Amphibious operations, which traditionally have been live examples of Multi Domain Warfare since they harness the best capabilities/ aspects of individual services. Whilst services have their own operating cultures and Standard Operating Procedures (SOPs), MDW would hinge on jointness or convergence across domains.

Aids to successful conduct of MDW

An important aspect determining success of MDW would be communications compatibility of the forces concerned. As an example, one of the factors underlying the success of US forces during the Gulf Wars was their far superior communications capability compared to that of the Iraqis. They were able to maintain close coordination, disseminate sensor and intelligence information and enable coordinated strikes over an expanded theatre of operations. While the deployment of troops and application of munitions during the second Gulf war had dropped drastically, the demand for communications had increased dramatically. For example, in Operation Desert Storm in 1991, 542,000 US warfighters were deployed and used 99 Mbps of satellite communications. In contrast, only 350,000 warfighters (almost half compared to Desert Storm) were deployed during the second Gulf War but they used a total of 3,200 Mbps of satellite communications. This is almost a 60 fold increase in bandwidth utilization on a “per warfighter” basis. [1] While further analysis

[1] www.dsta.gov.sg, Future Communications in a Net work Centric Paradigm, pg 3

would be needed, it would not be an exaggeration to infer that the intensity of future battles would be proportionate in nonlinear terms to the communications bandwidth applied. Communications connectivity and bandwidth are also pivotal to MDW and would become a critical success factor in future battles. Also in order to have an effective MDW, a network centric environment with good intelligence, surveillance and reconnaissance (ISR) capability is necessary so as to reduce the sensor to shooter chains.

In our case, current communication systems either do not meet the mobility or range requirement or both. In an integrated 'C4ISR' (Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance) future, the communications range must at least be as far as the range of the stand-off weapon. Issues of electronic warfare vulnerability, information assurance, and overcoming sporadic but frequent intermittent communications loss must be resolved. Providing a dedicated link is feasible. However, synergizing such links to form a coordinated and integrated network with an element of stealth is a technical challenge. In the future, where more nodes co-exist in a network, an exponential increase in network capacity is required. System availability is also a major concern since persistence becomes the key criterion and this will normally conflict with what is physically achievable.

Another important aid or instrument affecting outcome of MDW would be Unmanned Aerial Vehicles (UAVs) and drones integrated with all three services. As UAVs enter mass production and their prices fall significantly, they could be deployed in larger numbers economically. A communicating fleet of UAVs could be explored to provide force protection and precision attack capabilities. UAVs are anticipated to be fielded in greater numbers in the future. The competition to build and sell the next-generation UAVs and Unmanned Combat Aerial Vehicle (UCAV) is fast heating up in the world. In the future, with commercialization, UAVs could be cheap enough to be dispensable, which means that they could be launched for a particular mission without the need for considering their return, unlike manned missions, in some specific situations. Asymmetric strategies such as the Japanese “kamikaze” flights that devastated the Allied navies in the Pacific during World War II could possibly be executed at a comparatively lower cost with higher efficiency. UAVs have a great potential to shape the battlefield by providing tactical responsiveness and extending the sight and reach of sensors and shooters.

Multidomain operations also bring together capabilities from at least two of the following domains: land, maritime, air, cyber, space and the electromagnetic spectrum. The current focus on multidomain rises from a growing sense that the space and cyber domains will have an important impact on future military operations. In addition, there is likely to be involvement of artificial intelligence, robotics and lasers, all of which can help win wars. Some of these capabilities will work and some will not and we should factor that in our planning considerations. In our case, with the likely formation of Defence Cyber and Space Agencies and Defence Special Operations Directorate of the Integrated Defence Headquarters, there would be greater interdependence of one service on the other, as far as intelligence inputs and Special operations are concerned. [2]

Another important aid to MDW is Info warfare, which has traditionally been used since times immemorial during wars with the aim of deception or surprise. The biggest example in history of info warfare is of the D-Day landings of 1944, wherein the allied forces sent out false broadcasts of the landings. The code word for the operation was, ‘Operation Fortitude’ which was a deception strategy employed by the Allied nations as part of an overall deception strategy (code named ‘Bodyguard’) during the build-up to the 1944 Normandy landings. Operation ‘Fortitude’ was divided into two sub-plans, North and South, with the aim of misleading the German high command as to the location of the invasion. Both Fortitude plans involved the creation of phantom field armies (based in Edinburgh and the south of England), which threatened Norway (Fortitude North)

[2] Times of India, Sep 25, 2018, Unified Tri service agencies to handle Cyber-space, Space and Special Operations Directorates by Rajat Pandit

and Pas de Calais (Fortitude South). The operation was intended to divert Axis attention away from Normandy and after the invasion on 6 June 1944, to delay reinforcements, by convincing the Germans that the landings were purely a diversionary attack.[3] Closer home is a recent example of info warfare in the Indian Navy during the 'Kargil conflict'. The Eastern Fleet of the Indian Navy was deployed to the west coast during that time, as a precautionary measure to augment forces on the western seaboard, in case of a need and both Fleets had assembled at Kochi for work up together. This activity found its way in the media and sent shock waves in the Pakistan Navy.

Examples of Multi Domain Warfare

As mentioned earlier and from a naval perspective, Amphibious Operations/Amphibious assault has historically exemplified MDW, since capabilities and core expertise of all three services, across various domains like Air Defence, cyber, space etc are exercised to their full capacity. In our context, this kind of operation gains salience, due to the dispersed location of our island territories from the main land, both on our west and east coasts. In addition, we also have strategic interests overseas, especially our offshore oil assets spread all over the world. An amphibious operation is similar to but in many ways different from land, naval and air operations. At its basic, such operations include phases of strategic planning and preparation, transit of Army troops and equipment to the intended theatre of operations by naval ships, during which time, ships become vulnerable to enemy surface, air and subsurface attack, pre-landing rehearsals and disembarkation, troop landings, beachhead consolidation and conducting inland ground and air operations. Historically, within the scope of these phases a vital part of success is often based on elaborate logistics support, naval gunfire support and close air support. One of the pre requisites of such an operation is beach softening, which can be achieved by the use of air power, artillery or Naval Gunfire Support (NGFS). It may be conducted in order to execute further

[3] www.wikipedia.com/ Operation 'Fortitude'

combat operations ashore, capture or recapture territories, obtain a site for an advanced naval or air base, deny the use of these facilities to the enemy and to target the enemy's Centre of Gravity (COG). Amphibious operations employ a range of military assets and resources integrating virtually all types of ships, aircraft, weapons, special operations forces, landing forces etc, which include Army and Air Force assets etc. making it the most complex of all operations. [4]

There have been numerous examples of Multi Domain Warfare during large Amphibious operations in history like 'Operation Chromite', the Inchon Landings in Sep 1950 in Korea which altered the complexion of war or during 'Operation Neptune' or Normandy Landings in June 1944, mentioned earlier. The most recent example of a successful amphibious operation, which also exemplified the concept of MDW was during the Falklands War of 1982, between the UK and Argentina, wherein the Royal Naval task force comprising 43 Naval ships, 22 Royal Fleet Auxiliaries and 62 merchant ships embarked troops from the Royal Marines, 3 Commando Brigade, 5th Infantry Brigade, 2nd and 3rd Parachute Regiments and Royal Artillery. The task force traversed almost 8000 nm into South Atlantic from the UK for almost a three month plus complex operation, codenamed Operation 'Corporate'. At the beginning of the war, in a typical validation of MDW, Royal Air Force Vulcan bombers took off from Ascension Islands, somewhere midway between UK and Falklands, flew almost 15000 km, bombed Port Stanley airfield in Falklands and denied its use by the Argentine Air Force. Later this airfield was used for the war effort by the RAF Phantoms and Naval Sea Harriers, which had taken off from the two British Aircraft Carriers, HMS Hermes (later INS Viraat) and HMS Invincible. Another example of MDW was during the Battle of Goose Green by 5th Infantry Brigade, wherein extensive co-ordinated bombardment was carried out by NGFS provided by the frigate HMS Arrow and Artillery cover by 8 Field artillery Battery. [5]

[4] Indian Maritime Doctrine, INBR 8, page 82

[5] www.wikipedia.org/Falklands War

In our case, an example of MDW was during the IPKF operations in Sri Lanka in 1987. When the Indian Army troops were being inducted in Sri Lanka in IAF aircraft and IN ships, there were IN warships patrolling the coast of Sri Lanka to ensure the safe passage of Indian troops to Sri Lanka as also a kind of blockade to check foreign merchant ships bringing arms and ammunition to the LTTE militants.

The most recent example of Multi Domain Warfare is Operation Iraqi Freedom (OIF) of 2003, which validated some of the touted benefits of a joint and fully networked force, massing of effects rather than force, higher force exchange ratios through better situational awareness and coordinated engagements, Some factors that contributed to these numbers: application of precision weapons (almost 10 times more accurate) against Iraqi ground troops (compared to Desert Storm of 1991), rapidity and intensity of strikes (munitions in OIF were delivered over three weeks versus six weeks for Desert Storm) and the reduced preparation time of the Iraqis (the Iraqis had five months to prepare in Desert Storm compared to just few weeks in OIF).[6]

Likely use of MDW in the Indian context

Though MDW has been used in many campaigns in some form or the other, its usage in the spirit of its current construct is in the futuristic realm and its practical application seen with some skepticism. However, there is a possibility of good co-operation between the IN and IAF, especially given that with both services having their respective communication satellites, communication compatibility should not be a problem. However some examples of MDW could be as follows:-

- A Guardian Predator Drone, which as per some reports, is likely to be acquired by the Indian Navy, which has a huge endurance, di

[6] www.dsta.gov.sg, Future Communications in a Net work Centric Paradigm, pg 3

recting an IAF/Naval fighter aircraft or passing on information in real time to an Air Force Air Early Warning (AEW) aircraft, which can then direct Air Force/Naval aircraft for a mission. [7]

- An AEW aircraft of the IAF vectoring a Naval fighter aircraft in an Air Defence scenario over sea or vice versa i.e. an IN AEW helicopter, Kamov-31, operating from a naval ship at sea and vectoring an Air Force aircraft in an AD scenario.
- A P-8I air craft of the IN, shepherding an IAF aircraft like Jaguar in the maritime strike role to engage a surface target. P-8I can also be used for comprehensive picture updates.
- The P-8I aircraft has the capability to undertake Synthetic Aperture Radar (SAR) mapping of targets inland, which can be passed in real time for targeting by the Army or IAF.
- During NGFS operations, Naval ships may need gunfire spotting support from Army or IAF helicopters for accurate shore bombardment.

Another possibility of MDW is in the field of Special Operations. As is well known, the Indian Navy's Marine Commandoes (MARCOS) operate in various contingencies with the Indian Army. The most important co-operation is in the Kashmir valley in the 15 Corps Area of Operations. Whilst the MARCOS provide water front security against terrorism/infiltration through Wular lake, they are also equally adept in the traditional concept of CI ops and are being regularly utilized in that role. Similarly there is possibility of special forces co-operation between the IAF Garuds and MARCOS in aspects like duck drops, infiltration ops etc. Further, special forces across all services have the niche capability to undertake operations like counter insurgency, counter terrorism, hostage rescue, intelligence ops, unconventional warfare etc. In all of these there can be tremendous co-operation during MDW.

[7] The Economic Times, Dated Jul 15, 2018

Constituents of MDW from Naval Perspective

As far as Maritime operations are concerned, all units which are part of the multiple domains have to be on the common operating grid and that is provided by Maritime Domain Awareness or MDA. It is an all encompassing term that involves being cognizant of the position and intentions of all actors, whether own, hostile or neutral, in the constantly evolving maritime environment or areas of interest. It entails intelligence on foreign units including warships, submarines and aircraft for monitoring their deployment trends and intentions, as also information on merchant ship movements, which is vital for protection of own trade and forewarning of any untoward activity like piracy, maritime terrorism etc. Information on fishing fleets helps in detecting unwanted presence of rogue boats.

An effective MDA organization therefore encompasses the oceanic areas to be kept under surveillance and serves to help establish traffic patterns prevailing at choke points and in coastal areas. Maintenance of MDA is a unique requirement for maritime warfare governed by international law, since maritime conflict zone is neither static nor limited by geographical constraints. Hence even in a conflict zone unless otherwise notified, suitable international shipping traffic is likely to continue. [8]

The key ingredients of MDA are Intelligence, Surveillance and Reconnaissance (ISR). However the most important enabler of MDA is Network Centric Operations (NCO). As a result of transformation in warfare brought out by advances in information collation and dissemination technologies, widely dispersed forces can be networked with real time exchange of information, which can also include Army and Air Force assets. NCO forms the backbone of MDA concept, whereby integrated battle space awareness is developed to a high level by data linking of widely dispersed sensors available with the force. This information is collated, sifted and analyzed across the force in real time which can

[8] Indian Maritime Doctrine,INBR 8, 2009,74,75

reduce the fog of war to a great degree. NCO is aimed at exchanging information across domains such as Air Force, Army, Coast Guard etc. This will also employ space based capabilities with application and integration of satellites for communications and networking. These provide connectivity across the maritime theatre and strengthen the Information Decision Action (IDA) loop with rapid, real time, information collation and dissemination.[9]

All elements that contribute to MDA need to be progressively improved upon. Amongst these, the main thrust areas include Surface and Aerospace Surveillance, which further include satellite based surveillance, aircraft, UAVs, and ship-borne and shore-based surveillance systems. Joint and single service identification systems, with an ability to discern between friend, foe and neutral needs to be pursued, in conjunction with the surveillance effort. National advancements in information and communication technology also need to be harnessed, for maintaining secure, reliable and rapid information exchange. These will also aid in development of networked operations, and provide greater efficiency and effectiveness. Efforts to develop a broader Air Domain Awareness (ADA) as part of MDA also needs to be pursued, including by harnessing air traffic information.[10]

Capability for safeguarding and also obtaining information in cyber space is critical and needs to be continuously developed. While MDA is enabled by networking, it is NCO that gives it full effect. The Indian Navy is developing itself as a network centric force, wherein aspects like Satellite Capabilities, NCO capabilities across the IOR will be predominant factors. Satellite capabilities for maritime and joint operations need augmentation to cater to the needs of NCO, offset vulnerabilities and increase redundancy. Further Airborne Early Warning aircraft enable networked operations.

[9] Ensuring Secure Seas: Indian Maritime Strategy, p 66

[10] Ensuring Secure Seas: Indian Maritime Strategy, p 95

Network Integrity is another field, which requires exchange of operational data and information for targeting and cooperative engagement and requires establishment of Secure and High Quality of Service (QoS) networks, with assured integrity and adequate bandwidth for a high tempo of operations. The networks need to be developed over multiple media, and upgraded periodically to meet contemporary operational requirements. The establishment of Information Management and Analysis Centre (IMAC) at Gurgaon has been a major step in this regard. This is being progressed and further developed in terms of technology, with linking of systems for sharing of data, and computer aided correlation, filtering, selection and dissemination of relevant information. Technologies for Multi Platform, Multi-Sensor Data Fusion (MPMSDF) are being pursued. This process will be strengthened by the Information Fusion Centre for Indian Ocean Region (IFC-IOR) commissioned recently at Gurgaon for the Indian Navy, which will also contain information on white shipping. The same will also be available from foreign observers, manning the IFC-IOR, on similar lines as the practice in Singapore IFC, where there is also an IN officer posted.

An important aspect for data integration is that Geographical Information and Position Fixing Systems need to have a common data base. The use of common data across different units requires a common, geographical information system, across domains, with adjustments for inherent errors across dispersed spaces and dimensions. This needs to be pursued alongwith indigenous satellite-based position fixing system, to provide requisite accuracy to enable precision weapons engagement for maritime and joint operations.

Whilst the maritime domain has been covered extensively in the paragraphs above, another important sub-domain that needs to be considered in the context of MDW is the underwater domain. With the proliferation of submarines around the world, both conventional and nuclear, submarines play a very important role in various aspects of warfare, be it warfare at sea or influencing affairs on land by use of sub launched cruise missiles including IRBMs/ICBMs launched from submarines. Also the Remotely Operated Vehicles (ROVs) may in future replicate the UAVs in the underwater spectrum and add another dimension to the concept of underwater warfare, adding to the concepts of surprise and deception.

Conclusion

MDW is a concept, which is being driven by the US Army to bring to bear the best capabilities of various services and domains to effect in a war scenario. Though traditionally there have been three domains of warfare, i.e. land, air and maritime, while considering the concept of MDW, various other domains such as cyber, space, outer space etc are also being factored in, as also technologies such as Artificial Intelligence, robotics, lasers etc. Though MDW has been in vogue for ages in various types of warfare, especially in case of Amphibious operations, the US initiative is a concept as of now and is meant to ensure that they remain uncontested and ahead of their potential adversaries, i.e. China and Russia in case of a war scenario in totality, especially in the domains of cyber and space. However, the factor which will underscore the efficacy of MDW would be the speed and security associated with communications, network centricity as also the safety and protection of satellites, which themselves can become vulnerable with weapons like Anti Satellite missiles.

***Vice Adm HCS Bisht, PVSM, AVSM, NM (Retd)** is a former FOC-in-C, Eastern Naval Command and a Distinguished Fellow of the CENJOWS, New Delhi

MULTI DOMAIN WARFARE IN THE INDIAN CONTEXT

Air Mshl Ramesh Rai VM (Retd)*

Capturing the exact character of a future war with definite certainty is extremely difficult, but it could be assumed that a future war will be multi domain and multi-dimensional with information domination. The military environment will keep getting infused with rapid advances in precision, range, stealth, artificial intelligence, robotics, weapons and missiles implying that threats from air, land, sea and space will come with enhanced lethality. With cyberspace having emerged as the fifth domain, we can safely postulate that cyber threats will combine with other domains enhancing the lethality further. Our adversaries are likely to blend conventional, asymmetric and hybrid capabilities across all domains and expand their military activity beyond the air, sea, and land to space and cyberspace. This compels us to re-examine our military concepts and doctrine since domination in war will no longer be gained through domination in a single domain and the focus needs to shift to cross domain synergy. Cross-domain synergy implies employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of other. The idea of operating across domains isn't very new as each service, for example, has been using the space and cyberspace for information sharing and air force operations routinely have an impact in other domains. It is the rapid growth of capabilities tied down to the space and cyber domains that calls for combining them to evolve a cohesive war fighting concept. Presently, operations are conducted in and occasionally across the five domains; the need is to move further and transform making domain integration a norm rather than an exception.

India sits in the throes of immense security concerns, between its Western and Northern neighbours. Pakistan has mastered the art of employing regulars and irregulars along with non-state actors and insurgents. It is already waging a hybrid war of sorts in Jammu and Kashmir. China's doctrine of unrestricted war conceptualises "Cocktail Style" methods of combining different forms of warfare.[1] Chinese doctrine for future war conceptualises that war would no longer be about using armed forces alone and the whole nation and the society would become part of the battle given the penetrability of cyber, space, information, and economic warfare.[2] We face an environment of a rising China, and an ever belligerent Pakistan, that will bring integrated multi-domain approach to war fighting to try to counter our conventional strength. We can expect Pakistan to employ irregular forces along with their conventional to complicate the battle and are probably moving quickly to integrate cyber and space tools with their conventional forces. In this backdrop, India would certainly have to contest a multi domain war and formulating a credible multi-domain warfare capability would be a prerequisite for victory.

Our military forces have been structured as three domain-centric Services i.e. the Army, Navy and Air Force and these translate to the three kinetic domains e.g. land, maritime and air. The Army and Navy were formed when conflict was possible only in the land and maritime domains. The Air Force was created after WWII when impact of warfare in the air domain was significant. The emergence of AIR as a domain had led to the evolution of the Air Land Battle Concept for battlefield coordination between surface and air forces. In future battles, the use of space and cyber domains will become increasingly likely and their battlefield coordination would likewise be imperative. A fundamental

[1] http://www.dtic.mil/dtic/tr/fulltext/u2/a509132.pdf..unrestricted warfare

[2] Ibid.

principle of our warfare concept has been the recognition and acceptance of separate domains in which operations were principally led by one Service and capabilities of the other combined to influence the outcome. Implying that advances in one domain could be leveraged by employing some of the capabilities of the other domain/domains. Hence the cross-domain employment has been in vogue in our armed forces and the concept needs to be taken further and to intermesh space and cyber domains in toto war fighting.

The multi domain warfare concept at its very core entails combining fires capability across all domains by employing joint and combined kinetic and non-kinetic fires to achieve the desired effects. It is in this realm that the services will need to evolve the concept by first understanding how space and cyber domains will contribute to war fighting, understanding the tenets and then identifying the organisation, doctrine, technology and capability that would be required for their integration. It will require redefining concepts of operations, command and control approaches, organisational forms, force structure and support in these domains. Once identified, we would need to set up an institutional process that conceives the organisational, structural, technological, capability enhancements, operational reforms and demonstrates them to be attainable. The institutional question looms large here, as at one end each service calls to form separate space and cyber domains and at the other is the need for combined space and cyber capabilities to be shared across services much like sharing airpower. Irrespective which model is followed there will be coordination, cooperation and prioritizing issues which will have to be overcome by laying down enabling policy, structures and communication networks and knowing that we are to fight as a joint team and that multi domain solutions and will walk with us in the future.

The essence of multi domain warfare is combining all five domains. Our military forces have been structured as three domain-centric Services i.e. the Army, Navy and Air Force and these translate to the three kinetic domains e.g. land, maritime and air. Just like the Air

Land Battle had led to the creation of battlefield coordination between surface and air forces through respective commands, Cyber and Space Commands would have to be established to conceive and co-ordinate operations in respective domains. These commands would need to generate, control, prioritize, deconflict, integrate, synchronize their operations to accomplish the assigned mission in concert with other domains. Thus, at the very outset there would be a need to establish space and cyber commands for multi domain warfare to actualize.

We must not conceive multi domain warfare as operations merely combining with space and cyber domains to enhance the air/land/sea campaigns. These must be conceived so as to generate offensive and defensive capabilities from these domains as well to create complex dilemmas for the adversary. The cyber domain would have to operate through all warfare domains at the strategic, operational and tactical levels to execute and combine cyber ISR, cyber-defence and cyber-attacks with kinetic fires to create necessary effects. The space domain would be a significant force multiplier by providing communications, positioning, environmental monitoring, space-based intelligence and ISR. U.N. treaties prevent nations from weaponizing space hence space cannot used to cause physical damage to adversaries. The biggest challenge lies in how these operations will be integrated in the overall strategy to meet the military and national objectives.

The complexity of space and cyber military operations and integration across domains argues for laying down a foundation to include multi domain operational concepts, infrastructure, communication networks and inter domain connects. There would be issues of structures, command and control from a functional, organizational or operational standpoint. These would have to be resolved. The challenge would be to readapt from domain-centric focus to the multi-domain environment at the three levels of war. Since the operational level is responsible for the integration and alignment of tactical level missions to achieve strategic objectives, a conceptual framework at the operational level would be needed once enabling policy, operational concepts, structures and procedures are in place. Multi-domain expands the targeting landscape based on the extended ranges, lethality, integrated air defences, cross-domain fire support, and cyber/electronic warfare systems[3]. There would be a need to understand these expanded battlespaces and how our capabilities in each domain can combine at the operational level. Various approaches would need to be explored and experimented to arrive at viable solutions. Once the operational level commanders understand the future battlespace, they can begin to assess command and control relationships and how they will execute multi-domain missions and how to train for them.

Multi-domain war fighting entails knowledge of what is happening in various domains that could affect the operational situation. Hence a multi-domain connect is necessary if we are to integrate and exploit information from multiple sources, including sensors, databases, intelligence, reconnaissance, and surveillance to formulate an integrated response. Best suited tool for such a task would be encrypted data link architecture for net-centric warfare across each domain. The architecture should provide connectivity within the domain and with other domains. Such a distributed network system would need to have a high degree of connectivity so as to take the least time to establish an accurate common operational picture to facilitate information sharing for enhanced situational awareness. Thereafter, comes collaborative targeting for which a targeting and decision grid would have to be appropriately conceived and created in the network.

To build a connect between sensing and targeting across omains we would need to combine aspects of network-centricity, combat cloud and combined fires. This tall requirement which will call to bring together the operational, technological, technical and analytical ingenuity of the entire nation so that we develop our very own military data distribution

[3] https://overthehorizonmdos.com/2017/08/28/multi-domain-battle-tactical-implications/

system. For this, we will have to conceptualise and articulate the nature and characteristic of our approach to a network centric war and then define the entities, their mission capabilities and technologies to combine their operational capabilities. We will need to define the grid construct of the sensing, information, effects and command grids and layer them to receive, process, store and communicate information over the network i.e. quick and secure exchange of tactical data like pictures, text messages, imagery and digital voice in real time to be used by combatants / platforms / entities in each domain. Sensing and Information grids would form the basic construct to amalgamate the big picture .Sensing grid could comprise every sensor that can be hooked on to the net, anything ranging from dedicated sensing systems even to the single soldier on the battlefield. The air force already has in place its integrated air defence system (IADS) with the most dominant sensor i.e. the airborne warning and control system (AWACS) intermeshed with air borne, land-based radar networks. The IADS would need to be extended to other battle field and ship borne sensors and made more robust with ground-based air defence systems such as Surface-to-Air Missiles and Anti-Aircraft Artillery, along with fighters at airbases around the country. The combat cloud would be the repository of sensed information from which any combatant could extract the combined 'big picture' for improving situational awareness in his respective context. This would not be an ordinary task since sharing the right information with the right person at the right time would be a tough challenge. The combat cloud would enable targeting information and designation as data could be pushed from one node to another without the need for the platforms to communicate directly thus expanding the battle space.

Shooters, manned or unmanned, from each domain would form the effects grid. They will engage targets based on sensor grid information distributed across the communications grid and combine to create desired effects. The combination of manned and unmanned aircraft, surface-to-air missile systems, surface to surface systems, ship borne systems, electronic jammers and cyber systems will have to be well conceived to get the desired results. For example, we could carry out a SEAD attack on the enemy air defence system either by using the AIR domain (aerial bombing) or CYBER domain (cyber-attack on routers, data base, computers or displays) or a combination depending on the effects a commander desires. Such decisions could be conveyed on the command grid that would connect Commanders in the field to decision-makers at the headquarters or command and control centres. In this grid, the prime function would be of passing instructions to the field commanders to actualize the combine of various fires over the entire battlespace. However separate combat models for a conventional war and an irregular/hybrid war would be required since these come with disparate operational concepts and course of action analysis.

Multi domain warfare will have to rely profusely on data and connectivity for success. Hence, a robust network, with high band width and full interoperability within domains would be necessary. In warfare terms, it would imply heavy collaboration between information sharing and combining fires across domains which calls for a well-conceived and developed network, network support, information sharing infrastructure, the combat cloud operational construct and the decision-making loop. It is apparent that such an arrangement would be highly complex and complicated requiring extensive technological and operational agility in weaving them together. The Chinese are known to be developing such a network with the four multi-domain grids. We will have to not only match up to the battle field complexity in terms of systems, if we are win a future war, but our training would have to lay great emphasis on orchestrating a multi domain network centric war. Fundamentally, once networked, own decision-making must get faster so that it stays within the enemy's OODA loop cycle. In this will lie the key variable that will determine success or failure. In networked warfare, the time compression in decision making and consequent force application is pivotal to winning a war. Our commanders will need training for this important dimension of conducting warfare as success or failure will depend on which force is better trained in using networks.

India has been the target of the irregular and unrestricted warfare capabilities of Pakistan and China. The hybrid threat will be more pronounced in the future as China consolidates on its new operational concept of fighting an informationalized war. In a two-front war, the hybridity could vary from a mix of regular forces using conventional weapons intermeshed with irregular forces using irregular tactics with support of terrorists and insurgents, cyber intrusions, and possibly some dimension of social and economic warfare. While the armed forces would be called upon to tackle the regular war component and portions of the irregular war, the cyber intrusions, economic, industrial or social dimensions would need a whole of nation approach. This would call for the war to be centrally orchestrated at the highest level after understanding it in its entirety to evolve a cohesive response for each threat or a combination. Core members of a future war team would need to include military experts, cyber experts, technologists, terrorism and insurgency experts along with decision makers from within the government at the highest level. Their task would be to develop a conceptual frame work to orchestrate coordinated warfare in every domain. As with the story of the blind men and the elephant, the team would have to not only look at different facets of the changing character of war, each trying to describe what they see, but look at the whole elephant. This would be required urgently to put our capability building and organisation in the right perspective.

Hybrid war is amorphous in nature, the trajectory it takes is difficult to predict. It has the potential to transform into conventional or a multiple sub-conventional war. India would have to stop seeing a future conflict through the prism of a conventional military response only since a hybrid war would need a hybrid response. In this complex scenario, our armed forces, which have been equipped, trained, and structured to fight conventional wars would have to readapt conceptually. While retaining their conventional capabilities, they would have to adapt to engage the irregular and sub-conventional components in the cyber back drop/multi domain construct.

Air forces are already well versed with multi domain operations but the aspect that becomes critical for air forces is to fly and fight in cyberspace. Air forces conduct and win wars by maintaining full spectrum capability i.e. control of the air, strike, air defence, air mobility and ISR to assure the surface forces would be able to operate without undue interference from enemy air power. In a future hybrid, multi dimension war, criticality would lie in retaining full spectrum capability that could be contextually flexible to be effective in regular and irregular wars in, from and through cyber space. The key doctrinal update would be to integrate the net centricity into the war fighting doctrine and operational concept. Air forces exploit the third dimension of the operational environment and leverage speed, range, flexibility, precision, tempo, and lethality to create the desired effects within and from the air. This will now require an intermesh with all domains through/with/from the cyber and space domains. From a multi-domain perspective, air force would have to train to apply combat power across the strategic, operational, tactical levels of war and simultaneously control the tempo of operations in our favour in concert with the surface forces.

Threats of the future will compel us to change the way we must fight. Today, our adversaries leverage technological advances to blend space and cyber operations and the battle field acquires a multi domain complexion. This invokes us to evolve a multi domain response which entails combining fires across domains to create the desired effects. For such a transformation, multi-domain connects in our minds and heart first and then a combine of our sensors and shooters is necessary. A multi domain war would have to be structured as a Net-Centric War and orchestrated like so. Structuring a Network Centric War will not be easy and will require defining the battle space players with their roles and responsibilities, nature of information required to be exchanged, their connectivity, the degree of coupling across domains and developing the technologies for the same. There will also be challenges at the policy, organisation, structures, communication and thinking level. These will have to be overcome. As with any new military concept, the success will depend on the leadership's commitment to change and to accord a forceful direction to bring disparate Service interests and functional areas (space, air, sea and land) together to function through a common network. All stake holders will have to come on board shedding respective domain biases and endeavour to understand what is of importance in multi domain operations to prioritize then break domain stove pipes and integrate. Above all, it will require a cultural change by broad consensus and acceptance of the whole idea.

***Air Mshl Ramesh Rai, VM (Retd)** is a former AOC-in-C, IAF Training Command

SPECIAL OPERATIONS FORCES - INTEGRAL TO MULTI DOMAIN WARS

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

Before evolving a conceptual framework, structures, role, organisational and operational effectiveness and efficacy of Special operations Forces (SOF) in the future nature of wars characterised by Multi Domain warfare (MDW), it will be prudent to comprehend both MDW and Special Operations in the Indian Context.

Multi-domain battle is a concept designed to overcome the adversary's integrated defensive capabilities, avoid domain isolation and fracturing, and preserve freedom of action. The SOF must be able to penetrate adversarial defenses at a time and place of our choosing, in more than one domain, by opening windows of domain superiority to allow maneuver inside the adversary's integrated defense. The rate and speed of current and future world events will not allow the time to synchronize federated solutions. In order to present the enemy with multiple dilemmas, SOF must converge and integrate multi-domain solutions and approaches before the battle starts. The need is to become sensor-shooter agnostic in all platforms, and maintain a common operating picture.

The MDW concept, principally involves responding to a set of strategic-military *and* operational-tactical concerns, which are: -

- How to deter the escalation of violence, defeat adversary operations to destabilize the region, and turn denied spaces into contested spaces should violence escalate?

- How to manoeuvre from contested strategic and operational distances and with sufficient combat power in time to defeat enemy forces?
- How to conduct deep manoeuvre by air, naval, and/or ground and special forces to suppress and destroy enemy indirect fire and air defense systems and reserve forces?
- How to enable ground forces to defeat the enemy in the Close Area?
- How to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

The multi-domain battle concept is expected to integrate three key areas, organizations and processes, technology, and people. Changes in organizations and processes will be designed to provide different and better-focused Army tools to joint forces to overcome loss of superiority or parity in certain domains, particularly on land along our disputed borders, air, sea, cyberspace and internal security challenges. The major domains of warfare remain unchanged, it is the simultaneous, non linear exploitation of all domains in many battle spaces which changes the dynamics of future wars and hence the imperative to build cost and combat effective capabilities.

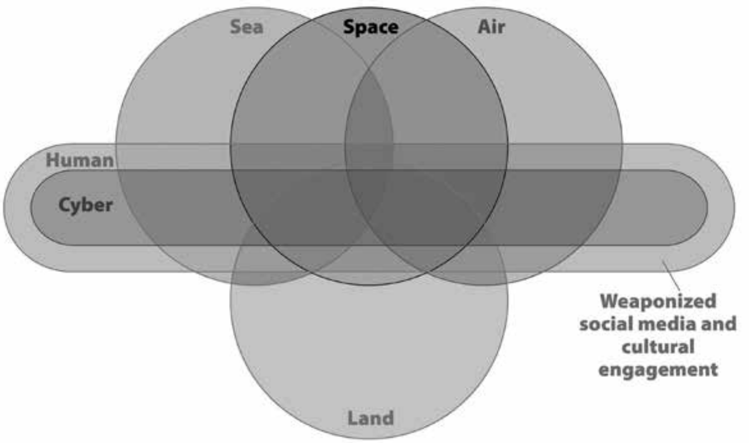

Figure. Multi-Domain Battlefield (Graphic by Arin Burgess, *Military Review*)

The nature of war has been and will remain an act of imposing one's' will on the adversary. However, the character of war i.e. how future wars will be waged and fought has undergone a change due to numerous geo-political and socio-economic factors, technological advancements and military innovations. Future conflicts are likely to involve states or a state-sponsored actor as one of the participants of the conflict. States will also predominantly determine the spectrum, location and duration of conflicts. The last major driver of change that has had the foremost impact on character of war and the future operating environment is technology. Technological developments including artificial intelligence (AI), machine learning, data analytics, additive manufacturing, robotics, unmanned weapon systems, nanotechnology, quantum computing, brain-computer interface, bio-technology etc are rapidly changing the way future wars will be fought. Arguably the most important potential technology of all is AI. AI would overcome the four challenges of data processing – scale, speed, complexity, and endurance – necessary to analyze the increasing data from connected sensors. This will enable unmanned systems to have enhanced mission duration and effectiveness, reduce operating costs and risks to military personnel. Advancement in AI will also enable development of other complex technologies including autonomous systems, additive manufacturing, biotechnology, manufacture of advanced materials etc.

The security challenges for India can no longer be defined and definite, as these are likely to be hybrid, conducted in many battle spaces by multiple means driven by a collective ideology, plausibly without any direct attribution and without any overt physical military application of combat power ab-initio. A collusive or collaborative threat from both China and Pakistan is a probability which India should consider seriously. 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 its all weather friend China and a collaborative threat from Pakistan would be imminent, as it takes on a mightier India preoccupied with China along the Northern Borders. Hence, it would be prudent to conclude that during a future Indian military conflict with China, Pakistan will come to China's military aid but reverse may be likely but not a serious threat.

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 / 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. 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. In effect Indian armed forces should be present relevant and future ready. As the future security challenges are in multi domain India needs to build cost and combat effective capabilities and SOF will be the ideal start point.

Wars in today's context cannot be fought with outdated organisations and structures, wherein the Army, the Navy and the Air Force conduct operations in a linear stand-alone mode, with coordination and cooperation dependent on personalities. War is a joint endeavour, wherein all elements of national power and all resources of the union are synergised. This truism is even more relevant in the present context, as warfare today is a complex phenomenon likely to be waged in the multi-dimensional and multi-domain space. This complexity will increase in the future. The reasons include high technology, the nature of modern war, new threats and challenges and the reality of nuclear weapons in the arsenal of our potential adversaries. Consequently, a SOF and a joint force, which acts in an integrated manner, are not just desirable but an imperative. The complexities of the future security environment demand that India be prepared to face a wide range of threats of varying levels of intensity. Success in countering these threats will require skillful integration of the core competencies of the service specific SOF into an integrated force structure. However, reorganisation by itself will not succeed in achieving such integration. What is also required is a change in mindset, a change that makes every soldier, sailor and air warrior feel that he is a member of the Indian Armed Forces and not just the Indian Army, the Indian Navy or the Indian Air Force. This is best achieved by first integrating the Special Operations Forces (SOF), a force which is by far the most battle hardened and combat rich in the world having a proven record of success under the most challenging situations. The SOF is not only a force multiplier but also a game changer, a force best suited to adapt to future multi domain warfare in the Indian context.

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

The recently released 13 page Land Warfare doctrine amplifies the SOF employment. Quote ' Special Forces Capability - Special Forces shall be equipped, structured and trained to ensure their application in *multiple employment opportunities for exponential gains*, to achieve our military objectives. Their equipment profiling, standards of training and employment strategies must form a vital component of our overall deterrence capability, both in unconventional/ conventional domains.' further stating that the 'Force Projection Capability- India's role as a regional security provider mandates a force projection capability to further our national security objectives. *A Rapid Reaction Force comprising Integrated Battle Groups with strategic lift and amphibious capability will be an imperative for force projection operations*.' However, there appear obvious contradictions in the signals emanating from the Armed Forces and the MoD on the proposed restructuring of the SOF, with the latter biased towards raising a Special Force Division capable of effectively executing more surgical strikes and the armed forces wanting a 360 degree focus on structuring and employment of Special Forces in critical missions at the Strategic- operational levels of war prevention and war fighting.

The Land warfare doctrine goes on to simply but logically highlights the security environment, concerns and the nature of future wars. India's security concerns are impacted by a dynamic global and regional security environment. As India transforms from an emerging and rising power to a risen responsible power, it will need credible military capabilities to project military power, assist friendly foreign countries in times of crisis from unconventional threats and HADR. The continuing proxy war with Pakistan, the ever increasing and omnipresent threat from terrorists, the imperative to safeguard our national interests and assets dictate that we enhance capacities and build capabilities to face future threats and challenges. Future conflicts will be characterised by operating in a zone of ambiguity where nations are neither at peace nor at war - a 'Grey Zone' which makes the task more complex. Wars will be Hybrid in nature, a blend of conventional and unconventional, with the focus increasingly shifting to multi domain Warfare varying from non-contact to contact warfare. Non-Contact and Hybrid domains of conflict are now being integrated into the conventional and sub conventional realms and could be non-declaratory and non- attributable in its execution, a characteristic of Grey Zone Warfare that needs to be catered for.

Indian Armed Forces would have to be prepared for multi-domain battles with varying intensity and duration. These would include sub-conventional conflicts involving radicalized proxies and limited use of latest technologies to conventional conflicts of varying scale involving long duration non-contact phase, hybrid warfare, under an overall nuclear overhang. Information warfare including cyber, psychological and electronic warfare resources will be increasingly employed both during peace and war. Conventional conflicts post 2030 will gradually see the use of networked artificial intelligence supported stealth unmanned systems in land, sea and air domain, precision guided hypersonic weapons, long range high energy weapon systems, space based sensors and weapons, to name a few. These advanced technologies would be fielded by not only major but regional powers as well. This construct dictates that the nation build adequate and appropriate capabilities especially so in terms of SOF.

At present each service has its own SOF which has grown over the years. These are service specific and more often than not, there is competition and conflict of interests, rather than cooperation and coordination, be it their roles and tasks, equipping, training and command and control. Existing SOF of the Armed forces include nine Parachute (Special Forces) Battalions and five Parachute Battalions of the Army, an 800 strong Marine Commando Force (MARCOS) organised on the concept of the US Marine SEALS and a 1000 strong IAF Garud. The NSG (SAG) and the Special Group manned and led by the Army for internal security and hostage rescue are under the MHA. These are elite forces, where every man is a volunteer, highly trained and motivated. This force is among the most battle hardened and combat rich force equal to if not better than the best in the world. The SOF is both force multiplier and substituter. These forces provide the theatre commanders with low cost high effect options to target high value military objectives in depth areas, thus giving the much needed strategic and operational reach during war. SOF are assigned missions at the strategic, theatre and operational level and tasked to execute direct action, intelligence, surveillance and reconnaissance tasks during war to delay, disrupt and destroy high value targets in depth areas. During peace they are mandated to execute CT and CI operations, special reconnaissance, hostage rescue, capability building of Friendly Foreign Countries, and above all, training for war. The recently demonstrated capability 'Ex Bahubali' by the Indian Air Force of lifting nearly 500 tonnes in a single wave is an apt testimony if required that India's SOF have the capability and ability to intervene with a substantial force in its areas of interest.

What is lacking is formal structures to optimize the potential of the SOF. It is an imperative to structure, equip, enable and empower our Special Forces to be effective contributors to the future MDW challenges. These are cost effective forces with high payoff and a high degree of assurance of success. In 2012, the Naresh Chandra task force recommended creation of a Special Operations Command (SOC), Cyber and Space Commands. With the Modi led NDA government demonstrating an urgency and resolve to address National Security concerns, it was hoped that the three commands, as recommended will be finally sanctioned, paving the way for an effective command and control structure and the much needed jointness and synergy among the SOF. The Government for reasons not known has shied away from exploiting this force multiplier and decided to raise a Special Operations Division (SOD) under a Major General/ equivalent officer, which is at best a half measure and will be detrimental to effective employment, deployment and exploitation of SOF. A major weakness in this interim arrangement is the lack of a lean, mean, agile and versatile joint force under a single commander empowered and keyed in to the national decision making apparatus. This can only be achieved by raising a SOC. The SOC should be structured and organised as a truly integrated tri-service command with integral lift capabilities.

The tasks assigned to SOC during war would be to secure/

destroy high value targets in the strategic domain and operational depth in furtherance of national military objectives. During peace, or rather no war no peace the SOC will be the first responder to any emerging or impending threat to our national interest in the region. The scenarios for its employment could include hostage rescue of Indian nationals and diplomats, evacuation of Indian nationals, reinforcement or assist in evacuation of United Nations Peacekeeping Missions, assist FFC from threats by inimical elements within, albeit on invitation, assist in HADR missions in the region and beyond and capacity building of Armed Forces of FFC. An empowered SOC will also be a credible 'threat in being' contributing to war prevention. Given the envisaged roles and tasks the SOC has to have a direct access to the national decision making body (CCS) in times of crisis and strategic missions. The national security structures and the SOF should prepare to counter threats in the multidomain warfare, linear wars now being only a subset of multidomain wars. The SOF are not only agile but also most suited to adapt to future security challenges. The role of the SOF to meet and mitigate these threats that undermine India's strategic interests needs to be refined and defined.

Another major implication of the future operating environment is the necessity to accord higher priority to information warfare and develop suitable concepts that fully utilize all its capabilities. This will enable, quickly establishing dominance over the adversary in any future conflict. Large investments would also need to be made to develop new technologies, in conjunction with the civil private industry, as most of these technologies are dual use. This will entail framing suitable policies for increasing interface with the civil industry. The Armed Forces would also have to assess the impact of new technologies especially as they would increase transparency of battlefield, precision, range & lethality of engagement. Thus, over the long term, existing manpower levels may need significant reduction so that adequate funds are available for capital acquisitions. However, sub-conventional conflicts will continue to be manpower intensive in the coming decades. This is primarily because suitable technologies that will enable better force effectiveness with minimal collateral damage, will take considerable financial investments. Battlefield transparency and speed of decision making by utilizing AI will reach phenomenal levels, thus posing cognitive challenges for armed forces relying on human manned legacy systems. Unmanned systems that are autonomous with precise and intelligent targeting capability would require that own forces must be comparatively smaller in size, task oriented, highly mobile & with decentralized decision making. This will enable them to disperse and concentrate as per operational requirement. This is where the SOF will be critical and crucial to operating in the multi domain battles. Military leadership challenges will be posed by speed of maneuvers, multiple domains in which operations will have to be conducted and 24x7 nature of operations. In the absence of contact leadership, morale of troops due to the numerous battlefield challenges will also be impacted. Leadership challenges will again dictate that Special Operations capability be exploited as these will be the first responders with higher probabilities of success in high risk missions likely to manifest in MDW.

***Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)**, Director CENJOWS, is a former DGMO of the Indian Army

CYBER WARFARE : A KEY ELEMENT OF MULTI DOMAIN WARS

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

“War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously.” Actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption can be termed as cyber warfare. Strategic cyber-attacks could be on a nation’s critical primary infrastructure and utilities, whilst operational cyber-attacks are against adversary’s military. A very comprehensive definition of cyber warfare could be “The strategic, operational, and tactical level action across the spectrum during peace, crisis escalation, conflict, war termination and restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.” It can include denying battlefield commanders information, keeping sensitive messages secret, spreading propaganda, traditional hacking and so on. Defensive cyber operations would be to protect information in any form, maintain its confidentiality, integrity and availability. The aim of information warfare is to: “corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity and availability of one’s own information”. Cyber warfare involves targeting computers, online control systems and networks and grids of national utilities and of military. It involves both offensive and defensive actions. Unlike conventional war-fighting which requires logistically supported standing armed forces with kinetic weapons, the cyber attack can be initiated from a single computer by a single operator at an unknown remote location. The disruptive power of cyber warfare has been well established and therefore all major countries are building capabilities for both protective and offensive purposes.

The number of cyber security incidents has been gradually increasing in India. These incidents include phishing, website intrusions and defacements, virus and denial of service attacks among others. Pakistani hackers compromised 10 Indian websites which included National Aeronautics Ltd, Army Institute of Management and Technology, Defence Institute of Advanced Technology, and the Board of Research in Nuclear Sciences. Indian Government took the first formalized step towards cyber security in 2013, by formulating National Cyber Security Policy (NCSP). It also announced in mid 2018 a plan to create a new tri-service agency for cyber warfare. The Defence Cyber Agency (DCA) will work in coordination with the National Cyber Security Advisor (NCSA).

Cyber Domain

To make sense of cyber warfare requires understanding the cyber domain, and accurately defining the cyber environment. Operational planning must take into account the spectrum of threats. Understanding the complexity of implications and the intentions of actors will help develop effective cyber warfare strategies. Cyber domain includes the Internet's architecture, devices connected to the Internet, and wired and wireless networks. Rather than existing within finite borders, it mimics other natural systems such as bacterial colonies and expanding galaxies, where billions of nodes expand in all directions. Complexity also stems from the exponential growth of computing power and the number of devices connected. As of June 2018, 4.2 billion (55%) of the 7.6 billion population of the world was connected on internet. There were nearly 1 billion web hosts with over 25 billion pages. Over 3.5 million blog posts are published on the Internet every day. Over 500 million tweets are sent and over 3.5 billion Google searches are made every day.

Since the cyber domain was designed for openness, security is not inherent in the system. Networks and the software built on top of them ride on an inherently open backbone, and as a result, multiple layers of security need to be built in to ensure system and data integrity. Vulnerabilities are akin to deficiencies in the human immune system. Several characteristics of the cyber environment shape cyber warfare, including rising levels of convergence (single device for many activities), the speed of interactions, the inextricable human element, and the empowerment of the individual within the cyber domain. Enforcing security measures such as installing anti-virus software, creating hard passwords etc all fall as task on the individual. Things happen at the speed of light and therefore any action in cyberspace can be faster and lead to far reaching geographic effects than in other domains. Military has to realize that electrons are much faster than ground forces. Because knowledge transmission is now nearly costless, individuals in loose networks can rapidly learn the most effective attack techniques and exploit previously unknown vulnerabilities. Because of the open design of the cyber domain, defence is inherently more costly and time consuming than offensive. Asymmetry in the cyber domain generally favors smaller and more agile actors. These actors often don’t have a permanent physical address and can mask their virtual ones. This is a key point in order to develop effective mitigation strategies.

Types of Threat

Cyber warfare can present a multitude of threats. At the most basic level, cyber attacks can be used to support traditional warfare. For example, tampering with the operation of air defences via cyber means in order to facilitate an air attack. Soft threats could be espionage and propaganda. There have been many cases of international electronic eavesdropping in the recent years such as stealing personal data by Chinese, and spying by US agencies against even partner nations as revealed by Edward Snowden. Sabotaging military C4ISTAR networks or civilian utilities is part of sabotage. Denial-of-service attack typically by targeting sites or services hosted on high-profile web servers such as banks, credit card payment gateways etc. Massive power outage caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma. Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion. It is a form of psychological warfare through use of social media or fake news websites. It is a form of warfare that seeks to de-legitimize the political and social system on which our military strength is based.

Cyber Attack Modus Operandi

The distributed nature of internet based attacks means that it is difficult to determine motivation and attacking party, and it is unclear when a specific act should be considered an act of war. All militaries are now hiring cyber-warfare experts to defend critical networks and security of sensitive information. Hacktivists or cyber-terrorists use their knowledge and software tools to gain unauthorized access to computer systems they seek to manipulate or damage often just to draw attention to their cause. Cyber has a great scope for industrial espionage.

Political Will

The execution of any kind of war is ultimately a contest of political will. Even cyber terror acts are designed to achieve some political objective, even to demoralize a populace or forcing a government to negotiate. Political objectives must be clear for the ultimate goal of cyber warfare. Whether or not a “Cyber 9/11” will happen, countries must prepare. Deterrence has to be built.

Military Effects and Approach

Historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid. The worldwide flood of powerful, inexpensive, and readily available commercial technology is mandating a much more sophisticated approach to military affairs. Computer processing power has been doubling every two years. In the new security environment, the pace of cyber, directed energy, nanotechnology, robotics, and biotechnology advancements is far beyond the normal capacity to predict their effects. Advanced information technology is also changing our perspectives of multi-domain interdependence. Ability to project conventional power is eroding swiftly as state and non-state actors acquire advanced capabilities to offset the military's strength. Unable to compete with powerful militaries, adversaries are leveraging technological advances to create their own asymmetric advantages. Numerous countries are working on high-powered microwave (HPM), directed-energy, and electromagnetic pulse (EMP) weapons that could destroy electronic systems.

Over 40 percent of the world's active satellites are in low Earth orbit. Adversaries can deliver effects from EMP through a multitude of nonnuclear modes that produce a wide array of outcomes ranging from temporary interference to system destruction. Other targets include ballistic missiles, submarines, aircraft, as well as man-packed systems. Militaries are also investing in inexpensive low-power jammers to inhibit the positioning, navigation, and timing necessary for effective strike operations. On the other hand advances in technology are improving adversary's ability to defend. Integrated air defense systems are becoming increasingly resistant to electronic suppression by using passive sensor technologies such as infrared search and track. These technology leaps are being augmented with surface-to-air missiles that have advanced tracking and longer ranges.

Cyber & Space Critical Combination

Denial access to vital satellites that are needed for intelligence, surveillance, and reconnaissance, communications, early warning, and navigation, could severely affect a Commander's planning, decision, and execution cycle and could render operations in the air, on land, and at sea ineffective. Space allows virtually unimpeded access to monitor missile-launch detection and missile tracking. Space systems have varying degrees of vulnerabilities. Satellites are nearly impossible to hide. They move along predictable paths, that can't be changed easily. Adversaries can employ a variety of attack options, including kinetically striking the ground stations, jamming or spoofing links, and using directed energy to dazzle or partially blind the satellite. ‘Parasitic microsatellites’ could latch onto a satellite and disable it, alter its orbit, or hijack the information gathered by it. EM Spectrum (EMS) is the sole medium for transmitting and receiving information and signals in space. The frequency bands that space-based systems use within the spectrum are fixed and cannot be changed after launch. One of the key constraints of this battle-space is that only 1 percent of the spectrum accounts for 90 percent of its military and civilian use. The effectiveness of the EMS is also complicated by electromagnetic interference between systems, EMP, and natural phenomena such as lightning, solar flares, and precipitation. Commanders must understand how to operationally assess the impact of forfeiting these systems and employ other capabilities. Consequently, military’s foundational principle of ‘centralized control and decentralized execution’ will be forced to shift to a distributed-control approach that adapts to operational changes. Local superiority in combinations of domains is now required.

Hybrid Response Approach

Cyber warfare touches all warfare domains - ground, sea, air, and space. The economic dimension is also significant. It could result literally in “death by a thousand cuts”. There is a need to address cyber vulnerabilities, increase information flow options, intelligence efforts, and coordinate security through prevention, adaption and appropriate reaction. Need to continually educate all military and civilian stakeholders in addition to securing the networks and nodes themselves. It is also critical to educate average citizens about enhancing the security of their own computers and networks. Education should include resilience training, hands-on scenario response, as well as technical and social engineering. While the vastness of the cyber domain could overwhelm any nation, collective understanding could improve response.

Cyber Weapon's Life Cycle and Vulnerabilities

Vulnerabilities that the cyber weapon relies on may be removed by manufacturer at any time. Once used, the signature of the weapon can be added to detection systems and blocked. Cyber weapons do not self-destruct and can be reverse engineered. Seizing the initiative means finding the zero day vulnerability and exploiting it before the enemy reacts. Retaining the initiative translates to constantly looking for new vulnerabilities, or finding back doors to ensure multiple paths into a system. While Shanghai Cooperation Organization (SCO) has shown interest in regulating cyber warfare and a collaborative effort between the SCO and NATO could produce more globally acceptable results, the technology is so expansive that any list of banned cyber weapons would be obsolete within days.

The New Multi-domain Imperative

The militaries face a new reality – one with "multi-domain" challenges. The way military builds its force, integrates its planning, and synchronizes its operations must change quickly. In modern military lingo, there are five inter-related domains: land, maritime, air, space, and cyberspace. The cyberspace domain is wholly man-made and is ever-changing. In the emerging 'multi-domain reality', an attack will often come from multiple domains simultaneously: jamming of radios and data-links, persistent surveillance, and precise, long-range fires. Military needs to instill in its commanders the ability to deal with ambiguity and incomplete information — the fog of war in the digital age — yet continue to operate in a manner consistent with the intent. Force posture, power projection, and presence in all domains will require greater integration of all services and agencies. The services are unfortunately still reluctant to trade proficiency in their core competencies for futuristic-sounding but potentially empty promises of multi-domain prowess. This will have to change.

International Cyber Warfare Evolves

In the 2006 war against Hezbollah, Israel allegedly used cyber-warfare was part of the conflict. Israel attaches growing importance to cyber-tactics, and along with the U.S., France and a couple of other nations, is involved in cyber-war planning. Many international high-tech companies are now locating research and development operations in Israel, where local hires are often veterans of the IDF's elite computer units. In September 2007, Israel carried out an airstrike on Syria and reportedly used cyber-warfare to allow their planes to pass undetected by radar. Following US decision to pull out of the Iran nuclear deal in May 2018, cyber warfare units in the United States and Israel are monitoring internet traffic out of Iran and have noted a surge in retaliatory cyber attacks from Iran. Similarly Iranian hackers were sending emails containing malware to diplomats who work in the foreign affairs offices of US and its allies. Cyber-warfare in the United States is a part of the American military strategy of proactive cyber defence and the use of cyber-warfare as a platform for attack. They are clear that a cyber-attack is just as a traditional act of war. In 2013 Cyber-warfare was, for the first time, considered a larger threat than conventional terrorism. As a doctrine, the Pentagon has formally recognized cyberspace as a new domain in warfare as critical to military operations as land, sea, air, and space. In 2009, President Barack Obama declared America's digital infrastructure to be a 'strategic national asset', and in May 2010 the Pentagon set up its new US Cyber Command (USCYBERCOM) to defend American military networks and attack other countries' systems. EU and UK have also set up a cyber-security operations centers. The government and corporate infrastructures will continue to be defended by US Department of Homeland Security and private companies themselves. China has plans of winning information wars by the mid-21st century. Others like Russia, Israel, Iran and North Korea are also having Cyber Armies. The PLA is having dedicated 'information warfare' units to develop viruses. Cyberspace technology is emerging as an 'instrument of military power'.

With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Cyberspace will become a main front in both irregular and traditional conflicts. The United States has used cyber-attacks for tactical advantage in Afghanistan and against North Korean missile program.

Chinese Cyber Warfare Ability

Nearly 120 countries have been developing ways to use the Internet as a weapon. China's 'hacker army' is known to have be 100,000 experts. China is using access to Microsoft source code and 'harvesting the talents of its private sector' to boost its offensive and defensive capabilities. They have had a number of high-profile cases of espionage, primarily through the use of a decentralized network of students, business people, scientists, diplomats, and engineers from within the Chinese Diaspora. Reportedly there are over 1,000 Chinese cyber spies. Chinese targets in the United States have included aerospace programs, including Space shuttle, C4ISR data, high-performance computers, nuclear weapons design, cruise missile data, integrated circuit design, among others. Chinese are also targeting India, Russia, Canada, and France. China's main target is to acquire foreign military technology. Chinese government uses new space-based surveillance and intelligence gathering systems, anti-satellite weapons, anti-radar, infrared decoys, and false target generators to assist in this quest. There is increased education of soldiers in cyber warfare. They have built many virtual laboratories, digital libraries and digital campuses. China's technological capabilities are being linked to the beginning of a new cyber cold war. The exposure of the People's Liberation Army (PLA) Unit 61398 in Shanghai by the Mandiant cyber security firm highlights the PRC's ability and willingness to conduct cyber exploitation and cyber attack operations globally. The PLA is actively creating the strategic guidance, tools, and trained personnel necessary to employ computer network operations in support of traditional war-fighting disciplines. PLA's assessments of current and future conflicts note that campaigns will be conducted in all domains simultaneously but that its emphasis on the electromagnetic spectrum has driven the PLA to adopt a much more comprehensive approach. The Chinese strategy known as integrated network electronic warfare combines electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield information systems that support an adversary's war-fighting and power-projection capabilities.

Legal issues

There is still no widely accepted international legal framework. The Shanghai Cooperation Organization (SCO) has defined cyber-war to include dissemination of information 'harmful to the spiritual, moral and cultural spheres of other states'. In contrast, the United States' approach focuses on physical and economic damage and injury, putting political concerns under freedom of speech. A Ukrainian professor of international law, Alexander Merezhko, has defined cyber-warfare as the use of Internet and related technological means by one state against the political, economic, technological and information sovereignty and independence of another state. A "Digital Geneva Convention" has also been proposed.

India's National Cyber Security Policy -2013 (NCSP) and Structure

The NCSP recognizes that Cyberspace is a complex environment supported by worldwide distribution of information and communication technology devices and networks. Because of immense benefits, the cyberspace is used by citizens, businesses, critical information infrastructure, education, health services, military and governments, among others. Cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and connected devices. There therefore was a need to create suitable cyber security eco-system in the country. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services. The plan is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents. The Department of Information Technology created the CERT-In in 2004 to thwart cyber attacks in India. In 2011, there were 13,301 cyber attacks, therefore India created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defence, space and other sensitive areas. It operates 24x7. A high-profile cyber attack on 12 July 2012 breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs (MEA), Ministry of Home Affairs (MHA), Defence Research and Development Organization (DRDO) among others. The Cyber threat is overseen by the National security Adviser (NSA). India faces an acute shortfall and needs thousands of experts. Many steps have been initiated that include the isolation of various security agencies to ensure that a synchronized attack could not succeed. On 26 November 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was reportedly as a revenge for the Mumbai terror Attacks. Pakistan Cyber Army retaliated and hacked the website of India's top investigating agency, the Central Bureau of Investigations (CBI).

Defence Cyber Agency (DCA)

Defence Cyber Agency (DCA), a new military entity mandated with the defensive, deterrence and offensive aspects of cyber warfare is being set up and will be operational in next six months. DCA will initially directly employ about 1,000 people drawn from the Indian Air Force (IAF), the Army and the Navy, besides from the Integrated Defence Staff (IDS) and will be a precursor to the setting up of a cyber command in the future. It will engage in defending military assets and resources and also use its offensive capabilities in proxy cyber warfare like those being indulged in by non-state actors and terrorists. The IDS will ensure synergy and inter-linkages among the various constituents of the military. Besides looking into forensics and other verticals, the DCA will audit based on potential risks and threat perceptions. It will have key linkages with the agencies dealing with cyber crime issues. DCA would exploit and utilize the technology available with the country's rich resources base of young software entrepreneurs and technocrats. Cyber warfare domain is already live and any aspiring power has to build capabilities and keep abreast of the developments.

***Air Marshal Anil Chopra PVSM, AVSM, VM, VSM (Retd)** is a Delhi based Defence Analyst

Technology Enabled Multi Domain Warfare : Nano Tech, AI & Robotics

Brig (Dr) Navjot Singh Bedi*

Introduction

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

War is just an extension of politics and winning a war depends on achieving your political ends. More often than not, war is usually the last resort and since time immemorial, tribes and nations have waged wars. In times to come modern technology will enable warfare in many ways which were hitherto unimaginable. Technological growth includes incremental developments and disruptive technologies. The former is a development intended to follow on from the previous technology. For example the transition from flint lock and muzzle fed rifles to bolt action rifles and later on to semi automatic rifles. Disruptive technologies however are those where a new method replaces the previous technology and makes it redundant, for example the replacement of horse mounted cavalry by Armoured Fighting Vehicles (AFVs). Emerging technologies in general denote significant technological developments that broach new territory in some significant way in their field. Examples of currently emerging technologies include information technology, nanotechnology, biotechnology, cognitive science, robotics, and Artificial Intelligence (AI).[1]

The Multi Domain Warfare (MDW) concept is envisioned as a more complex concept that will expand the operational scope and reach of a nation's strategic-military establishment, thereby potentially thwarting the operational parity that near-peer competitors and other lower-end threats are alleged to be acquiring. Though there are many technologies which will drive these changes and which will play a major role in all future conflicts, prominent amongst them being Space, Cyber, Communication, Nano Technology, Artificial Intelligence (AI) & Robotics etc. Space capability is being exploited mainly in the fields of communication, Positioning, Navigation, Timing and Surveillance applications apart from other Space applications and explorations. Therefore, development of Space exploitation capabilities and selective development of counter Space capability will be instrumental in enhancing national security.

Cyberspace today is a complex environment involving underlying ICT infrastructure used by common citizens, businesses, Government including military across the world thus blurring boundaries in time and space. The ever-emerging technologies coupled with activities ranging from e-mails, e-commerce to social media have led to unimaginable expansion of Cyberspace. Cyberspace has acquired strategic position by virtue of its global reach and its rapid integration into the social, political and economic discourse and framework. Malfunctioning or breakdown of a well-knit web may have serious implications on social well-being, economic and business interests of a Nation.

Some analysts such as Martin Ford, author of The Lights in the Tunnel: Automation, Accelerating Technology and the Economy of the Future,[2,3] argue that as information technology advances, robots and other forms of automation will ultimately result in significant unemployment as machines and software begin to match and exceed the capability of workers to perform most routine jobs. As robotics and artificial intelligence develop further, even many skilled jobs may be threatened. This is aptly true in the realm of military and applicable to the laws of war-fighting.

Acronyms of Emerging Technologies

Since most of these emerging technologies are not employed in isolation but in concert with two or three other such emerging technologies, thus a large number of acronyms have come up and few of them are as listed below:-

- NBIC, an acronym for Nanotechnology, Biotechnology, Information technology and Cognitive science, is currently the most popular term for emerging and converging technologies, and was introduced into public discourse through the publication of Converging Technologies for Improving Human Performance, a report sponsored in part by the U.S. National Science Foundation[4]

- GNR (Genetics, Nanotechnology and Robotics)also propounds the same concept. It first found mention in Bill Joy's article in 2000 on Why the future doesn't need us[5].

- "GRIN",for Genetic, Robotic, Information, and Nano processes/ nano-technology,[6] was first used by Journalist Joel Garreau in Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies — and What It Means to Be Human . The book is about the march toward a potentially post human future in which emerging technologies will allow humans to shape their bodies and minds, or possibly destroy life on earth, or even the universe.

- "GRAIN", for Genetics, Robotics, Artificial Intelligenceand Nanotechnology.[7]is used by Science journalist Douglas Mulhall in his book titled Our Molecular Future: How Nanotechnology, Robotics, Genetics and Artificial Intelligence Will Transform Our World uses "

Convergence amongst these technologies is evident and it is a critical elements underwriting the MDW concept. Convergence is defined as the integration of capabilities across domains, environments, and functions in time and physical space to achieve a purpose. MDW requires convergence between inter-organisational and military, as well as lethal and nonlethal capabilities, across multiple domains and environments, in time and space. These create create windows of advantage that enable the Joint Force to manoeuvre or gain a position of advantage. In this article, an attempt has been made to list out certain niche technologies which will empower MDW.

The aspects of Space exploitation, threats and counter Space capabilities and of Cyber have been discussed in various forums and are not being deliberated here. This paper will only discuss the role played by three enabling technological domains ie Nano Tech, Artificial Intelligence (AI) & Robotics, in enabling and empowering MDW. These will be discussed in the subsequent paragraphs.

Nano Technology

Nano Technology is a science dealing with manipulating matter at molecular scale. Nano actually symbolizes a scale which is 10 raised to the power of minus nine ie a millionth sub-part.The nano sized particles exhibit different properties, other than those exhibited by their bulk (matter) counterparts. Instead of gravitational forces and Newtonian laws, which are applicable to normal sized particles, in case of Nano particles the concepts of Quantum mechanics, interplay of Electro Magnetic forces and effects due to random molecular motion become more pronounced and are more relevant. Due to the inherent advantage derived from small size, Nanotechnology finds enormous scope in military applications ranging from Nano Fiber for camouflage & stealth, Body Armour, Nano Robotics, Nano drones, Armed Robots etc. Few of such applications have been explained in subsequent paragraphs.

Nano Fibers for Structures and Body Suits. Due to the small size and inherent strength on account of Quantum mechanics, interplay of Electro Magnetic forces and other factors, the Nano Fibers are especially found suitable for improved weaponry and body suits with enhanced strength. This facilitates preparation of intelligent fabric with Computer and Communication Technology interweaved into the fabric, which is especially useful formaking 'BodyArmour'. This type of body armour is light weight, and can be made more intelligent by incorporation of Health Monitoring system with Tagging and Tracking facility. This is a major technological break through, especially in remote in-accessible areas where advance medical support is not easily available, as this type of body suit permits remote diagnostics and management of health parameters.

Nano Robotics. Due to the inherently small size, the Armed Robots can be made miniaturized, thus providing a smaller cross sectional area to be targeted, which in turn enhances their survivability and reliability. These Nano Robots thus become more accurate, lethal, efficient & reliable on the battlefield. In order to overcome their disadvantage in terms of small size (which is actually an advantage in most spheres of combat), such Nano Robots can be employed in clusters and can be remote controlled. This has the added benefit of preventing loss of valuable human life in battlefields.

Unmanned Air Surveillance. Surveillance using Unmanned Aerial Vehicles (UAVs) is already creating waves and Unmanned Combat Aerial Vehicles (UCAVs) are being put to effective use by a No of developed nations to carry out precision strikes, with virtually no loss of life and nearly 99% assured success / strike rate . So acute is the problem that nations have developed and designed weapons to specifically target UCAVs and UAVs. This is where the magic of Nano Technology comes to their aid due to the inherent advantage derived from small size. Using Nano Technology now Nano Drones having Nano processors can be made. These will be light weight and power efficient devices and will provide their adversaries with a smaller cross sectional area to be targeted, which in turn makes them difficult to be detected and enhances their survivability and reliability. The Nano Drones can form a Smart/Surveillance Dust in which large number of Nano drones can form a decentralized net with computational and wireless communication capabalities. Thus due to the large numbers in the swarm, the disadvantage of limited computational power available ina single Nano Drone can also be overcome by the Smart/ Surveillance Dust, comprising of a swarm of such miniature drones.

Adaptive Camouflage & Stealth Coatings. It's been correctly said that "you can't shoot what you can't see." This is precisely why so much emphasis is given in all armies , to impart training in training in Camouflage & Stealth techniques. Nanotechnology however steps in with technology to assist this niche technique. With ever increasing Battle field transparency making soldiers and weapon platforms invisible/ difficult to detect is of paramount importance. Using nanotechnology, the Electro – Chromatic properties of materials/ protective coatings can be altered dynamically to adapt to surroundings. Cloak Of Invisibility **[8][9]**is made possible due to camouflage/ cloaking microscope tips at optical frequencies. Thus the shooter or target platform is there but is not visible to the adversary, which enhances both it's lethality and survivability manifold.

Nano Sensors. These are extremely small in size with high sensitivity and large surface area. They are capable of on chip sensing, intelligent power savings & wireless communications, all of which makes them extremely useful for military usage. In addition these are low cost & disposable, which lends them suitable for mass production and for deployment in remote, inaccessible areas, where retrieval, repair and recovery is either difficult or not economically/ tactically viable. This attribute thus lends them suitable for various Military Applications, few of which are as listed below:-

- Bio Chemical sensors for detecting NBC activity.
- Integration with Body Suite for Health Monitoring.
- Battle field surveillance.
- Forming Wireless Nano Sensor Networks comprising of large

number of Nano Sensors operating in cohesion to cover large area's.

Nano Biotechnology. Nano Biotechnology incorporates diagnosis and administration of drugs and is especially relevant for wounded soldiers using Nano Sensors. Nano Sensors embedded body suits are generally used in remote inaccessible areas where advance medical support is not easily available, as this type of body suit permits remote diagnostics and management of health parameters. Remote monitoring of Soldiers Health to maintain peak levels during Operations and during war like situations is very important and this is made possible in a big way by Nano Biotechnology , aided by Nano Sensors. This is especially useful in case of troops deployed in remote, inaccessible areas, where on call medical evacuation is either difficult or not feasible/ tactically viable.

Artificial Intelligence (AI)

AI is intelligence demonstrated by machines in contrast to natural intelligence displayed by humans &other animals. It is defined as study of "Intelligent Agents" and can be described to be any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. In AI a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" & "problem solving. Certain prominenttraits /capabilities that researchers expect an intelligent system to displayare:-

- Reasoning, problem solving
- Knowledge representation
- Planning
- Learning
- Natural language processing
- Perception

- Motion and manipulation
- Social intelligence
- General intelligence

Tools of AI. AI has developed a large number of tools to solve the most difficult problems in computer science. Many problems in AI can be solved in theory by intelligently searching through many possible solutions, however AI automates this process through iterative learning. The logical proof can be viewed as searching for a path that leads from premises to conclusions , where each step is the application of an inference rule. Logic is used for knowledge representation and problem solving. The decision tree is perhaps the most widely used machine learning algorithm. Neural networks, or neural nets, were inspired by the architecture of neurons in the human brain and have simply automated an existing time tested physiological function.

Applications of AI. High-profile examples of AI include autonomous vehicles (such as drones and self-driving cars), medical diagnosis, creating art (such as poetry), proving mathematical theorems, playing games (such as Chess or Go), search engines (such as goole search), online assistants (such as Siri), image recognition in photographs, spam filtering, prediction of judicial decisions and targeting online advertisements. With social media sites overtaking TV as a source for news for young people and news organisations increasingly reliant on social media platforms for generating distribution, major publishers now use artificial intelligence (AI) technology to post stories more effectively and generate higher volumes of traffic.

Now all these above mentioned generic applications of AI can be put to effective use in the military. Autonomous vehicles (such as drones and self-driving cars) can be effectively used for surveillance and bomb disposal tasks. AI can facilitate remote medical diagnosis at inaccessible high altitude locations and can help in solving mathematical problems which are a key in cracking cryptographic codes. Wargames, search engines especially programmed for military use, image recognition in photographs, prediction of strategic/ operational/ tactical decisions by the adversary are some other areas where AI can play a major role. AI can also be used to shape the environment by generating content and posting stories more effectively over various social media platforms, in order to generate favourable opinion for the Armed Forces and for the nation.

Shape of Things to Come. An example of AI being rampantly used is IBM Watson. Roles in IT companies that were typically assigned to employees with over 10 years of experience—the mid-level bracket—are now going to machines. For example, Capgemini is using IBM's cognitive consulting tool Watson to assign people to projects, while Infosys is building a machine-learning platform that will help project managers take decisions to make better trade-offs between the number of people needed for a project and the timeline for completion. Such a transition can be expected to take place in the Armed Forces also where the background data / facts and figures would be prepared and presented by AI enabled machines to the commander for his decision. Possibly certain mundane aspects of the execution will also devolve down to such machines.

Robotics

Robotics is an interdisciplinary branch of engineering and science that includes mechanical engineering, electronics engineering, computer science, and others. Robotics deals with the design, construction, operation, and use of robots, as well as computer systems for their control, sensory feedback, and information processing. These technologies are used to develop machines that can substitute for humans and replicate human actions. Robots are ideally suited for military applications and are being used in dangerous environments (including but not limited to bomb detection & deactivation), manufacturing processes and environments where humans cannot survive. Robots are suited for operating in an NBC/ NBC prone environment, where precision measurement / action is required and where it is not advisable for humans cannot to operate. Many of today's robots are inspired by nature, contributing to the field of bio-inspired robotics. Robotic Surgery [10][11] [12] can relive surgeons to perform other life saving tasks/ superviserobotic surgery.

Exo- Skeletons are an extension of robotics with mil applications and applicability of the same was seen in the movie "Avataar. Exoskeleton will drastically reduce the need for Armoured Fighting Vehicles (AFVs) as each soldier will be an intelligent Armoured Fighting platform. Since times immemorial, armies created obstacles to separate the mounted cavalry from the foot infantry (wooded or iron stakes, boggy/ marshy ground etc). Later on the focus shifted on how to separate the tanks/ AFVs from the foot infantry and this gave rise to the Ditch cum Bundh (DCB) canal defence system. The Exoskeletons will help achieve the synergy of infantry and armour, which has been the challenge all armies have grappled with. Powered exoskeleton[13] will make feasible Future Force Warrior (like Iron-man). This will provide a solution for heavy lifting and for paralysis/ muscle related diseases, and possibly a Human Universal Load Carrier. Swarm Robotics[14] will also be possible due to swarm intelligence, autonomous robotics, nanorobotics, particle swarm optimization, multi-agent systems and behaviour based robotics.

Artificial Intelligence (AI) & Robotics

Convergence of both AI & Robotics will result in creation of AI robots. If the utility factor of both AI & Robotics is (say 'x'), then the utility factor of an AI Robot will not be twice 'x'; rather it would be 'x' square. Likewise if Nano-technology was to be combined with AI & Robotics then we would end up with AI Nanobot, with an extremely high utility factor. The military applications and employability of such an empowered weapon platform are endless and are limited only by imagination. Smart manufacturing represents a leap forward from traditional automation to fully connected and flexible systems. The question is: how ready is the industry to embrace the challenges and opportunities of this new era?

Pitfalls of AI and Robotics

How robotics, AI, and IOT are being adopted, how they should be adopted, and how they will transform the world is a moot question that the world leaders are seized of. What would be the impact on history of self-learning machines[15] —machines that acquired knowledge by processes particular to themselves, and applied that knowledge to ends for which there may be no category of human understanding? Would these machines learn to communicate with one another? How would choices be made among emerging options? Was it possible that human history might go the way of the Incas, faced with a Spanish culture incomprehensible and even awe-inspiring to them? Were we at the edge of a new phase of human history?

Conclusion

When considered in its abstract form, the MDW concept is intended to be an all arms and all capabilities affair. The MDW concept appears to be designed to degrade the deterrent potential of an anti-access system, and to render ineffective its kill-chain. The traditional approach followed by armies the world over is to neutralise a defender's anti-access system with overwhelming force. MDW however seeks to selectively target, in a bid to degrade and/ or destroy - key capabilities of anti-access system. All technologies listed above enable this desired end state.

To quote Vice Admiral (Retd) Arthur K. Cebrowski of the U.S. Navy, and John J. Garstka[16], at the turn of a millennium we are driven to a new era in warfare. Society has changed and the underlying economics and technologies have changed. Business models the world over have changed, hence it should not be surprising if the military did not. Due to increased connectivity, inter dependence, blurred boundaries, Cyber Space has become a Global Common and thus its governance has been a subject of debate for some time. Today there are 4 Bn Internet users, 3.8 Bn active mobile internet users and 8 Bn IOT Devices in the world. In India, with 330 Mn Internet users, 1 Bn Mobile Devices (30% Smart

Phones) & 1 Bn IOT Devices, our national stakes are huge in Global Cyber Space.

There are no binding laws on cyber space governance and even international organizations like UNGGE has so far failed to establish any cyber norms which are binding for all. Further, the way data is generated, consumed, analysed and labeled, it is the "New Oil" and has potential to generate conflicts. Digital society is truly global giving immense opportunities to common citizens, governments, businesses, etc. Chief of US Naval Operations Admiral Jay Johnson has called it "a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare,"[17] and it will prove to be the most important RMA in the past 200 years.

However, such connectivity/society brings with it innumerable vulnerabilities. Cyber attacks and disruptions cross over national borders, cultural and legal system in a flash/fraction of second. It is often unclear which jurisdiction applies and it is uncertain whether applicable laws can be effectively enforced. MDW is the next important development in waging war. Data is a commodity being effectively used by business houses and other entities to leverage their vested interests. Individual Privacy and National Security has become a debatable/live world-wide issue. The importance of making the correct strategic choices to adapt or even survive in such changing ecosystems[18] is thus important.

***Brig (Dr) Navjot Singh Bedi,** is a Senior Fellow, CENJOWS, New Delhi

References / Bibliography

1. Other examples of developments described as “Emerging Technologies” can be found at- O’Reilly Emerging Technology Conference 2008.

2. Joy, Bill (2000). Why the future doesn’t need us.Retrieved 2005-11-14.

3. “Machine Learning: A Job Killer?”

4. “Will Automation Lead to Economic Collapse?”

5. Roco, Mihail C. and Bainbridge, William Sims, eds. (2004). Converging Technologies for Improving Human Performance. Springer.ISBN 1-4020-1254-3.

6. Garreau, Joel (2005). Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies — and What It Means to Be Human. Doubleday. ISBN 0-385-50965-0.

7. Mulhall, Douglas (2002). Our Molecular Future: How Nano technology, Robotics, Genetics and Artificial Intelligence Will Transform Our World. Prometheus Books.ISBN 1-57392-992-1.

8. Rachel Kaufman (28 January 2011). “New Invisibility Cloak Closer to Working “Magic””. National Geographic News.Retrieved 4 February 2011.

9. “Breakthrough in bid to create ‘invisibility cloak’ as 3D object is made to vanish for first time”. Daily Mail. 26 January 2012. Retrieved 3 March 2012.

10. “Doctors grapple with the value of robotic surgery”. Houston Chronicle. 16 September 2011. Retrieved 24 December 2011.

11. “Robotic surgery making inroads in many medical procedures”. The Jakarta Post. 8 March 2011. Retrieved 24 December 2011.

12. “Doctors Perform First Fully Robotic Surgery”. PC World. 21 October 2010. Retrieved 24 December 2011.

13. Christopher Mims (2009). “Exoskeletons Give New Life to Legs”. Scientific American.Retrieved 21 April 2009.

14. “Riders on a swarm”. The Economist. 12 August 2010. Retrieved 21 April 2011.

15. “How the Enlightenment Ends”; Henry Kissinger’s Views on AI; The Atlantic Journal; June 2018 Issue; Technology Section.

16. Network-Centric Warfare:Its Origin and Future by Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka, Proceedings, January 1998.

17. Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD, 23 April 1997.

18. James F. Moore, “The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems,” Harper Business, 1996.

SPACE A MAJOR FACILITATOR OF MULTI-DOMAIN WARFARE

Gp Capt GD Sharma, VSM (Retd)*

Changing Concepts of the war

The modern day's threats during war would be initiated simultaneously across several domains by the adversary. Winning this war requires recognition of adversary's actions in various domains and countering these with innovation, flexibility and with an integrated approach on all war fighting domains. The advent of new technologies have further added complexity to the war which now have spread from kinetic to non-kinetic zone.

It would also be a fallacy to believe that superiority in one domain i.e. air, land, maritime, space and cyberspace alone could win a war. In fact, it is a considered belief that no single service can win the war and even mere Jointness between services in conventional sense is inadequate to meet the challenge. Instead, a Multi-Domain warfare (MDW) concept could be considered which melds the services to fight as a single coherent war fighting unit. Therefore, the idea is to move beyond the jointness between services to a MDW concept.[1] This war fighting concept however, does not reduce the relevance of space whether to an individual service or when it melds with other domains as one war fighting unit. In fact, space enables building closer relationship between

[1] why it's time to eliminate the independent services: Michael c. Davies | may 11, 2017

services with better communication and cross exchange on data which are vital for command and control of the battle by the commander.

Critics of the concept however claim that MDW is merely a buzzword; the operations in multi domain always existed. It is another form of Joint operations.

Role of Space Assets

There is an increasing dependence of military on outer space assets in all versions of wars/conflicts (nuclear, conventional, and sub-conventional). In the four decades of the space age, the space has been used traditionally in five missions viz; for reconnaissance and surveillance, communications, navigation, meteorology, and geodesy. Space has the ability to provide these at the same time across several domains. In the process, it integrates operations and their command and control by communicating across various domains.

The reliance on space is born out of successful experience of using space assets by U.S. in 1991 Gulf war and thereafter, it obtained similar successes in all subsequent conflicts. It has firmed up a belief in militaries world over that future military skirmishes cannot be fought without credible support from the space assets. In support role the space acts as a facilitator as well as a force multiplier for the fighting forces. Now, space has emerged as an independent domain in MDW scenario for all the militaries. United States, Russia and China are major military space powers with considerable offensive and defensive space exploitation ability. Some developed nations of the European Union (England and France) too have considerable military space capability which is articulated in their space doctrines. Today, such support is so ingrained in daily operations in military that most soldiers, sailors, airmen, and marines assume it has been, and always will be, available for their use. With reliance on space comes a vulnerability that potential adversaries may try to exploit but, this does not lower the need for the military space capability. India has emerged as a major space power but our focus continues to remain predominantly towards civil use of the space.

Traditional Military use of the Space

Space laws based on treaties and principles as adopted by the United Nations in its resolution in 1963 ordains use of space for peaceful purposes only and prohibit placing nuclear weapons or other weapons of mass destruction in the outer space or on the celestial bodies. Nevertheless militarization of the space has taken place in the military supportive roles.[2]In six decades of Space Age after launch of Sputnik I, space has been used by the military for five so called traditional missions of reconnaissance and surveillance, communications, navigation, meteorology, and geodesy. [3] These inputs are needed to a good measure in land, air and maritime domains.

The capabilities derived from the space assets relate to ISR (for strike- target identification and location), Metrology and Oceanography (for continuous tactical weather predictions for streaming direction for carrier aircraft launches), communication (for command and control and for passing tasking orders, mission plans, target co-ordinates), Intelligence coordination, to launch precision attacks and for position, navigation with GPS.

The space has substantially enhanced the war fighting ability of the forces, provided the alert / warning of the adversary's war fighting ability and finally, endowed the capability to deter the adversary.

Space Assets that Enhance War Fighting Ability

- Signal Intelligence: To gauge enemy intentions and his tactical moves in real time.
- Imagery: Helps in identifying targets.

[2] http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspace-treaty.html

[3] Current and Future Military Uses of Space by ASHTON B. CARTER

- Navigation and targeting: For accurate maneuvering and weapon launch on enemy's positions and strategic/ tactical assets.
- Meteorology: Weather plays an important part in all military operations.
- C4ISR: Space is a C4ISR enabler for the Armed Forces in communication networking and command and control.
- Search and Rescue. Facilitates in providing relief to the needy during national disasters.

Space Assets that Alert/ Warn of the Adversary's War Fighting Strategy.

- Early Warning: Detect missiles launches with the help of infrared satellite sensors which pick up missile IR trails.
- Telemetry Tracking and Data Relay Satellite (TDRSS Capability).

Space Assets Those Endow Capability to Deter the Adversary

- Space Surveillance Awareness (SSA). To remain updated about where about of space assets (own and adversary's satellites)
- Satellite assisted Ballistic Missile Defence.
- Offensive Space.

A leading military power , military has its own satellite launch and control capabilities which consists of many diverse systems which include ground-based infrastructure, satellites and space launch vehicles, and the electromagnetic links that connect them.

Space Support to the Army. Army has been assisted with space based operations for well over half a century. For terrestrial war fighting by the army, a reliable and resilient space support has become a vital need in the twenty-first century. Space supports the Army in six war fighting functions of mission command, movement and maneuver, intelligence, fires, sustainment, and protection. Integrating space capabilities enables the commanders, down to the lowest echelon, to conduct unified land operations through decisive action and operational adaptability.

Space Support to the Navy. Satellite support has enabled the Naval Forces to acquire the blue water capability. These assist the Navy in Under Surface Warfare, Surface Warfare and in Naval Aviation. Space ensures that each naval domain is better informed. It particularly helps in the realm of the cyber security and good defence with defence in depth strategy. Naval forces will engage adversaries in four critical areas namely, Sea strike, Naval fire power support, Ship to objective manoeuvre and Strategic deterrence.

At the heart of the sea strike is the naval power projection that leverages C5ISR (command, control, communication, combat systems, Intelligence, surveillance and reconnaissance.) precision, stealth information and joint strike with other domains.

Space support to the Air Force. Much like other domains Air forces needs space support to achieve C4ISR capability which is a necessary ingredient for successful war fighting and other support in terms of target identification, position, navigation and precision targeting functions , to achieve all weather capability with space weather predictions. Space enables environment assessment for Ballistic Missile Defence (BMD) by detecting adversary's, missile launches and finally in bomb damage assessments.

Relevance of Space Assets in Multi Domain Warfare

What distinguishes the multi domain from the normal operation warfare model is that each service is not fighting its independent battle but its operations are coordinated as well as integrated with the operations in other domain. Multi-domain theory improves on the joint model by fully integrating domains, developing problem-based solutions, and creating options. In today's increasingly complex environment, it's not enough to know what's happening in one domain. In fact, the commander needs to know what's going on in multiple domains. For this to happen, war fighters must have the information across multiple systems to decide fast enough. Sharing of relevant satellite data on the adversary across the domains helps in achieving this. The commanders with surveillance data from satellites and from different platforms' sensors can construct a single holistic picture of the battlefield. This allows them to detect and counter adversaries with Precision Fire systems before these become threats. Thus the key word is integration of data from various platforms including the space for fast decision taking. Sam Tangredi, a US defence strategist opines that the problem behind the current joint ideology is "that it drives planning to the lowest common denominator of strategy." Although joint interoperability has continuously improved since the signing of the Goldwater-Nichols Act of 1986, the mind-set of equal contributions of all services must change. Tangredi accordingly suggested about the importance of tailoring force composition to each scenario. The space support however, will deliver capacity to the fighting echelons fighting in MDW scenario as it does in a individual service scenario or joint warfare. Space capabilities are so integrated that they function in a multi-domain battle unseen and unappreciated by many until something interrupts the advantages they provide. The future wars could likely involve extensive cyber campaigns and will likely extend into, or even start, in space.[4] Modern warfare has shown that GPS helps ships, aircraft, and troops to their objectives, and launch smart munitions, enabling them to hit targets requiring high levels of precision. Data from signals intelligence and imagery satellites fill critical intelligence gaps in denied areas that other air, sea, and land assets cannot observe without significant risk of interdiction or destruction. Satellite communications, can support tactical battles across the domains , at the same time provide links for

armed unmanned aerial systems, provide in-flight guidance to the cruise missiles to their targets , and help rescue operations all at the

[4] https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-3/V-Harris.pdf

same time.[5] Hence, space inherently has the ability to support the multi-domain battle.

India's increasing responsibilities as a net security provider of the security in the Indo-pacific region will require the creation of the tri-service capabilities for the military intervention singly or in conjunction with the strategic partners. Space alone can provide the surveillance in the vast expanse of the Indian Ocean region and beyond. It will also need to co-ordinate with armies like that of United States which is space enabled in all realm of war fighting. These capabilities are based on networking centric operations, the state of the art command and control system, air space based reconnaissance, surveillance, target acquisition and failsafe precision guided strike ammunition.[6] Though India has emerged as a space power it is still primarily achieved successes in civil use of satellites and in space exploration. India however, has been slow in seeking greater role for space in military operations. Military has been sourcing limited space data from ISRO's dual role satellites. Now forming of independent Space agency is on anvil and India has also launched dedicated naval and air force satellites in 2013 and 2018 respectively. Similar dedicated army satellite is also planned by ISRO.

Challenges to the Multi-domain Warfare

Space enabled capabilities while increase the capacities of the fighting forces many times, these can turn to be Achilles heel as well. Total dependence on space has its downsides. Adversary being aware of this fact would attempt to disable the satellites or at least interfere in their operations. Wide arrays of threats are faced by the space assets ranging from Kinetic (direct ascent anti-satellite weapons) to non-kinetic (jamming, cyber-attacks, Laser attacks etc). A satellite system consists of three basic components, the satellite, the ground station and the communication links. All these have varying degree of vulnerabilities.

[5] https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-3/V-Harris.pdf

[6] Excerpts from an article by Brig GurmeetKanmal

The Satellites are virtually exposed as this move along the predictable path and are visible from the large swath of earth. The adversary has variety of attack options including kinetically striking the satellite and the ground station and non-kinetically by jamming or spoofing the links using the directed energy to dazzle or partially blind the satellite. Future also hypothetically indicates use of the parasitic satellites that could latch on to the satellite and disable it, alter its orbit or hijack the information gathered by it. While there is need to develop resilience in space satellites, It is desired to develop Kinetic/ non-kinetic deterrence ability which may like nuclear deterrence and deter an adversary who may fear similar attack on his own satellites in response.

However, limitation in space capabilities by enemy action or otherwise will have cascading effects in other domains. To understand its implication, consider the fact that electromagnetic spectrum which empowers the space domain, is if attacked by the opponent or who manipulates the radio frequencies within the electromagnetic spectrum (EMS) through cyber or other means, could deny access to our vital satellites as space based capabilities are dependent EMS for operations. It is the sole medium for transmitting or receiving signals from the space. Additionally, these frequency bands are fixed and cannot be changed after launch of the satellite. EMS is crucial for communication, command and control, tracking precision attacks and host of joint functions. Cyber intrusion by the adversary could cripple the in theatre satellite which could put the deployed forces at risk. It could jam the signals coming from the GPS limiting its support to the aerial/ground platforms and their conduct of strikes/operations. Similarly, lack of actionable intelligence on enemy movements/manoeuvres and downgraded command and control and attack capabilities in the theatre can have serious implications on own forces. All this can happen by a cyber-attack on the satellite. Thus information has become prominent part of the war to an extent that whole war may resolve around seizing or manipulating the enemy data sphere. This has led to strategists prophesy that, next Great War will likely involve intensive cyber campaign and will likely extend in to or start in space. In view of these enabling capabilities, the adversaries are likely to invest in cyberspace or counter space weapons to seize the initiative. Our adversary, China is reportedly expanding its intelligence, surveillance and reconnaissance capabilities while concurrently developing systems those supposedly are targeted against America its main adversary, would affect us as well. Strategists from United States assert that Russia is possessing similar capabilities.

As long as space remains a key enabler for combat effects across multiple domains our adversaries will continue to look for ways to counter our space capabilities. Space operators have always leveraged cyber effects to derive military success through space. In fact, satellites are useless without the cyberspace links that allow the flow of data to or from them or the processors that transform the data to the meaningful information. Attack on cyberspace can easily exploit the vulnerability of the space activities and could cause cascading events that limit the adequacy of space effects.

Circumventing the Limitations

General David L. Goldfien USAF chief of Air Staff speaking at the Air Warfare symposium in Feb 2018, asserted that a smarter adversary requires an improved war fighting approach such as multi-domain approach. It would also provide a greater level of synergy and solutions to the emerging challenges of anti-access and anti-denial strategy as practiced by Russia and China.

To overcome the limitations, the leaders at the tactical level should consider employing the following steps in shaping their environment for the multi-domain command and control[7]Space which was seen as a force multiplier in support role along with cyber, is now emerging as independent war fighting domain. Its importance and synergy with cross domains must be understood. Limitations in achieving synergy in domains including the space can be overcome by the followings:-

[7] Preparing for multi-domain warfare –Lessons from space /cyber operations .www.airuniversity.af.edu

- **Know your Domain Well.** We must recognize how our domain fits in to the bigger fight. At the tactical level, we must understand how our actions enable the operational objectives and the leaders must effectively communicate this understanding to those they lead.

- **Identify and Collaborate with the Tactical Mission Partners.** Identify units of opposite domains and then collaborate to ascertain possible cross domain synergies that may contribute towards multi-domain mission success.

- **Train and Exercise Multi-domain Approach**. The tactical leaders should conduct joint training and exercises to strengthen multi- domain approach.

- **Document lesson Learnt**. Documenting the lessons learnt after observation, analysis of training and exercises are vital.

- **Apply Multi-domain lessons in Agreements, Plans and Tactics**. Multi-domain lessons as applicable to all domains including space and cyber should be codified in plans and tactics to achieve the mission.

Space as a Distinct Domain

Of late, there is a push to make outer space an exclusive and distinct military warfare domain. Realising the covert application of the space in all civil and military activities, President XI Jinping on coming to his office in 2012 has made becoming a “Space Super power” a priority for his government which has goal of sending a permanent manned space station in to orbit by around 2022, around the time India has planned a manned space flight.

Echoing President Jumping’s, sentiments, United States President Trump too has directed Pentagon to submit a proposal for setting up a Space force, an independent and distinct force separate force in the outer space domain.While architecture and functions of the planned U.S. space force are not clear but, it has set a clear prognosis for the future. Space will no longer remain a benign domain as before but, with will move towards more offensive roles in future regardless of the space laws which presently forbid it. Cautioning U.S. of any laxity in the space a committee headed by then Defense Secretary-designate Donald Rumsfeld had issued a proverbial warming as early as in 2001 which said that "If the US is to avoid a 'space Pearl Harbor,' it needs to take seriously the possibility of an attack on US space systems," Recently, similar opinion has been expressed by a Chinese general who declared Chinese resolve to take the war to the space more so as US its adversary is more dependent on space than any other nation.

Conclusion

The first gulf war threw open many possibilities on use of the satellites in military support role. Traditionally, the militarization space support role has taken place in six areas namely, reconnaissance and surveillance, communications, navigation, meteorology, and geodesy. These enhance capabilities in seven functional areas of the defence forces viz; Intelligence, Surveillance and Reconnaissance (ISR), ballistic missile detection, missile tracking and ballistic missile defence, environmental(metrological) monitoring, communication , positioning , navigation and tracking. Jointness between services has always been a buzzword, now concept of Multi-domain Warfare has emerged. What distinguishes the joint warfare from multi domain warfare is that the nature of joint is working together whereas, the nature of multi-domain is interoperability, working across streams with knowledge of others' capabilities. It envisions a greater degree of integrated actions across domains also integrating space and cyberspace operations. Modern day's wars call for application of the force simultaneously across several domains to outmanoeuvre the adversary. This will create multiple dilemmas for an adversary.

Critics often point out that Space domain cannot be exploited fully by the armed forces due to the legal hurdles thrown in by the outer space treaty which prohibits the military use of the space. This is not entirely true; the outer space treaty bans only location and testing of the nuclear weapons and the weapons of mass destruction but not the weaponry. This lacuna in the treaty has led to the development terrestrial conventional weapons such as anti ballistic missiles and anti-satellite weapons. The leadership of both China and U.S. have already expressed their intention to use the space as an independent domain. This means battle field will not remain restricted in the earth orbit but, may with time extend out to asteroids with claims and counterclaims to source these. Some estimate that market value of the exploitable mineral wealth in the space is much beyond our imagination. Hence, the boundaries of conflict are bound to expand to the space.

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

MULTI DOMAIN WARFARE –
LD WINE IN A NEW BOTTLE

Rear Adm Monty Khanna, AVSM, NM*

Every now and then we are confronted with a new term in military jargon which is marketed as a harbinger for a new concept in war-fighting that has the potential to radically change the manner in which force is applied for meeting political aims. Amongst the latest in the series is ‘Multi Domain Warfare’ or MDW. Pundits tell us that MDW is a new concept that will take war-fighting to a whole new level. Unlike ‘Joint Warfare’ which deals with the integration and cohesive functioning of the armed forces, MDW goes several notches higher. It basically involves synergizing all means available to government, be they diplomatic, economic, ideational and informational towards the fulfilment of military aims. Well..... What’s new? From my understanding on this subject, every commander worth his salt from Zhengis Khan to Collin Powell has attempted to do so and met with varying degrees of success. If he has not attempted the synergistic application of force using all levers placed at his disposal, either he has been incredibly powerful or incredibly stupid.

There are several stages to a contest of wills between two nations or two alliances. At each stage, while application of multiple levers of power will be in vogue, there will invariably be a dominant lever to which the others would need to align themselves. More often than not, in all less than war situations, the dominant lever would be ‘Diplomatic’. Once kinetic action gets initiated, a transition is made to ‘Military’. Going by the DIME construct, ‘Economic’ and ‘Informational’ levers would largely be supportive under all situations. This is quite akin to a key tenet of

Joint Warfare wherein we identify a 'Supported Commander' who is ably assisted by 'Supporting Commanders'.

During conflict, commanders are essentially charged with the responsibility of meeting military aims that flow from political goals, at a minimal cost in terms of lives and resources. Efficiency is therefore hardwired into the planning process, more so as lives are at stake in addition to expensive pieces of military hardware. Efficient application of force is resident on two key parameters. The first is the ability to synergise the application of force with all other levers of power that are available to a nation in a coherent manner. This requires an 'all of government' approach coupled with sound intelligence and a deep understanding on the complexities of the action-reaction cycle with respect to an adversary. The second parameter which lies more within the military domain is the ability to wisely orchestrate all the vectors available (terrestrial, airborne, maritime, space and cyber) so as to produce the maximum possible effects with the minimum expense of resources. This in essence is what we commonly refer to as 'joint warfare'. Efficient integration of both these two levels of decision making is what we would term as Multi Domain Warfare.

Decision making, as we know, is a process bound time consuming activity. While John Boyd may have articulated the OODA (Observe, Orient, Decide, Act) loop from a fighter pilot's perspective,[1] its applicability lies across all levels of decision making. Hence akin to Joint Warfare, national level decision making has its own OODA loop with an associated time line. As Joint Warfare has to be enmeshed with higher decision making for optimization of MDW, the challenge lies in ensuring that these decision loops, in their broader context remain synchronized at most times.

To some degree nations have always endeavoured to do so. While there have always been challenges hitherto, the complexities involved in doing so have increased with time. What has really changed in today's context? While the principle of synergy and coherence at all levels of decision making has remained unchanged, the enablers for compression of the OODA loop have found varying degrees of resonance at different levels of decision making. What are these enablers? The major ones are as listed below: -

- **Battlefield Transparency.** With a host of assets available today ranging from satellite based surveillance to drones of various shapes and sizes, coupled with identification means such as Blue Force Tracker (BFT), the battlefield in all spatial domains (land, sea and air) has become much more transparent. As a consequence, the utility of surprise has diminished unless it is coupled with adequate resources to operate within the OODA loop of the adversary. In such an instance, even if the adversary is forewarned of an imminent strike, he may lack the ability to respond adequately within the time available.

- **Networking and Communications.** The utility of early detection is predicated upon having the means to communicate. With the exponential rise in the generation and transmission of data, information dominance has become a prerequisite for achieving desired outcomes. Providing the means to rapidly shift enormous amounts of data securely and accurately to desired addressees is what modern day networks are designed to do. Redundancies are built in by using space along with radio and terrestrial circuits, so as to minimise disruptions.

- **Decision Support.** Given the quantum of data generated, a human brain is incapable of sifting through it in its entirety and extracting information that would be of relevance. This gap is being increasingly filled in by resorting to computational power that converts and presents the data in a form that is far easier for humans to digest thereby assisting the decision making process. With increasing usage of Artificial Intelligence, even the lower levels of decision making are being hived off to machines thereby greatly increasing the tempo of operations.

- **Precision, Reach and Lethality.** Modern day weapons are extremely accurate and selective. Driving a missile through a window in a building no longer raises eyebrows. Laser designation, precise satellite navigation, digital scene correlation, etc. have allowed the delivery of ordinance with pinpoint accuracy. Further, powered by efficient engines with energy rich fuels, ordinance can be released from extended ranges thereby decreasing the risk that the shooter is subjecting itself to. This has increased the lethality and destructiveness of warfare in general.

It may be seen that the above mentioned capabilities, largely driven by technology have had far reaching consequences on the manner in which today's wars can be conducted. It has brought about much greater transparency in the battle space by enabling data collected by a variety of assets operating in different domains, to be seamlessly fused into one composite shared picture. Powerful combat systems thereafter digest this picture and provide robust decision support with regard to employment of weapons which can be fired at extensive ranges at pin point accuracy. Networks also enable commanders to be constantly updated on shifting priorities and emergent requirements. If effectively used, they serve as a powerful tool to convert the Commander's intent into reality.

However, for optimising this process, there remains the essential requirement of enabling structures that are agile enough to leverage the compression of timelines that the use of technology allows. This brings us to the realm of joint structures and integration of the armed forces. Enough has been written on this subject. The requirement of a master puppeteer (read 'theatre commander') to seamlessly phase and sequence operations in all domains including space and cyber, over a wide front cannot be overstated. Only then would a military have a reasonable chance of operating inside the decision loop of an adversary thereby seizing the initiative and forcing him into a reactive posture. Most modern day militaries have made this transition to varying degrees. Those that have not place themselves at risk, should they be confronted by a competent adversary.

However, this is only one face of the problem. Effective pursuance of MDW requires the decision loops of all other government security related resource providers to keep pace with the militaries decision cycle. As technology has had a disproportionate impact in providing a military the means to compress the timeline in this respect, we now have a growing problem of asynchronization which is detrimental for simultaneity. How do we mitigate this issue and reduce the probability of dissonance in decision making at the national level?

As more often than not, the preeminent answer lies in structure. The biggest impediment to synchronization of the diplomatic, informational and economic lines of operations with that of the military during conflict are inadequate or archaic structures. It is imperative that structures adapt and reinvent themselves to remain relevant and capable of meeting the changing timelines of conflict. As technology compresses the military decision cycle, structures at the national level need to evolve, become agile and be capable of adjusting their rhythm to keep up with military dynamics.

In our context, it would involve the strengthening of the National Security Council and ensuring empowered and informed representation from all levers of government machinery that could be leveraged to gain advantage during any contest. Amongst the constituents, there would need to be a clear understanding on which is the lead agency tasked with confronting the issue at hand at a given time, as also on the transition of this responsibility with evolving circumstances. Supporting agencies would need to be fully conversant of the fact that their task is to indeed support the lead agency to the greatest extent feasible. The interface with the political establishment for seeking approvals where necessary as well as guidance on the further pursuance of operations should be well established and time sensitive in keeping with the existing tempo of events.

There would invariably be several instances where it is not feasible for an apex organization of this nature to keep up with rapidly evolving events on the ground. It is therefore imperative to resort to a high degree of delegation amongst the constituent agencies. Agency heads would also need to be advised and encouraged to sub-delegate their responsibilities amongst their subordinates. To prevent divergence as one goes down the hierarchy, which is inevitable if one were to follow a siloed approach, clear cross-connects through embedding of personnel or designation of liaison officers/points-of-contact at every level would have to be resorted to. This would allow lower echelons of diverse agencies to self synchronize without being confronted with the necessity of going up and down the chain over every request made for a resource. This is of paramount importance for MDW to achieve its objectives. Adequate levels of connectivity backed by underlying organizational confidence needs to be created and nurtured wherein junior commanders in the battlefield have the ability to call for resources which may be resident with a different service/department of government. General Stanley Mc Crystal in his book 'Team of Teams' speaks extensively of such an approach to decision making wherein as the Commander of coalition forces in Afghanistan, he reversed the traditional paradigm of '*decentralized operations with coordinated control*' to '*coordinated operations with decentralized control*' and in the process achieved astounding results.[2]

The United States military establishment with its penchant for acronyms has articulated a similar concept in warfighting as JAM-GC or the Joint Concept of Access in Manoeuvre in the Global Commons.[3] However, as per published literature, it primarily deals with command chains and decision making within the military domain. Hitherto, while a Joint Task Force (JTF) Commander would be appointed for a contingency (usually from the lead or 'supported' service) and be given assets from all domains (land, sea, air and possibly cyber and space from 'supporting' services), the coordination would largely happen only at the headquarter level. Each vertical essentially operated in a silo with the orchestration amongst them being done by the JTF commander and his staff. Under JAM-GC, the emphasis is on self synchronization. Lower commanders are empowered to requisition resources from ‘supporting’ services in different domains to assist them in mission accomplishment. This has the potential to substantially compress the decision cycle and force the adversary into a reactive posture. JAM-GC is hence a form of ‘joint warfare plus’ or ‘super-jointmanship’ so to speak.

MDW expands the self synchronization to agencies beyond the military into other levers of government; be it media, finance, telecommunications, shipping, railways, aviation, power, etc. It demands a high level of civil military integration. An apt example would be the concept of ‘People’s War’ propounded and practiced by Mao which relied on using all available national resources for attainment of military goals. Integration and synchronization of civil and military agencies was attained by embedding political officers in all headquarters thereby creating a dual command structure peculiar to most communist nations. Adopting such a structure even in lower formations such as battalions, ships and squadrons allowed for an unprecedented level of self synchronization between civil and military agencies. Undoubtedly, a dual command system of this nature comes with its own pitfalls. An MDW enabling structure in our context of unitary command would need to take heed of such shortcomings and evolve in a manner best suited to us.

In conclusion, it can be seen that MDW as a concept has existed since time immemorial. In yesteryears, it was arguably easier to practice MDW as more often than not, the military commander was also the political leader with all national resources at his beck and call. Today’s political structures are far more complex. The application of technology in the military domain has promise of compressing the decision making cycle to such a level where other levers of government would find it difficult to keep pace unless they adapt. Synchronization of decision loops is essential to achieve simultaneity – a critical tenet of winning tomorrows wars. To ensure optimization in the consumption of national resources for meeting war aims, we would need to do the following: -

- Embrace modern concepts of joint warfare, a key component of which is integrated or theatre commands. Spatial (geographic) and functional (inter-service) seams would need to be blurred to ensure optimum sequencing and phasing of military vectors.

- Strengthen the National Security Council and empower it (within defined boundaries) to call on resources resident in different government agencies. The ‘all of government approach’ is essential to create the necessary asymmetry to enable victory in conflict.

- Speeden up national decision making to a point where it can keep pace with the military decision cycle. Synchronization of these two loops will create greater opportunities of using simultaneity for creating war winning asymmetries.

- Decentralize decision making by empowering subordinates. Create inter-agency cross connects at multiple echelons so as to enable self synchronization instead of adopting a top down approach. Permit (within defined limits) cross domain requisition of resources without the necessity of going up and down siloed chains of command. This is key to the successful pursuit of Multi Domain Warfare.

***Rear Adm Monty Khanna, AVSM, NM** is a CI, Navy at DSSC Wellington

Endnotes

[1] Taylor Pearson, “The Ultimate Guide to the OODA Loop”, https://taylorpearson.me/ooda-loop/, (accessed on Jun 01, 2018).

[2] General Stanley McCrystal (U.S. Army, Retd) with Tantum Collins, David Silverman and Chris Fussel, “Team of Teams – New Rules of Engagement for a Complex World”, Penguin Random House LLC, 2015, Pg 198.

[3] Michael E. Hutchens, William D. Dries, Jason C. Perdew, Vincent D. Bryant, and Kerry E. Moores, “Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept”, Joint Force Quarterly 84, https://ndupress.ndu.edu/Media/News/Article/1038867/joint-concept-for-access-and-maneuver-in-the-global-commons-a-new-joint-operati/, (accessed on Nov 11, 2018).

CENJOWS PUBLICATIONS FROM NOV 2017 ONWORDS

S No	Nomenclature		Remarks
Synergy Journal- 2017			
Synergy-Feb 2017 – Theme: CDS(Chief of Defence Staff) and Need for Integrated Theatre Commands			Feb 2017
Synergy-Jul 2017 – Theme: Impact of Future Technologies on Warfare.			Aug 2017
Synergy Journal- 2018			
Synergy-Feb 2018-Theme: Future Security Challenges of India.			Feb 2018
Synergy-Aug 2018-Theme:Essential Elements of National Security Strategy of India			Sep 2018
Synodos Paper- 2017			
1.	Brig Ranjit Singh	Review of Policy Issues and Organisational Structures: Imperative for Enhancing Defence Cooperation	May 2017
2.	Lt Gen Gautham Moorthy, PVSM, AVSM, VSM (Retd)	Should Unorthodox Measures in Counter Terrorist Environment be Allowed to Trump Rules of Engagement?	May 2017
3.	Brig Ranjit Singh	India: A Global Military Training Hub	Jun 2017
4.	Brig Rajiv Kumar Bhutani (Retd)	Aslant Hat: Hitting Below the Belt	Jun 2017
5.	Maj Gen Harsha Kakar (Retd)	US's Latest South Asia Policy May Not Succeed	Sep 2017
6.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Looking Beyond Doklam: Is the Army Future Ready?	Sep 2017
7.	Col C Madhwal	China's Military Reforms & Implications for India	Aug 2017
8.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Exploiting Special Operation Forces-Beyond the Surgical Strikes	Oct 2017
9.	Maj Gen Bipin Bakshi, VSM	Social Media & the Indian Armed Forces	Oct 2017
10.	Col Laxman Singh	Revisiting India's Afghanistan Policy	Nov 2017
11.	Capt (IN) Ranjit Seth	Sagarmala-A Game Changer	Oct 2017
12.	Lt Col Nikhil Kapoor	India-Japan: Forging Strategic Partnership	Dec 2017
13.	Pinaki Bhattacharya	Chinese Armed Forces: Down five Decades	Dec 2017
14.	Air Cmde T Chand	Quantum Computing and Likely Defence Application	Dec 2017
15.	Maj Gen Harsha Kakar (Retd)	Can India Learn from the US National Security Strategy	Dec 2017

2018			
16.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Revisiting Maldives_ India's Military Intervention	Feb 2018
17.	Lt Gen Rameshwar Yadav, PVSM, AVSM, VSM (Retd)	CPEC: Fundamental Negative Paradigms	Feb 2018
18.	Lt Gen (Dr) NB Singh, PVSM, AVSM, VSM (Retd)	Mission Engineering the FICV	Mar 2018
19.	Shri R Chandrashekhar	India-Asean Relations: Way Forward	Mar 2018
20.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Post Wuhan – Imperative to ensure peace & Tranquility along the Line of Actual Control (LAC)	May 2018
21.	Col Harpreet Singh	Minimising Casualties in Counter Insurgency/Counter Terrorism Operations	May 2018
22.	Air Cmde T Chand (Retd)	Artificial Intelligence (AI) and its Applications for Defence & Security Forces	Jun 2018
23.	Rear Admiral Monty Khanna, AVSM, NM	A Case for Eliminating Permanent Commission at the Entry Level	Jun 2018
24.	Col Shyamji Yadav	Asean Discord in South China Sea	Jul 2018
25.	Rear Adm Monty Khanna, AVSM, NM	The Indian Air Force & Theaterisation-Misplaced Apprehensions	Jul 2018
26.	Col Arvinder Singh	Security Challenges in the Indian Ocean Region	Jul 2018
27.	Col Sumit Rana	Defence Production Policy 2018: Opportunities & Challenges	Jul 2018
28.	Brig HS Cheema	India-Bangladesh Relations A Way Ahead	Jul 2018
29.	Rear Adm Monty Khanna, AVSM, NM	Merger of Public Sector Shipyards-A Crying Necessity	Jul 2018
30.	Col Harpreet Singh	Blockchain: Military Applications	Jul 2018
31.	Rear Adm Monty Khanna, AVSM, NM	How Does China Build its Warships at a Fraction of our Cost?	Aug 2018
32.	Lt Gen K Surendra Nath, PVSM, AVSM, VSM (Retd)	Re-Attire, Re-Skill; Re-Serve; Enabling a Second Career to Veterans	Sep 2018
33.	Lt Gen Rajesh Pant, PVSM, AVSM, VSM (Retd)	Cybertronic Warfare-Beware the Monk!	Sep 2018
34.	Rear Adm Monty Khanna, AVSM, NM	It is Time We Raised Our Own Maritime Militia	Oct 2018
35.	Lt Gen (Dr) NB Singh, PVSM, AVSM, VSM (Retd)	Equipment Capability Planning.	Oct 2018
36.	Gp Capt Ashish Singh, VM, VSM	The Two Forms of Reforms	Oct 2018
37	Maj Gen Bipin Bakshi, VSM	Information Warfare: Redefining National Security	Nov 2018
38.	Brig (Dr) Navjot Singh Bedi	Social Media & The Armed Forces	Dec 2018

Occasional Paper-2017			
1.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Defence Reforms-Transforming Indian Military Force to Military Power	Aug 2017
2.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Status & Honour Civil-Military Status Equivalence and Pay-Parity Need for Urgent Intervention	Nov 2017
3.	Brig SC Joshi, YSM, VSM (Retd)	Operation Cactus Maldives	Dec 2017
2018			
4.	Maj Gen (Dr) PK Chakravorty, VSM (Retd)	Manoeuvre Warfare	Apr 2018
5.	Shri R Chandrashekhar	The India Myanmar Trilateral Highway: Present Status”	May 2018
6.	Lt Gen Sunit Kumar	Cyber-Alike Nontraditional Wars (Combined)	Jun 2018
Issue Briefs-2017			
1.	Brig Ranjit Singh	Pragmatic Approach to Command of Unit.	Feb 2017
2.	Gp Capt GD Sharna, VSM (Retd)	Exploiting Indian Military Capacity in Outer Space	Mar 2017
3.	Lt Gen Gautham Moorthy, PVSM, AVSM, VSM (Retd)	Whose Life is it Anyway?	May 2017
4.	Brig Deepak Malhotra	Harnessing Social Media by the Indian Armed Forces.	Jul 2017
5.	Gp Capt GD Sharma, VSM (Retd)	Countering the Emerging Civil Drone Threat	Aug 2017
6.	Shri R Chadnrashekhar	Strategic Partnerships-Strengthening India’s Defence Manufacturing Base	Sep 2017
7.	Brig (Dr) Rajeev Kumar Bhutani (Rd)	Operationalisation of India’s Ballistic Missile Defence	Nov 2017
2018			
8.	Shri R Chadnrashekhar	China Pakistan Economic Corridor: Furthering the Initiative and Progress on Projects	Jan 2018
9.	Shri R Chadnrashekhar	India’s Armed Forces in the National Military Security Matrix-Need for ‘Comprehensive’ Integration	Apr 2018
10.	Brig (Dr) RK Bhutani (Retd)	Profile: China’s President XI Jinping	May 2018
11.	Gp Capt GD Sharma, VSM (Retd)	Examin Role for India in the Indo-Pacific Region	Jun 2018
2019			
12.	Brig Ranjit Singh	Pragmatic Approach to Counter Chinese Juggernaut in the 21st Century	Feb 2019

Monographs-2017			
1.	Brig (Dr) Rajeev Bhutani (Retd)	Reforming and Restructuring : Higher Defence Organization of India.	Jan 2017
2.	Shri R Chandrashekhar	Pakistan's Defence Industrial Base: An Overview.	Jan 2017
3.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd) Rear Admiral Vijai S Chaudhari, NM (Retd) Brig Ranjit Singh	Defence Diplomacy and International Military Co-operation	May 2017
4.	Brig Ranjit Singh	J&K Imbroglio: A Comprehensive Approach to Normalcy & Strategy to Deal with Pakistan	Jun 2017
5.	Col Arvind Sharma	Understanding Special Forces, Special Operations, It's Structure & Organisational Imperatives for India's Special Forces in the 21st Century	Sep 2017
6.	Col Laxman Singh	India's Foreign Policy Panchseel to Panchmrit: Changing Paradigms	Oct 2017
7.	Brig Deepak Malhotra	Social Media and the Armed Forces	Oct 2017
8.	Shri R Chandrashekhar	Gilgit and Baltistan Regions of Jammu and Kashmir State	Nov 2017
9.	Shri R Chandrashekhar	The Tibet Autonomous Region	Nov 2017
2018			
10.	Shri R Chandrashekhar	China-Pakistan Economic Corridor: Furthering the Initiative and Progress on Projects	Jan 2018
11.	Shri R Chandrashekhar	Gilgit Baltistan – Political Control Under Pakistan Occupation & Recent Developments	Jun 2018
12.	Shri R Chandrashekhar	Pakistan Occupied Kashmir	Jul 2018
13.	Col Arvind Sharma	Analyzing The Training Methodology of Special Operations Forces (SOF) of Foreign Armies & Recommendations for Conduct of Special Forces (SF) Training	Oct 2018
14.	Dr Manabrata Guha & Prof David J Galbreath	The Multi-Domain Battle Concept: A Preliminary Assessment	Dec 2018

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: www.cenjows.gov.in - Email: cenjows@cenjows.gov.in)

APPLICATION FOR LIFE/ ANNUAL MEMBERSHIP

To,

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

Dear Sir,

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

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

3. My particulars are given below:-

(a) Name in full ………………………………………………………………........

(b) Address:-

(i) Office/Unit……………..

Pin Code ……………………… Phone No …………....................

(ii) Permanent/Residential …………………....................................

…………………………………………......................................

Pin Code…................................ Phone No................................

Mobile No (Optional)……..

(iii) Email ……………………...

Optional Fields

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

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

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

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

4. Areas of expertise or interest:-

(a) ………………………………………………………….. …………...........

(b) ……………………………………………………………………….........

(c) ………………………………………………………………….................

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

……………………………………………………………………………….

……………………………………………………………………………….

6. Proof of my identity (Copy of passport/ voters ID Card/ 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:-

(i) Serving/Retired Officers	-	Rs 1,500/-
(ii) Civilians	-	Rs 10,000/-

(b)	Annual Membership	-	Rs 1,000/-