ENHANCING PREPAREDNESS FOR CHALLENGES IN THE CYBER, EW AND IW DOMAINS

Brig (Dr) Navjot Singh Bedi*

Abstract

Mobile technology has integrated a number of technologies as multiple applications have converged into singular devices (ie mobile phone/ tablet/ laptop), with the ability to transmit wirelessly. However because of this, data based attacks can now impact the voice channels also, as voice over IP (VoIP) protocol allows voice to be carried over the data networks. On account of being a wireless device (and being the gateway to internet), mobile phone is therefore susceptible to exploitation of the Electro Magnetic (EM) spectrum. These mobile devices may have thus become a potent platform for propaganda (ie IW) as is often seen in the valley, for Cyber related activities but are consequently also susceptible to IW, Cyber Warfare and EW because the means to access & infect a computer network are now available at physical layer in the form of Radio Frequency (RF) linkages. Technologies like mobile phone, satellites, wireless backhaul radios, Software Defined Radio (SDR) etc in military networks are thus vulnerable to cyber-attacks through wireless channels also. Boundary lines between telecom, IT, Cyber, EW & IW domains have started blurring and there is a need to understand the role played by Cyber, EW and IW domains & the interplay between them.

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 make it redundant, for example the replacement of horse mounted cavalry by Armoured Fighting Vehicles (AFVs).Future warfare is likely to be Multi Domain Warfare (MDW) which is envisioned as a more complex concept that will expand the operational scope and reach of a nation's strategic-military establishment and will include a number of disruptive technologies. Though there are many such technologies which will drive these changes and which will play a major role in all future conflicts, this paper will only discuss the role played by Cyber, EW and IW domains and in Enhancing Preparedness for meeting Challenges in these domains.

Cyberspace & Cyber Domain

There has been a surge in the internet usage at not only the global level, but at the national level as well. The COVID pandemic since the last year and a half has seen an upsurge in the utilisation of internet for business, education, e-commerce and has consequently increased our vulnerability to Cyber-attacks. It's important to understand that cyber-warfare refers to the use of digital attacks by one country or nation to disrupt the computer systems of another, with the aim of creating significant damage, death or destruction, either directly or indirectly.

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. This section of the paper explains the subtle difference between Cyber Warfare (CW) and what cannot be classified as Cyber warfare, various response mechanisms for the same and capacity and capability building as a means of enhancing preparedness to meet challenges in this domain.

History: Disruptions in Cyberspace. In 2007 cyber war went from theoretical to actual, when Estonia found itself under a furious digital bombardment that knocked banks and government services offline. However, the DDoS attacks on Estonia did not create physical damage and it was not considered to have risen to the level of actual cyber warfare. However, the Idaho National Laboratory proved, via the Aurora Generator Test, that a digital attack could be used to destroy physical objects; in this case a generator. Stuxnet malware in 2010 proved that malware could impact the physical world. In 2013 the NSA said it had stopped a plot by an unnamed nation to attack the BIOS chip in PCs, rendering them unusable. In 2014 the attack on Sony Pictures Entertainment, blamed by many on North Korea, showed that it was not just government systems and data that could be targeted by state-backed hackers. In Dec 2015, hackers managed to disrupt the power supply in parts of Ukraine, by using a well-known Trojan called Black Energy. In March 2016 seven Iranian hackers were accused of trying to shut down a New York dam in a federal grand jury indictment. Nations are rapidly building cyber defence Nations are rapidly building cyber defence and offence capabilities. NATO in 2014 took the important step of confirming that a cyber-attack on one of its members would be enough to allow them to invoke Article 5, the collective defence mechanism at the heart of the alliance. In 2016 it then defined cyberspace as an “operational domain” ie an area in which conflict can occur: the internet had officially become a battlefield. In Oct 20, the Cyber-attack that shut down the

electrical grid of Mumbai, plunging millions into darkness, was reportedly a Chinese cyber-attack (as suggested by the New York Times). The 07 May 21 ransomware attack on Americas Colonial Pipeline was reportedly carried out by a criminal hacking group, for which the ransom in crypto currency of 75 Bitcom ie nearly USD 5 Million was paid. After this attack the US President signed a Cyber security executive order, establishing a series of initiatives designed to letter equip federal agencies with Cyber security tools and encourages improvements in digital security standard across the private sector, which has been hit by a spate of Cyber-attacks.

Implications. Cyber warfare or Disruptions in Cyberspace is going to be a significant component of every present and future conflict. Future wars will also be fought by hackers using computer code to attack an enemy's infrastructure, as well as troops using conventional weapons like guns and missiles. But unlike standard military attacks, a cyber-attack can be launched instantaneously from any distance, with little obvious evidence in the build-up, and it is often extremely hard to trace such an attack back to its originators. Modern economies, underpinned by computer networks that run everything from electricity, transportation sanitation to food distribution and communications, are particularly vulnerable to such attacks, especially as these systems are in civil domain, and are rarely designed to be secure against hackers. Thus digital attacks against vital infrastructure like banking systems or power grids, give attackers a way of by-passing a country's traditional defences. As per some experts, it's a case of when, not if.

Cyberwarfare vs "Not Cyberwarfare". Whether an attack should be considered to be an act of cyber warfare depends on a number of factors to include the identity of the attacker, what they are doing, how they do it and how much damage they inflict. Like other forms of war, cyber warfare is usually defined as a conflict between states, not individuals. As cyber war is best understood as conflict between nations, then that excludes a lot of attacks which are sometimes described as cyber warfare. For example attacks by individual hackers/ groups of hackers, would not usually be considered to be cyber warfare, unless they were being aided

and directed by a state (which is however a dangerously common trend). For example, cyber-crooks who crash a bank's computer systems while trying to steal money would not be considered to be perpetrating an act of cyber warfare, even if they came from a rival nation. But state-backed hackers doing the same thing to destabilise a rival state's economy might well be considered so. The nature and scale of the targets attacked and weapons used is another indicator of the differentiation. Defacing an individual company's website is unlikely to be considered an act of cyber warfare, but disabling the missile defence system at an airbase would certainly come at least close.

Continuum of Conflict. A moot point is that Cyber warfare does not take place only during actual hostilities! In this hyper connected digital world of ours, Cyber warfare is an everyday reality and without formally realizing it or acknowledging it, Cyber warfare related activities are already being carried out by various parties, (ie Individuals, Hack-activists, Non State Actors, State Supported Actors/ Direct State Involvement) during Peace, Low Intensity Conflict, Mid Intensity Conflict, High Intensity Conflict. Live cyber threats are in fact an ongoing process and all our actions need to be aligned to it. There is thus a pressing need to put in place response mechanisms to address these emerging challenges.

Present Capacity & Capability Building for Emerging Cyber Challenges

Cyber Capabilities of Two Nations. The best way to arrive at a figure on the Cyber qualified HR required is to take a cue from the capability of few nations. It is in comparison to all these that India needs to put in place a credible Cyber Force. Details of the same in respect of two nations are as listed below:-

(a) **China**. It has an established PLA Cyber Command & Strategic support Force (SFF). It can bank upon a dedicated force of 7000 persons but the strength may increase to 130,000 persons including the Cyber militia (which could be banked upon to augment the Cyber Force in times of hostilities). The

Mandaint Report lists out the Cyber capabilities of China. The Chinese JSD4 is a specialized unit dedicated for this activity. In the Chinese Philosophy, Electronic Warfare (EW) and Cyber Network Attack (CNA) are inter-mixed and they even talk in terms of Electro Magnetic Space Operation (EMSO). The EW and Cyber Operations are thus addressed in a combined manner. The Chinese also have a specialized unit i.e. Unit 61398 which is a part of JSD3 Deptt. A large number of Advance Persistent Threats (APT) (e.g Titan rain, Aurora etc.) have been rumoured to have been developed there.

(b) **USA.** US Cyber Command unifies the direction of Cyber space ops, strengthens DoD Cyber Space capabilities and integrates & bolsters DoD's Cyber expertise. As per literature available in open source, the cyber mission force available with the US Cyber Command is 133 Cyber Mission Teams (CMT's). The composition of these teams varies from 50-100 members each. The USA has approximately 6000 Cyber warriors. Their Cyber force is divided into 133 teams of which 60 are Defensive Cyber Warrior Teams and 73 are offensive in nature. These 133 Cyber Mission Teams are further sub divided into five different types of teams. These teams and their role and tasking, is equally applicable in the Indian subcontinent. These five types of teams are :-

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

(ii) **National Support Team (NST)**. These would provide analytical support to NMT and would be a team of highly skilled Cyber Technicians who would be employed to develop the cyber weapon to be launched by the NMT. Taken together, we may loosely assign the role of NMT and NST to the role

that is currently being performed/ envisaged to be performed by National Technical Research Organisation (NTRO) at strategic level, in India.

(iii) **Cyber Mission Teams (CMT)**. The CMT will be closely associated with the Operational plans at the Combatant Operational Command level and will provide cyber support for the same i.e. for the various theatre commands.

(iv) **Combatant Support Team (CST)**. The CST will provide analytical support to the CMT i.e. akin to analytical support being provided by NST to the NMT.

(v) **Cyber Protection Team (CPT).** The cyber protection team will have a primarily defensive role, which may be akin to the role of ESM (Electronic Support Measures), in the context of Electronic Warfare.

Present Capacity /Capability. Approximate 1500-2000 Cyber trained personnel are available with various Govt agencies and in private sectors the approximate capacity available would be about 15000 to include National Security Data Base (3000 plus), InfoSec Community (5000), Talent at School\Colleges & IIT's etc (3000 plus), Start-ups involved in new tech like AI\Robotics (1500 plus), and Independent Actors\Freelance Cyber Security Analysts (2000 plus).

Capacity Required. There is a need to put in place a frame work to bring clarity in the capacity required for various cyber security roles which are:-

(a) Undertaking R&D in new technology.

(b) Implementing existing technologies.

(c) Managing existing ICT infrastructure.

(d) Securing ICT infrastructure.

(e) Managing ICT infrastructure.

(f) Having adequate HR to fill all cyber related posts to undertake the tasks listed above is a practical way to put a figure on the HR required and a figure of 50,000 is a good figure to work with. However putting a cap on the type of Networks/ systems needed is rather difficult. It is thus evident that as on date, the force available with India needs to be considerably augmented.

Capability and Role. It can be seen that we need developmental teams to develop a Cyber weapon and operational teams to optimally launch the exploit. Since these are specific task oriented special units, hence their equipment profile and manning norms will be different, will be dictated by their role and are likely to be dynamic. However, as per the template being followed internationally, it can be safely assumed that each unit would require between 50-100 personnel. The availability of highly skilled cyber trained personnel and their retention is another issue which needs to be addressed.

Knowledge Sharing. Though individual groups of experts in this field often share knowledge / experience but these are exceptions rather than the norm. There is negligible expertise in development of Operating System (OS). The Service Sector needs to step in this field and if we have to be taken seriously as a nation, then like China, we must develop and use our own indigenous Operation System

Capability Demonstration. Of late there has been no capability demonstration to showcase our potential. Such a capability demonstration (as was witnessed in the Cyber-attack on Estonia), is essential and akin to a controlled nuclear explosion as it acts as a deterrence and wards off adversaries/ potential adversaries. There is apparently a lack of developmental activities to produce a “Stux Net” type of weapon (which possibly entailed four million man hours of research work by a joint team of personnel from two developed nations). Such a weapon, if indigenously developed is a game changer. This was an ideal Cyber weapon which was intended for re-use and gave three to four zero day

exploits. It was a type of Cyber weapon which is developed once in a century and was not intended to be exposed to the world. However its effect beyond anticipated reach, led to it being analysed in detail and to its subsequent exposure.

Human Resource. This is the “Achilees Heel” of this programme as the required number of skilled personnel are neither readily available nor have they been tapped. As explained, approx 6000 personnel are required to man and equip 133 functional Cyber Operations units of USA, which works out to roughly the strength of two infantry brigades. This figure may seem miniscule compared to the 1.2 million strong standing Army that India possesses but it may come as a surprise to many that it is extremely difficult to identify, recruit, train and retain this limited pool of manpower in such a niche field.

Identification & Recruitment of HR Talent. The people gifted in this field (yes gifted & not trained or skilled) are few and far between & hard to find. These are not your stereo type academically inclined individuals who will crack the UPSC exam for selection into Cyber Command. Nor would they be the type who conforms to the standard norms of military discipline. Such individuals would more often than not be rebels or non-conformists. They would be brilliant (possibly bordering on the edge of eccentricity) and focused only on cyber related activities (hacking, cracking, launching exploits, trolling the web etc).They might even be adjudged as misfits in society. An ideal Cyber warrior would not necessarily only be young teenage kids who are cyber savvy. An ideal Cyber Warrior would in fact be a person who has at least 10 years of experience in this field and who has moved on beyond the thrill of cracking a password or hacking into an account or defacing a website. However age and conventional experience would be required to be disregarded if we intend to nurture & recruit talent. This is so because its quite likely that the young disinterested teenager, who is forever busy on his play station PSP-3 or is a social misfit (preferring PC’s & on line face book chatting rather than face to face talk), might be a potential recruit to be one of your potential cyber warriors. It is in a way akin to the lateral

induction of JS level officers into the bureaucracy, as proposed by our Hon'ble PM, which was opposed by the entrenched lobby-but the moot point is are we ready for that in the Armed Forces?

HR Capacity Building. The approach should be long term. It must be analysed as to who would be the people in the field 15 years from now and the effort to train them should start from today. This is not just about recruiting people from the private sector and altering QRs to suit them to serve in sensitive government agencies. Instead, an effort should be made to develop them within the respective government agencies. The best example of one such long term recruiting programme is the SSB/ NDA exams and recruitment for the defence services. A similar approach should be carried out in identifying the Cyber specific talent very early and building up and nurturing the same. There is no better agency than the defence services to do this job. The Recruitment & HR policies to attract and retain suitable talent in field of Cyber space can be structured suitably.

Israel Model. Israel's programme of conscription for two years for serving in the **IDF** is for all citizens. However from amongst this pool of HR, the best talent who show technical capabilities, is supposedly identified and provided with an extended tenure of nine years, during which period they build the best systems for the Defence Services. The Israel govt identifies new technologies where R&D and manufacturing capability (ie Business requirement) exists and people with these skill sets leaving the IDF are given responsibility to create start-ups in these niche fields. The recruitment programme for India should thus incorporate both technical aspects to Capture. The Fire (CTF concept), as well as psychometric tests to discern the passion quotient of the prospective candidates.

Technology Capacity Building. India could identify a couple of high technology areas like IC fabrication, 5G & IoT, Propriety Communication Technology, AI, Cryptography & Pure Mathematics and pump in money into R&D to develop indigenous models of the same. An economically priced model of this could be mass produced for commercial supply,

in order to capture the market and generate profit. The profit could be used to further improve the product, which could then be priced slightly higher for supply to elite group of customers and possibly later compete at the global forum also, thus generating more profit. Hopefully the cycle would make our product manufacturing self-sustaining and perhaps even profitable. In order to achieve this, there is a need to develop new R&D facilities and nurture new faculty and suitably reward, acknowledge & retain talent in order to build indigenous items as per global scenario.

Immediate Mitigation Techniques. While capacity & capability building may take time, measures pertaining to People, Processes &Technology can be taken immediately. These are:-

(a) **People**. Continuous awareness campaign, trained system administrator, operational & functional Security Op Centre (SOC) & periodic engagement with LEAs.

(b) **Processes**. There should be a regular Cyber drills including Business continuity Plans (BCP) and Disaster Recovery (DR) plans must be in place and rehearsed.

(c) **Technology**. All internal PCs must be scanned thoroughly with end point protection and AI based behavioural detection platforms should be used to monitor probable suspects. Honeypots could be used to lure and find Red Flags and one can consider using VMS/ appliance for internet browsing. In addition measures be addressed for hardening of devices.

Research & Development (R & D) Support Wing. Offensive Cyber Ops Units can't be expected to develop Cyber Weapons (as is generally expected of various Cyber organisations). For development of graded cyber weapons we are not looking at tapping "Script Kiddies". We need to develop and carry out hard core research. These developers would be distributed amongst various Cyber Operations Support units/ teams and each unit will be unique and different and will be involved in development of a Cyber weapon for use by a Cyber Operations Unit. This wing is in fact

a key enabler of the capability of cyber agency to translate the intent into action. The range of R & D activities will be very wide and will start from the requirement to evolve platforms to fire and control Cyber Weapons. Development of indigenous Penetration Testing tools (of the standard of Core Impact, Impact Canvas, Metasploit etc) would be another key task of the R&D wing. The entire "exploit" should to be properly packaged and should facilitate ease of use by the Cyber Operations Unit.

Cyber Doctrine. A Joint Cyber Operations Doctrine needs to be promulgated at the earliest. Guiding principles for such a doctrine should include that the following: resources for Offensive Cyber Operations must be deployed down to tactical levels. In any scenario involving state-to-state conflict which may not necessarily imply declared hostilities but also hostile actions attributable to adversary state, the primary authority/ responsibility for Cyber Ops should rest with the MoD/Armed Forces, including authority over cyber resources available with other ministries. In addition a completely fresh HR and training philosophy should be evolved to meet the unique needs of Cyber Ops.

Cyber Training. Structured training for Defensive Cyber Ops is already being carried out by the three Services. Extensive training for Offensive Cyber Ops, right up to post-graduate level, should be carried out at respective premier training institutions within the three Services (for example, Naval Signals School Kochi for Navy and AFTC for IAF and Military College of Telecommunication Engineering for the Army). Efforts should be made to sponsor specialist post-graduate courses in Cyber Ops, including ethical hacking, to be conducted at leading educational institutions within the Country and abroad.

Electronic Warfare & Information Warfare Domain's

EW being a precursor to IW but now comprises part of IW, hence both are being discussed together, with the aim being to suggest Information Warfare (IW) and EW structures which are effective enough to match up to the challenges of 21st Century warfare. However, given the existing

status of EW & IW preparedness of our Armed Forces, the viability requirement is, perhaps, the greater challenge. Thus, in order to move pragmatically from where we are to where we wish to be, this analysis adopts a transformational, as opposed to a revolutionary approach towards achieving the desired capabilities. Though EW is an old and established concept, yet is still evolving. However IW being a nascent, complex and dynamically evolving field of warfare, developing the conceptual and doctrinal basis for IW structures is an important first step. Equally important, in this highly specialist field, identifying the right human resource (HR) philosophy is at least as important as arriving at optimum organisational structures and should, in fact, be a driving parameter while arriving at choice of structures. *[1]*

Concepts Doctrine & Existing Organisational Structures

EW. There is an on-going debate in the US Department of Defence (DoD) whether or not a sixth domain, namely the Electro-Magnetic (or EM) Domain, needs to be added to the existing five-dimensional battle space construct.[8] The motivation for such thinking is the increasing importance being accorded in the US to developing Electronic Warfare (EW) capabilities after decades of neglect, perhaps spurred by the rapid advancements made in this field by formidable potential adversaries, particularly China.

IW in 21st Century Battlespace. IW was previously nothing more than just a supporting means for conducting a kinetic multi-domain battle in the physical domain. Today, however the scenario is radically different, with the US having established a Cyber Command in 2010,[2,3] China working with fervour to achieve dominance in the information domain by building capabilities, notably its Strategic Support Force (SSF),[4] and most significantly, Russia demonstrating an increasing degree of maturity in the IW field, going by the success of its information campaigns in Estonia, Georgia and Ukraine.[5] The powerful role of social media in the de-stabilisation/overthrow of established regimes during the Arab Spring (which in Russian perception, was the result of “subversive information

technologies of the West"), brought in a new dimension to war-waging in and through cyberspace.[6,7] The concept of *Information* Warfare took root in the 1990s and has matured remarkably after the turn of the century.

IW Doctrine. The first Joint IW Doctrine was issued in 2005, which was revised in 2010, the current version. The first Indian Army (IA) IW Doctrine was issued in 2004. A revised doctrine was subsequently promulgated in 2010, which is the current version.

Tri Service IW Establishments. At the tri-services level, there are two organisations related to IW: the erstwhile Defence Information Assurance and Research Agency (DIARA) and the Defence Intelligence Agency (DIA), both functioning under the aegis of HQ Integrated Defence Services (IDS).[9] Originally established as the Defence Information Warfare Agency (DIWA), DIARA subsequently got re-designated with it's focus being on Cyberspace Operations. DIARA has recently been upgraded to the Defence Cyber Agency (DCyA), which is hopefully a precursor of the Cyber Command proposed by the three Services. The DIA coordinates the intelligence effort of the three Services and provides a common interface with the civil intelligence community. DG DIA is a member of the Intelligence Coordination Group, which works under the NSA. He is also a member of the National Information Board (NIB) as well as the Apex Committee on Satellite Surveillance Board. He controls the strategic assets like Defence Imagery and Photo Analysis Centre (DIPAC) and Signals Intelligence (SIGINT).

Individual Service Specific IW Establishment. Integrated employment of Information Operations (IO) is being carried out as a staff function at various headquarters. At Army Headquarters level, the Additional Director General Military Operations (ADG MO) (IW) is responsible for all aspects of Cyber, EW and PSY Ops. Similarly, the Indian Air Force (IAF) has the Directorate of IW. The ADG Public Information (PI) is an ad hoc organisation in the Army chartered to carry out the Public Affairs / Information function. As regards field formations, specific IW related staff set-ups exist at some higher headquarters, while at others this function

is carried out by the operations staff officers in addition to their other duties. As regards individual IO functions, establishments exist for the Cyber Ops and EW functions, but not for Psy Ops. The defend function for Cyber Ops and EW is the combined responsibility of all users of the network end-points and of the EM spectrum respectively. The specialist task of defence of common user networks (for both Cyber and EM spectrum aspects) is primarily the responsibility of the Corps of Signals in the Army (and its equivalents in the other two sister services).IW & Cyber establishments which are presently in existence are as under:-

(a) **Cyber**. The Army Cyber Group (ACG) is mandated to carry out all aspects of Cyber Ops for the IA, less the implementation of offensive measures. It also functions as Cyber Emergency Response Team (CERT)-Army. Some of its primary functions include cyber audit, cyber forensics, cyber evaluation of new systems, etc. Policy formulation and cyber audit in the field formations is carried out under the aegis of IW staff, with the primary manpower resource for the audit teams being provided by Signals.

(b) **EW**. Army EW resource being scarce, EW groups/ sub-groups are presently placed directly under Command Headquarters from considerations of efficient utilisation. Notwithstanding this, their employment is entirely at tactical levels in close support to the fighting formations. The application of this resource is primarily for execution of the “Attack” and “Exploit” sub-functions. In the IAF and the Indian Navy (IN), EW effort mostly focusses on platform based non-communication (anti-radar) capability. There is a major capability building required to be undertaken in this domain.

(c) **IW/PSYOP**. Presently, there are no formal PSYOP establishments in existence.

(d) **Public Relations Organisation (PRO)**. Public Affairs (PA)

is the purview of Ministry of Defence (MoD) & its PR machinery ie PRO Defence. Regional PROs posted at various stations report to the PRO Defence and are not under local formation commanders or staff, thus remaining largely out of sync with the needs of our Armed Forces.[10]

Human Resource Development (HRD). Some of the main highlights of the HRD philosophy being followed by individual Services are as given below:-

(a) **Cadre Management**. In the case of officers, postings to all IW assignments (Cyber, EW, IW) are on tenure basis. For other ranks a special trade, common for SIGINT and EW tasks, exists in the Corps of Signals.

(b) **Training**. IW training for officers is conducted by Army War College, with some participation from the IN and the IAF. EW and Cyber Security training for Army officers is conducted by the Military College of Telecommunication Engineering (MCTE), Mhow which is the declared Centre of Excellence (C of E) for these disciplines. For the IAF, IW training is being conducted by their IW School at Bangalore. For subordinate ranks in the army, structured training for EW/SI is being conducted by the Signal Training Centres. Joint training is being carried out presently only on EW, on a rotation basis, by Army, Navy and Air Force and at their respective training establishments at Mhow, Kochi and Gwalior. There is some participation by the Navy and the Air Force on IW courses being conducted by the Army for officers at the Army War College, Mhow. PsyOP exposure is being given to officers as part of command oriented courses at various levels, or capsule courses at civilian institutions mostly on a volunteer basis. There is no specialist training being conducted within Services specifically for PSYOP or Strategic Communications.

Limitations & Suggested Remedial Measures

IW Doctrine. There is a need to substantially update existing IW doctrines at the Joint Services as well as individual Service levels. In view of the ambiguity in the definition of IW terminologies worldwide, these doctrines must make a deliberate effort to rigorously define terms as applicable in the Indian context. The doctrines must emphatically endorse the operational imperative that conflict in this artificial and virtual dimension is at par with the traditional notion of conflict in the physical realm and not is merely in support of it. The doctrines should characterise and classify Cyber Ops, EW and Psy Ops as the major streams of IW and as being distinctly different. An unequivocal stress must be laid on the critical importance of achieving specialisation in each of the IW functions, and a viable HR philosophy spelt out to meet this end.

EW Doctrine. *Joint Doctrine For Electronic Warfare: 2010* published by HQ IDS, Ministry of Defence (MoD) lays down the doctrinal concepts in EW domains. This document merits a review in light of the overwhelming advances in improved communication, information, surveillance, reconnaissance capabilities and net-worked command and control elements, which must be gainfully exploited to fight a high-tech warfare. A revised Joint Doctrine on EW, followed by separate EW Doctrines by each of the three Services, needs to be promulgated. The doctrines should emphasize the critical role of EW in 21st Century battle space, as well as the degree and manner of coordination with cyber resources, in order to achieve the desired synergy in military Infospace.

EW Organisation. The recently concluded Armenia – Azerbaijan conflict has brought to light the efficacy of Drones and a soft kill option against the same is through ECM using EW. With the ever expanding use of the EW spectrum for diverse weapon platforms, there is a need to enhance the number and capability of EW units. The quantum of Army EW units/formations needs to be significantly increased with the aim being to provide an EW Group per Corps HQ in order to provide the requisite EW support to fighting formations. Once additional EW

formations are raised, these should be placed under Corps Headquarter for integrated functioning, with EW Sub-Groups being placed in support of Divisional Headquarter. The model of Integrated Control Centres Blocks (Communication plus Non-Communication) is recommended to be adopted for optimal utilization of EW resources. ELINT resources should ideally be merged with the EW Groups. Strike Corps EW elements should be equipped to have matching mobility and be deployed well forward (within combat groups) for achieving a tangible force-multiplier effect. Specific requirements of providing EW support in mountainous and High Attitude Areas needs to be addressed.

EW and SI Units. The EW organisations are best structured to acquire tactical SIGINT through its ESM function. However, in Counter Insurgency (CI) scenarios within the country, SI units too, under the direct control of the Tri-Services SI Directorate, are deeply involved in this activity. Existing command and control structures are not conducive for achieving the requisite synergy between these two capabilities. Thus lateral sharing of intelligence at various levels in the hierarchy of these two organizations is recommended. Likewise, ELINT resources are currently placed under the Military Intelligence (MI) Directorate, whereas radar signatures collected by ELINT units are primarily meant to be exploited for ECM by EW units on outbreak of hostilities. Thus merging ELINT resources with the EW Groups would be an optimal solution.

EW HR Philosophy. HR philosophy for EW is recommended to be modified based on the following considerations:-

(a) **Cadre Management**. In general, a much higher degree of specialisation than what is presently existing is considered essential. In the case of officers, the postings policy must be modified to ensure repeated tenures in EW establishments. For instance, criteria for command of an Army EW Sub-Group/ Group must require at least one/ two prior EW tenures respectively. For other ranks, EW specific trades (operators/ mechanics) must be created and rotated strictly amongst EW units/ establishments (and not in SI units).

(b) **Training**. The quality and quantum of structured training at all levels, including through conduct of joint services courses, needs to be significantly upgraded. Also, specialist components of IW courses should be conducted by designated centres of excellence in the respective disciplines and select personnel be sent abroad to attend super specialization courses.

(c) **R&D and Project Management**. Skill development for execution of EW tasks is equally challenging as for cyber skill development. However project management for EW systems requires highly specialised expertise, especially as Indian R&D in this area is presently not comparable to global standards. A fillip to domestic R&D, can be given by including by private players, and by making special endeavours to obtain the best technology existing in the world market. The govt to govt procurement route be adopted for specialist technology as this may not be freely available. The quality of our Project Management Organisations (PMOs) in all three Services need to be improved and supported by giving project based long tenures to EW specialists in PMOs.

IW Doctrine, Cadre Mgt & Training. Future wars are likely to be characterized by ascendancy of technology. "Information Warfare Doctrine For The Indian Army: 2010" published by Headquarters Army Training Command (ARTRAC), lays down the doctrinal concepts in Information Warfare (IW). In order to develop IW to the desired degree of maturity, stiff resistance to modifying organisational charters as they exist today would first need to be overcome. Thereafter, considerable efforts will need to be devoted to developing expertise in all the IW disciplines, especially as regards building up narratives and management of social media, most of which happen to be in very nascent stages, especially in the context of the complex 21st Century battlespace.

(a) **IW Concepts and Training**.Limited exposure by way of short capsules on media management is being provided at the Institute of Mass Media, under aegis of HQ IDS and in some

of the command oriented courses at different levels of service. Commanders and staff entrusted with IW tasks, by virtue of their tenure-based assignments, carry them out mostly on the basis of their general military experience, as also on the strength of short-term institutional knowledge which might exist within their establishments. This ad hoc approach to Perception Management (PM) & IW disciplines needs to be improved upon, especially in today's information intensive world. Suitable steps be initiated for developing these disciplines to a degree of professional maturity, duly adapted to our strategic environment. A joint doctrine for IPO, covering concepts and employment modalities for individual functions as well as the interplay amongst them, needs to be promulgated. To the extent feasible, it is desirable to issue a similar doctrine (if not same) separately for the Army IAF & IN such that all the three services are in synch and reinforce each other's efforts. In this field, time is of essence and one cannot be found to be reacting. We should in fact have narrative ready for various situations/scenarios, with well laid out timelines / triggers for taking various actions. To the extent feasible, the authority to take action/ release media bytes, as per the planned & rehearsed narrative needs to be delegated to the GSO1 / Col (and equivalent rank officers) manning the desk at the instant, as time is of essence.

(b) **IW Cadre Management**. Although trained manpower for the IW disciplines is required by all the three Services, presently there is no specialist manpower available with any of the Services barring a handful number of people trained in capsule courses. A suitably structured tri-Service training institute should also be established as a centre of excellence under aegis of HQ IDS for the IW discipline of PM, Social Media & Info Ops. Initially training in these fields could be conducted at the Army War College. PSY Ops demands staff as well as ground resources for executing operational tasks. Specialist training needs to be imparted for

all personnel involved in PSY Ops tasks. Cadre management at officer level could be based on providing repeated tenures In IW / PI /PRO, after suitable specialist structured training has been imparted. The Defence PRO needs to be recast as per the operational needs of the Armed Forces to rise up to the challenges of the Social Media & Information Age. PRO should be placed under command of the Armed Forces and additional cadre may be recruited if needed. The ADG PI as an organisation should carry out its tasks through the IW cell/section at each formation Headquarter, down to the Corps Headquarter. The activities of these cells should be coordinated by the Operations staff at all levels. These cells must carry out 'truth projection', and be involved in the PSYOP functions of shaping the narrative in the Social media. Being a national effort, close coordination with the Ministry of Home Affairs (MHA) as well as Ministry of External Affairs (MEA) is needed for effective execution of IW tasks.

Conclusion

The potency and overwhelming lethal effects of Cyber warfare, Electronic warfare & IW has outpaced the technological development in conventional military weapons space, changing the very character of future wars, and the role of cyber warfare in them. A conceptual understanding of the large number of disciplines involved between Cyber, EW & IW and, more importantly, the interplay amongst them, is key to evolving optimum organisational structures. The key driver for bringing about the requisite improvement / transformation would be the conviction that the nature of warfare in this Information Age is changing in fundamental ways. The EW, Cyber & IW Ops do not merely support operations but at times lead / shape the conventional operations and may even preclude the use of conventional boots on grounds. All this demands, more than merely organisational changes, radically new models of HR philosophy, covering recruitment, training and career progression aspects for the technically inclined EW, Cyber & IW specialists. For this to happen, a

change in existing mind-sets is essential, which by far is the greatest challenge.

***Brig (Dr) Navjot Singh Bedi** is a former Senior Fellow Centre for Joint Warfare Studies (CENJOWS), New Delhi

Bibliography

1. Mathew S. Cohen, Charles D. Freilich and Gabi Siboni. "Israel and Cyber space : Unique Threat and Response". International Studies Perspectives (2015)0, 1-15.
2. Keir Giles. "Information Troops"- a Russian Cyber Command? Conflict Studies Research Centre Oxford, UK.
3. James A. Lewis and Katrina Timlin. "Cyber security and Cyber warfare.Preliminary Assessment of National Doctrine & Oganisation Center for Strategic and International Studies.
4. William Slater and Matthew Crosston, "A Brief Arief Analysis of Russian Cyberwafare Capabilities – Past, Present and Future".
5. Gil Baram. "The Effect of Cyber war Technologies on Force Buildup : The Israeli Case". Military and Strategic Affairs/Volume 5/No. 1/May 2013.
6. Colonel Deepak Sharma. "China's Cyber Warfare Capability and India's Concerns". Journal of Defence Studies.
7. Charles Billo. "Cyber Warfare : An Analysis of the Mean and Motivations of Selected Nation States". Institute for Security Technology Studies at Dartmouth College.
8. Joseph E Sission. "Fleet Cyber Command/Tenth Flee: Enabling Cyber Unity of Effort". July 2016 91
9. John.F.Sarkesain, Thomas W. O'Brien. "A Framework for Achieving Dynamic Cyber Effect through Distributed Cyber Command Control/ Battle Management (C2/BM)". The Aerospace Corporation.
10. Noman R Howes, Michael Messino, John Sarkesain. "On Cyber Warfare Command and Contrl". Institutes for Defence Analyses.
11. Thomas.C. Wingfield. "Integrating Legal and Policy Factors in Cyber Preparedness".
12. Jean-Loup Samaan."The RUSI Journal, Cyber Command". Royal United Services Institution.
13. Hans_LngeLango. "The Academic Debate on Cyber Security". Internasjonal Polikk 71(2).
14. M.C. Libicki. "Conquest in Cyberspace National Security and information Warfare". Cambridge University Press.

15. Tipping the Scales: the attribution Problem and the Feasibility of Deterrence Against Cyber Attack". Research Article.

16. Rechard Baskerville. "Agile Security for Information Warfare: A Call for Research". Research Gate Publisher.

17. Brig Navjot Singh ; Proposed Role and Organizational Structure of Cyber Command and Cyber Operations Units, published in July 2016 issue of SYNERGY, journal of CENJOWS; https://cenjows.gov.in/upload_images/pdf/Layout%20Inside_Synergy.pdf

18. Mathew S. Cohen, Charles D. Freilich and Gabi Siboni. "Israel and Cyber space : Unique Threat and Response". International Studies Perspectives(2015)0, 1-15.

19. James A. Lewis and Katrina Timlin. "Cyber security & Cyber warfare. Preliminary Assessment of National Doctrine & Oganisation Center for Strategic and International Studies.

20. William Slater and Matthew Crosston, "A Brief Arief Analysis of Russian Cyberwafare Capabilities – Past, Present and Future".

21. Gil Baram. "The Effect of Cyber war Technologies on Force Buildup : TheIsraeli Case". Military and Strategic Affairs/Volume 5/No. 1/May 2013.

22. Colonel Deepak Sharma. "China's Cyber Warfare Capability and India's Concerns". Journal of Defence Studies.

23. Charles Billo. "Cyber Warfare : An Analysis of the Mean and Motivations of Selected Nation States". Institute for Security Technology Studies at Dartmouth College.

References

1. Toward an Effective and Viable information Warfare Structure for the Indian Armed Forces* Lt General RS Panwar, AVSM, SM, VSM, PhD (Regt)

2. The Department of Defence Cyber Strategy, Office of US Secretary of Defence, Washington, Apr 2015, pp. 5.

3. Cyberspace Operations, US DoD Joint Publication 3-12 (R), 05 Feb 2013.

4. The Strategic Support Force: Update and Overview in China Brief, Volume 16 Issue 9 The Jamestown Foundation, Dec 2016.

5. Michael Connell and Sarah Vogler, Russia's Approach to Cyber Warfare, CNA's Occasional Paper, March 2017.

6. Keir Giles, Handbook of Russian IW, Fellowship Monograph No 9, NATO Defence College, Nov 2016, pp. 9, 36.

7. Keir Giles, Countering Russian IO in the Age of Social Media, Digital and Cyberspace Policy Program, Council on Foreign Relations, New York, Nov 2017.

8. Sydney Freedberg, Spectrum (EW) Should be a Domain of Warfare: Rep. Bacon, Breaking Defence, 29 Nov 2017, https://breakingdefense.com/2017/11/spectrum-ew-should-be-a-warfighting-domain-rep-bacon/

9. Brig Vinod Anand, Integrating the Indian Military: Retrospect and Prospect, Journal of Defence Studies Vol 2 No 2, Winter 2008, IDSA, pp. 36-37.

10. Lt Gen S A Hasnain, Image Challenge for The Indian Armed Forces, Vivekanand International Foundation Blog, Mar 2016, http://www.vifindia.org/article/2016/march/14/image-challenge-for-the-indian-armed-forces-take-it-by-the-horns.