INFORMATION DOMINANCE: KEY ENABLER IN MULTI DOMAIN OPERATIONS

Brig Rajeev Ohri, VSM (Retd)

Abstract

Various erstwhile domains which were isolated but contributing to national power have been synergised through Information Domain. This has resulted in a paradigm conceptual shift with emergence of concepts like MDO and its contribution to CNP. The paper attempts a full spectrum understanding of information domain i.e. what all does it encompass, impact of compute and communication fusion and high speed wireless technologies, information domain sovereignty, niche and emerging technologies convergence, impact on new world order and civil military fused organizations and structures required to seamlessly absorb, manage and utilize these technologies to be ahead of the conflict/ competition curve in MDO scenario. The key to successful conduct of MDO is realignment from a technology centric to Protection, Control and Denial (PCD) based capability centric approach. Convergence of national resources in Information domain is the key to conduct MDO of the future.

Introduction

The world is transitioning from a bipolar to a multi polar geo strategic arena with aggressive competition in multiple domains other than military. Our national endeavour to restructure world organisations and realign international power structures is also based

on emergence of multiple domains which are contributing not only to Comprehensive National Power (CNP) of a nation but also a new world order. The traditional way of power evaluation, has also undergone a transition with emergence of multilple domains other than military playing a major role in national power projection. National Security, a subject which was considered a military exclusive and limited to land, air and sea domains has now graduated to a multi domain 'Whole of Nation' approach. Equally important is the synchronization of military capabilities with nationally integrated Instruments of Power.[1] The reasons for this shift need to be understood to identify core areas which have a direct bearing on national power and security. Emergence of concepts like Multi Domain Operations (MDO) (see Figure 1) are conceptually linked to CNP. MDO existed from ancient warfare times, but ability to conduct MDO through combination of Kinetic and Non-Kinetic means is a paradigm shift in recent times. The Non-Kinetic component is fundamentally everything other than the land air and sea domains. Since information domain plays a key role in synergising this capability it has become a major binding component of MDO and National Power. Information domain impacts efficiency of all domains. Ability to influence, convince and persuade beyond national boundaries has tremendously enhanced due to Information and communication technology transformation. Capabilities in niche technologies in Information domain need to be strategically synergised for Information dominance in MDO scenario. It will not be an exaggeration to say that concept of MDO has emerged because of Information domain.

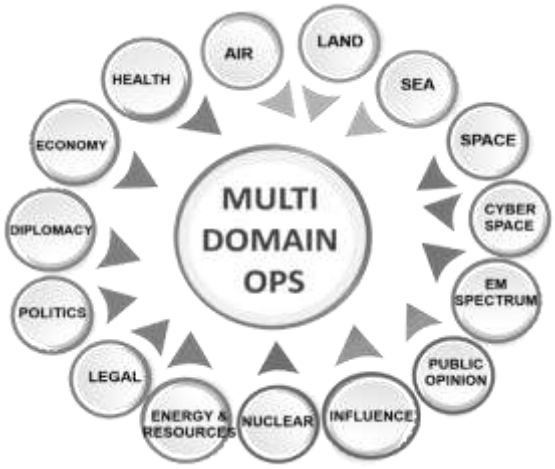

Figure 1 : Multi Domain Operations

Information Domain Emergence and Its Implications on MDO and CNP

The developments in Information domain in last few years has globally transformed war fighting and conceptually changed the security paradigm of many Armies and countries. A careful look at the multiple domains clearly brings two aspects viz each domain has an information domain backbone on which it is surviving and secondly the synergistic impact and linkage of each domain towards national power is made possible through information domain. Therefore, information has become an all encompassing domain which is critical for not only day to day successful operation of all domains but ability to share information across domains is the main enabler for synergizing multiple domains resulting in comprehensiveness in National Power.[2]

In order to catalyze MDO, strategic culture along with information domain awareness within each ministry/ department handling each domain needs to be built. The traditional national organizational structures which evolved with evolution of technologies, now need to realign to the converged information domain reality. Certain ministries like Ministry of Electronics and Information Technology (MEITY), Communications and I&B need convergence at National level for synergizing information domain for efficient MDO capability. Organisations need realigning from a technology centric to capability centric approach. Accordingly, regrouping of technology based organisations into capability based structures will be step in right direction for effective MDO capability.

Each domain requires three major capabilities viz Protection, Control and Denial (PCD). Protection is basically defence of the assets. We can also categorise it as Resource Enabler. Denial is offensive capability to deny the resources to adversary, or Resource Disruptor and Control is asset management or Resource Management to utilize the domain resources efficiently. Enhancing capabilities to protect own critical assets and deny these to the adversary in all domains have become vital to the National Security construct. Since Information Domain is the key to MDO, PCD concept template is recommended to be applied on this domain to generate national capabilities. It is important to not only handle the domain holistically but also have dedicated national level agencies for Protection, Denial and Management of Critical Information Infrastructure. Since Defence Networks

are an important asset of this Information Infrastructure, national expertise in both Civil and Military holds the key towards building capacities in securing, management and denial of not only defence networks but also information domain involved in national capability building. Erstwhile concept of segregating military from civil is no more relevant in 21st century multi domain whole of nation approach to conflicts / competition. Each domain organization needs to create a PCD capability within itself, besides the national level information domain PCD capability.

It is important to understand full spectrum understanding of information domain i.e. what all does it encompass, what is the new paradigm and emerging red lines on information domain sovereignty, where are niche and emerging technologies converging towards impact on new world order and finally the organisations and structures required to seamlessly absorb, manage and utilize these technologies to be ahead of the conflict/ competition curve in MDO scenario.

Information Domain : Emerging Technologies and Imperatives

Major technologies which have transformed the concept and conduct of operations in 21st century are primarily in Information domain. Core technology pertaining to Information and Communications Systems, Cyber,[3] EW and Space has majorly impacted our C4ISR (Command, Control, communication, Computer, Intelligence, Surveillance and Reconnaissance), degradation capability, OODA (Observe, Orient, Decide, and Act) cycles, Non-contact warfare through autonomous platforms, predictive analysis through AI and Big Data and overall ability to impose will on adversary with better perception management capability. The paradigm shift of flow of Info from wired to wireless domain has brought convergence of Cyber and EW domains. Accordingly, concepts on Cyber & Electro-Magnetic Activities (CEMA) have evolved in major Armies of the world.

The two major technology disruptions which are impacting Information domain and MDO are convergence of compute and communications and high data rate communication capability from wired to wireless domain. The erstwhile Combat Net radios which were the only means of exercising Command and Control are now getting replaced by Software Defined Radios, 4G/5G mobile communications, high bandwidth capable Satellite

handsets with inbuilt information processing capability for Navigation, Decision Support and military utility applications. This has resulted in major enhancements in Mobility, precision, battlefield transparency, shared situation awareness and overall shortening of OODA loop. If UAV (Unmanned Aerial Vehicle) / drones have revolutionised warfare, then the backbone of this revolution is Electromagnetic Spectrum (EMS) domain. From a spectrum perspective, all flow of info takes place in the EM Spectrum which has expanded from HF (High Frequency) / VHF (Very High Frequency) to the extremities of Light Waves. Therefore, denial of spectrum to adversary, control of vital Info flow, electromagnetic sovereignty and extraction of vital data and intelligence from spectrum have become synonymous with national power. In other words, spectrum has become a important sub domain of information warfare as is evident from organisation changes carried out by leading armies of the world. The EMS aspects need to be understood from Indian defence forces context in conjunction with existing pillars of our information philosophy. Creating CEW (Cyber and EW convergence) enabler and disruption capabilities is the recommended technology way ahead in Indian context.

Since synergy of MDO in modern warfare is enabled by Info domain, it is imperative that ministries like Railways, Telecom, Space, Air and Surface Transport, Power, Finance, Information and Broadcasting etc which are directly or indirectly involved towards defence capability, create strategic verticals for better planning, coordination and execution of projects for understanding impact of their overall capability to defence and CNP. Their information networks and data are vital targets for adversary information offensive and have a huge impact on our national defence capability. It is evident that this information domain linkage amongst ministries or domains requires a strategic infusion in all relevant ministries. Civil Military Fusion holds the key to this infusion and conduct of successful MDO.

Creation of National Critical Information Infrastructure (NCII) was a felt need in cyber domain and accordingly a protection centre was created. The NCII includes everything from financial systems and energy grids to transportation networks and government operations. Criticality of these domains for not only military but also for national power make them vulnerable to adversary info attacks. In order to protect the NCII from

malicious actors, it is important to have a robust security strategy in place. Cyber and EM sovereignty is gaining more importance than our traditional borders. There are large number of stake holders, as far as the NCII is concerned.[4] These include Transport, Telecom, Power and Energy, Banking and Financial Institutions, Strategic and Public

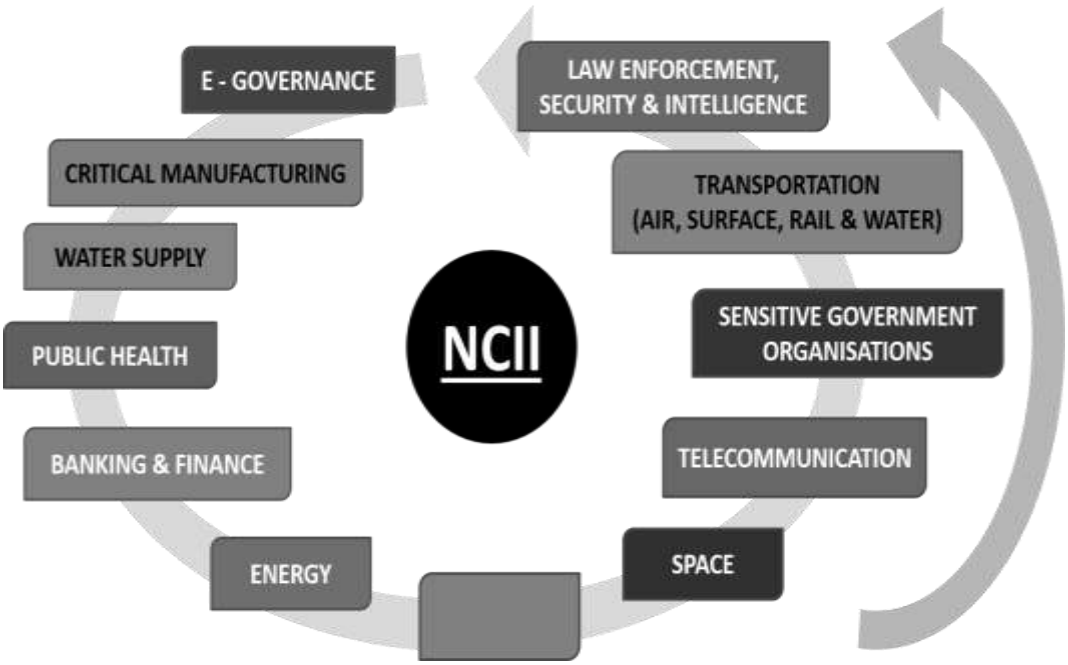

Figure 2 : National Critical Information Infrastructure

Enterprises and Government offices (see Figure 2). Each one of these sectors / organ has a charter to protect its assets. The role of the military in protecting NCII is limited to the protection of their own assets, just like every other stakeholder. With Info and Spectrum becoming key components of National Power, creating capabilities for its defence along with denial of this capability to adversary have become imperative for any nation.

Capability Development in Information Domain

Lack of CMF has resulted in Indian Armed Forces lagging behind in terms of technology. This is inspite of India being a superpower in the fields of information communication technology (ICT) and space. While the IT sector is booming, with new startups and businesses emerging every day, the Armed Forces are still struggling to evolve into an

agile eco system at par with national industry with adaptive capability for technology absorption.

Spectrum is the domain that needs major attention due to shift from wired to wireless and the convergence of Cyber and Electro Magnetic Spectrum operations. However, it is also the domain where expertise lies with the Academia, R&D and Industry. Synergy between the Armed Forces, Research and Development (R&D), Academia and Industry would prove to be a powerful engine of innovation and is a must for achieving the desired end state of Info Domination through CMF.

The Indian Armed Forces can benefit immensely from this synergy. The industry has the required expertise and experience to help the armed forces modernize their capabilities specially in areas of non kinetic warfare. The two can also cooperate in research and development to develop new technologies that can be used by the armed forces. It would also go a long way in fueling the dreams of "Make in India" and "Atmanirbhar Bharat".

However, for this synergy to be effective, the CMF in the Info Domain has to follow a whole of nation approach, with an Umbrella Information Organisation (see Figure 3) at the National level. This has to be an empowered Info domain organization, with cross ministerial linkage with MeitY, Information and Broadcasting (I&B), Finance and the Industry ministries. Such an umbrella org is the solution to handle Info domain holistically and create synergy amongst all stakeholders. This will also provide a template for capability based organization rather than technology centric approach. Convergence of national resources in Information domain is the key to conduct MDO of the future. All domains also need to build PCD capability around this template, so that there is a seamless connect between various ministries and MDO agencies. Since defence domain is one of the main components of MDO, need for Information Command (Figure 4) on similar capability based organization is imperative. This will synergise our national resources for suitable national MDO capability on lines of developed nations and counter response to northern adversary information domain organization.

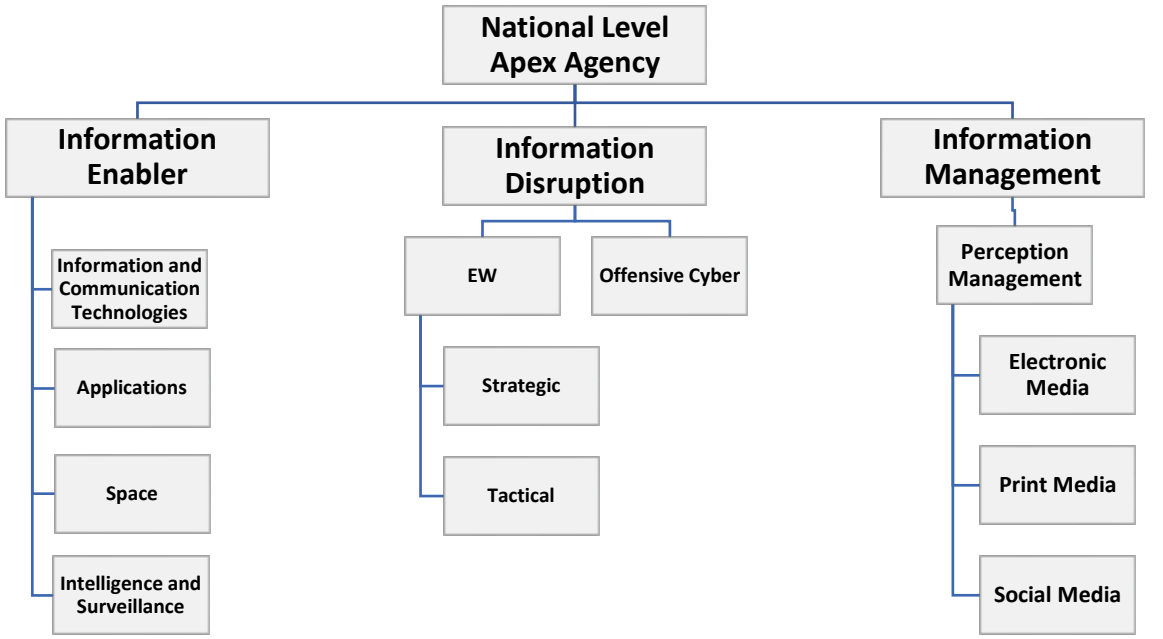

Figure 3 National Information Umbrella

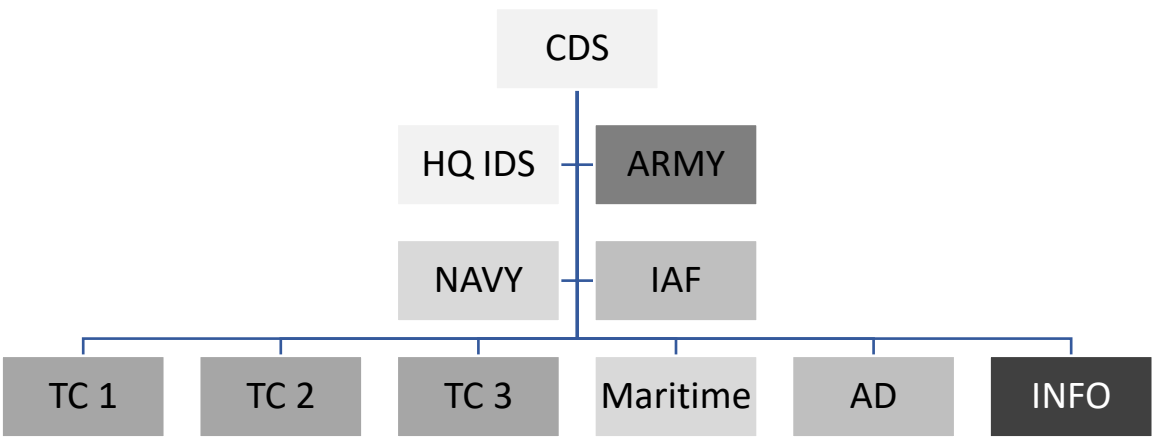

Figure 4 : INFORMATION COMMAND - KEY TO MDO

Further sub division of Info enabler verticals needs to be based on synergy of various niche emerging technologies based on logical grouping given in Figure 3 above. This will pave the way for futuristic coherence of emerging technologies into tangible operational

capabilities. It is important that capability development in these verticals / technologies is handled by appropriate agencies / organisations which have the ability to synergise stakeholders and take it to logical conclusion. Adhoc tasking and piecemeal actions will result in time and effort dissonance. Therefore, formulation of appropriate logical structures based on technology convergence and CMF is the way forward.

Recommendations : Defence capability, CMF, MDO and CNP

- **Military Information Service**. Information and EMS domain requires a specialisation oriented de novo look at HR management. In view of the limited HR availability and major capability thrust required to create and sustain evolving defence information infrastructure, there will be a requirement to induct non-combatant subject matter experts for effective management of the backend infrastructure and processes. This will enable combatants to handle the challenges in combat zone. Creation of a non-combat Military Information Service will be a step-in right direction. This will assist in not only taking on backend Information domain tasks but also bring Civil Military Fusion to a logical conclusion.

- **EM Spectrum Operations**. Since Information exchange is shifting from wired to wireless mode, Electromagnetic spectrum domain is the defining domain for MDO. National PCD capability in this domain is imperative to conduct Electromagnetic Spectrum Operations (EMSO). Spectrum is key Information enabler through Spectrum intelligence and Surveillance. In order to build a national EMS capability, it is important that there is seamless exchange of spectrum intelligence exchange between national agencies and field formations. This capability is recommended on lines of Geo Intelligence framework. The huge spectrum intelligence gathering capability of field units can be utilised by multiple agencies through this framework. This will also facilitate in removing overlaps in multiple agencies undertaking similar spectrum related tasks but also overcome the technology challenges faced by field formations. In Information Security area, high capacity data transfer capability shift from wired to wireless has brought to fore the requirements of over the air security protocols. Security development and testing agencies need to find de novo solutions for this

evolving dimension. Moreover, in a joint force concept, interoperability will hinge on seamless information security.

In the Spectrum Management. area, demand for this premium resource from multiple agencies is going to increase by the day. Evolved solutions will facilitate a collaborative and deconflicted spectrum usage philosophy. R&D in this domain will pay rich dividends in future. Electro Magnetic Interference (EMI) / Electro Magnetic Compatibility (EMC) aspects will also gain prominence with enhanced density of emitters and intense dependence on EM radiations by multiple stake holders in combat zone. Expertise in combat zone spectrum management is a requirement which will gain prominence. In Information Denial capabilities, spectrum will play a key role in strategic target degradation. Therefore, need for a strategic EW capability under national info umbrella is imperative for MDO and CNP.

- **Navigation Technologies.** GIS and Geo location has emerged as key technology for not only military but also civil agencies. It is imperative, that the vulnerability of these technologies be minimized by indigenous terrestrial solutions rather than global space based solutions.

- **Mobile Technologies**. The form factor, processing capability, data capacity and multi utility applications of mobile segment has direct relevance in military domain. Somehow, in absence of a military grade mobile technology with inbuilt Electronic Protection features, this high utility, relatively low-cost technology has not been exploited for military purposes. It is time this challenge is thrown open to industry to make this technology available to military for C4ISR in a contested EM space in the form required. This will be a good alternative to SDR technology since, infrastructure for creating military mobile in Indian context with non-expansionist ideology is relatively easy to implement.

- **Training Transformation**. In order to leap frog in Info domain, there will be requirement of training transformation based on CMF. While the leadership has to adapt to hybrid approach of handling kinetic and non-kinetic domain, the execution has to adopt a specialisation approach. Multinational collaboration and cooperation

will be key for a faster transition.[5] Collaboration with appropriate civil agencies based on core strength, infrastructure sharing, common training protocols need consideration.

Conclusion

The evolving global conflict scenario indicates a clear shift from pure kinetic to MDO scenario, where nation states need to evolve from traditional kinetic attrition concepts to developing PCD capabilities in multiple domains. This transition has been catalysed by information domain which itself is gravitating towards electromagnetic spectrum capabilities. Concepts like Information and Electromagnetic sovereignty are taking centre stage. Multiple technologies primarily in information domain are evolving rapidly. The solution space for information dominant conflict lies in finding indigenous, simple workable solutions. The ever-evolving technology poses challenges of fast obsolescence and high cost. Tendency to run after every new technology needs to be curbed. Nation states need to follow capability based approach to converge technologies towards developing PCD capability in each domain. Since information domain is the binding force for MDO, it is imperative that a national information umbrella organisation created which converges national capabilities towards an efficient structure which provides a template for all domains. Civil Military fusion hold the key for bringing strategic culture in all domains and enhancing technical capability of defence domain. Nation states with ability to synergise all stake holders of this domain through CMF have better probability of success in dominating info and EMS space.

****

Brig Rajeev Ohri, VSM (Retd) is an alumnus of IMA, Dehradun. His operational assignments include Signals Intelligence during OP VIJAY, Commanded Signal Regiment in OP HIFAZAT, Deputy Brigade Commander of Strike RAPID Brigade in Deserts and Chief Signal Officer on Line of Control in OP RAKSHAK J&K. The officer has done UN tenures in Rwanda. Brig Ohri has had staff tenures in WARDEC, MS Branch, GSO1 (Ops) in new raising HQ IGAR (S), Col (Ops & Plg) in Information System & Brig PMO SURAJ where he was awarded VSM for his contribution to EW capability building.

NOTES

1 Multi Domain Operations in NATO https://www.act.nato.int

2 Chapter: 1 The Multi-Domain Operations and the 2035 Operational and Technology Environment National Academies of Sciences, Engineering, and Medicine. 2021. Powering the U.S. Army of the Future. Washington, DC: The National Academies Press. https://doi.org/10.17226/26052.

3 Domain Operations in Future High-Intensity Warfare in 2030 https://codcoe.org

4 The Italian Defence Approach to Multi-Domain Operations https://www.difesa.it

5 Unlocking Training Technology for Multi-Domain Operations https://www.rand.org