16th Major General Samir Sinha Memorial Lecture, 2018

Towards an Effective and Viable Information Warfare Structure for the Indian Armed Forces*

Lieutenant General RS Panwar, AVSM, SM, VSM, PhD (Retd)[@]

Introduction

The primary focus of this work is to suggest Information Warfare (IW) structures which are effective enough to match up to the challenges of 21st Century warfare. However, given the existing status of 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.

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 importantly, 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 the choice of structures.

In the complex 21st Century battlespace, the role of IW is gaining prominence vis-à-vis the entire spectrum of conflict. Nonetheless, organisational structures for any military capability must necessarily be optimised for a “total conflict” scenario, as this is likely to be the most demanding in terms of resources. Scenarios lower down on the escalatory ladder could then be catered for through suitable modifications to structures and processes.

At the outset, it is also pertinent to highlight that there is no common understanding of the term “Information Warfare”. Indeed, the interpretations of this and other related terms are so diverse that, in order to carry out a coherent discussion on the subject, it is important to clarify the sense in which terminologies and associated concepts are used. Against the above backdrop, the attempt here is to first dwell on the basic considerations, and then outline an approach for creating the right IW structures for our Armed Forces.

Concepts and Doctrine

IW in 21st Century Battlespace

Until just about a decade ago, it would have been hard to find theorists and practitioners of IW who claimed that IW was more than just a supporting means for conducting a kinetic multi-domain battle in the physical domain. Today, the scenario is radically different, with the US having established a Cyber Command in 2010,[1,2] China working with fervour to achieve dominance in the information domain by building capabilities, notably its Strategic Support Force (SSF),[3] 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.[4] 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.[5,6]

It is interesting to note that while it is the concept of *Information* Warfare which took root in the 1990s and matured remarkably after the turn of the century, it is *Cyberspace* which found its place alongside the traditional domains of land, sea and air and then space, in a multi-dimensional battlespace.[7,8] This is perhaps because of the unique characteristics of cyberspace, allowing cyber-conflicts of various hues to occur during peace as well, without fear of escalation.

The term *Cyber* itself eludes a precise definition, with one view stating that it has lost all meaning.[9] In its most generic interpretation, *Cyber* is in fact a synonym for *Information.* The most common perception of the term *Cyberspace* would probably be as follows: information (at rest or in motion) and information systems, inter-connected as a global network (the Internet). But what if the network in question is air-gapped, as was the Iranian nuclear facility intranet which was attacked using the Stuxnet malware? Would an isolated network of combat radios transporting voice, data and even video information in a tactical scenario be considered a segment of Cyberspace?

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 battlespace construct.[10] 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. It needs to be kept in mind, however, that assigning *domain* status implies designation of a separate jurisdiction together with suitable allocation of resources.

If the EM Domain is indeed designated as the sixth warfighting domain, then the only major sub-component of IW without an associated domain would be Psychological Operations (PSYOP), making it a notable exception. Against this backdrop, rather than designating a separate domain for each IW capability, it is worth considering whether there exists a case for replacing *Cyberspace* with *Infospace* as a warfighting domain.

Existing Organisational Structures – Indian Armed Forces

Tri-Services Level

Doctrine. The first Joint IW Doctrine was issued in 2005, which was revised in 2010, the current version.

IW Establishments. At the tri-services level, there are two organisations related to IW: the Defence Information Assurance and Research Agency (DIARA) and the Defence Intelligence Agency (DIA), both functioning under the aegis of HQ Integrated Defence Services (IDS).[11]

(a) Defence Information Assurance and Research Agency (DIARA). Originally established as the Defence Information Warfare Agency (DIWA), DIARA subsequently got re-designated to its current nomenclature. It was initially established to handle all aspects of IW. However, while on paper the functions remained the same, the focus of DIARA is on Cyberspace Operations (CO). Approval has been accorded late last year to upgrade DIARA to the Defence Cyber Agency (DCA), which is a whittled down form of the Cyber Command proposed by the three Services as early as 2012.

(b) Defence Intelligence Agency (DIA). The Defence Intelligence Agency (DIA) coordinates the intelligence effort of the three Services and provides a common interface with the civil intelligence community. Director General 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).

Training. Joint training is being carried out presently only on EW, on a rotation basis, by the Army, the Navy and the 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.

Public Relations Organisation (PRO). Public Affairs (PA) is the purview of the Ministry of Defence (MoD) and its archaic PR machinery, termed PRO Defence. Regional PROs posted at various stations report to the PRO Defence, and are not under the local formation commanders or staff, thus remaining largely out of sync with the needs of our Armed Forces.[12]

Individual Service Level

At the Service level, integrated employment of Information Operations (IO) is being carried out as a staff function at various headquarters. As regards individual IO functions, execution establishments exist for the CO and EW functions, but not for PSYOP or its concomitants (PA, Military Deception (MILDEC). It is pertinent to note here that the Defend function for CO and EW is the combined responsibility of all users of the network end-points and EM spectrum respectively. Also, the specialist task of defence of common user networks (both cyber and EM aspects) is the responsibility of the Corps of Signals (and its equivalents in the sister services).

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

Staff Organisations. At Army Headquarters level, the Additional Director General Military Operations (ADG MO) (IW) under Military Operations Directorate is designated as the Chief Information Security Officer (CISO) for the IA and is responsible for all aspects of CO, EW and PSYOP. Similarly, the Indian Air Force (IAF) has the Directorate of IW. The ADG Public Information (PI) is an ad hoc organisation chartered to carry out the PA 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.

IW Establishments. IW establishments which are presently in existence are as under:-

(a) **CO**. The Army Cyber Group (ACG) is mandated to carry out all aspects of CO for the IA, less the implementation of defensive 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.

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

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 (CO, 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 the 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 for these disciplines. For the IAF, IW training is being conducted by their Information Warfare School at Bangalore. For lower ranks, structured training for EW/SI is being conducted by the Signal Training Centres.

PA 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 the Services specifically for PSYOP/MISO/PM, MILDEC or Strategic Communications.

Effective and Viable IW Structures

Having discussed the conceptual underpinnings of the major IW functions and the interplay amongst them, and to some extent the IW organisational structures in the Indian Armed Forces, this section attempts to suggest how one might move towards more effective structures in a manner which is feasible.

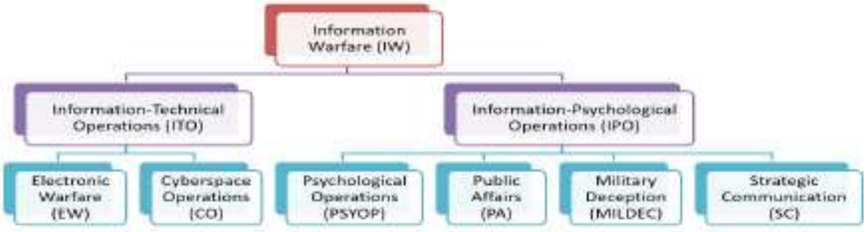
IW Doctrine

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 be based on the model of a five-dimensional battlespace, with Infospace rather than Cyberspace as the fifth dimension. They 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 merely in support of it.

The doctrines should characterise and classify the following major streams of IW as being distinctly different: Information-Technical Operations (ITO), comprising of CO and EW functions, and Information-Psychological Operations (IPO), covering PSYOP, MILDEC, PA and SC. Also, mechanisms to achieve inter-stream integrative and intra-stream synergistic effects should be spelt out.

In addition to its traditional orientation towards foreign audiences, SC should be defined and characterised so as to be responsive to the prevailing Counter Insurgency (CI) scenario in terms of the desired perception management, without resorting to the term PM. An overview of other aspects brought out in succeeding paragraphs with respect to individual doctrines (CO, EW, IPO), as also the manner in which the Intelligence function relates to IW capabilities, must also be spelt out in these doctrines.

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. The logical relationship amongst IW streams and functions is depicted below.

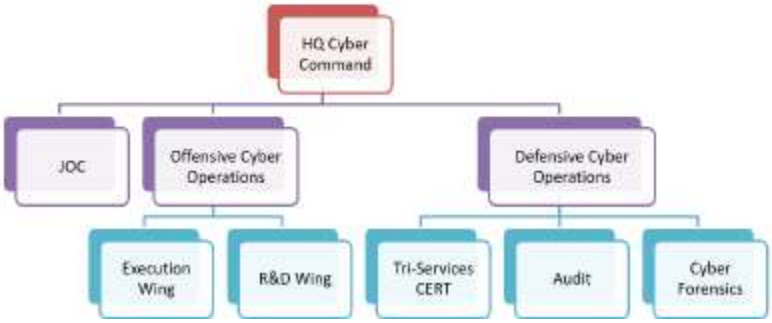

Information Warfare (IW)
Information-Technical Operations (ITO)
Information-Psychological Operations (IPO)
Electronic Warfare (EW)
Cyberspace Operations (CO)
Psychological Operations (PSYOP)
Public Affairs (PA)
Military Deception (MILDEC)
Strategic Communication (SC)

Information-Technical Operations

ITO as a separate major sub-stream of IW, signifies the strong synergetic relationship which exists between the CO and EW functions. The level of operational deployment as well as the nature of expertise required to take these functions towards greater maturity have also been indicated. Keeping all these factors in view, it is felt that organisational convergence across these two functions should be achieved by having a common line directorate for them in each Service. However, purity of the individual functions should be maintained at the functional unit level. Synergy in their operational deployment is recommended to be achieved through either staff coordination or, in specific scenarios, through task-based grouping of teams from both these domains of expertise. Intra-ITO staff coordination at each Headquarter must be by the specialist line directorate component at that Headquarter. However, overall staff coordination between the ITO and IPO functions should be carried out by the IW/ Operations staff at each Headquarter. Since EW manifests itself primarily at the tactical level, an important underlying assumption here is that employment of CO at the tactical level is considered to be an operational imperative.

CO: Way Forward

Doctrine. A Joint Cyber Operations Doctrine needs to be promulgated at the earliest. Guiding principles for such a doctrine should include the following: resources for Offensive Cyber Operations (OCO, to include CNA and CNE) must be deployed down to tactical levels; in any scenario involving state-to-state conflict (which may not necessarily imply declared hostilities), the primary authority/ responsibility for CO should rest with the MoD/Armed Forces, including authority over cyber resources available with other ministries; and, a completely fresh HR philosophy should be evolved to meet the unique needs of CO.



Organisation. A full-fledged tri-Services Cyber Command should be raised for carrying out OCO (CNA/CNE), with the same urgency and determination as was the case for the Mountain Strike Corps; as part of this Command, in addition to a Command HQ, cyber units should be raised and deployed down to tactical levels, along with intermediate subordinate HQ as felt necessary; while HQ may be inter-Services in structure, Service purity should be maintained at unit level, similar to the model which has been adopted by the Signal Intelligence Directorate (SI Directorate); cyber units should be of two broad flavours: cyber execution units and cyber R&D units, with each of R&D units focusing in a different area of expertise in support of the execution units; command and control structures should be put in place in line with the philosophy of 'centralised control, decentralised execution', in order to address the disadvantages of deploying offensive cyber resources at multiple echelons; suitable linkages should be established with EW organisations at all levels for achieving the desired synergy between these two capabilities.

HR Philosophy. HR philosophy is recommended to be modified based on the following guidelines:-

(a) Line Directorate. One of the following three options is available for consideration: raise a separate Inter-Services Cyber Corps; raise service-specific Cyber Corps; or, raise sub-cadres within existing Service Line Directorates. It is recommended that, to begin with, the last option be adopted. In the case of the IA, the only suitable candidate line directorate is the Corps of Signals, which is already mandated to carry out Defensive CO (DCO/CND); similar solutions be identified in the IN and the IAF.

(b) Cadre Management. A permanent cadre for OCO be put together through selections, based on aptitude, from within existing uniformed cadre already available and trained for DCO, as well as by means of direct recruitment from expertise available within the country. The Territorial Army (TA) option may be considered only to meet surge capacity, once permanent sanctioned cadre has been fully made up. In the case of officers, to begin with a profile based on repeated tenures ('concentrations') should be considered as a career progression model, whereas for other ranks, induction into the cyber cadre should be on a permanent basis.

(c) Training. Structured training for DCO is already being carried out by the three Services. Extensive training for OCO, right up to post-graduate level, should be carried out at respective premier training institutions within the three Services (for example, Military College of Telecommunication Engineering for the Army). Efforts should be made to sponsor specialist post-graduate courses in CO, including ethical hacking, to be conducted at leading educational institutions within the Country.

EW: Way Forward

Doctrine. A 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 battlespace, as well as the degree and manner of coordination with cyber resources, in order to achieve the desired synergy in military Infospace.

Organisation. The quantum of Army EW units/formations needs to be significantly increased (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 in support of Divisional Headquarter. The model of Integrated CC 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 (please see section on the Intelligence function below). 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.

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.

R&D and Project Management. On the one hand, skill development for execution of EW tasks is not as challenging as for cyber skill development. On the other, project management for EW systems requires highly specialised expertise, especially as Indian R&D in this area is far below global standards. Although efforts should be made to give a fillip to domestic R&D, including by private players, in the interim special endeavours must be to obtain the best technology existing in the world market, especially as this may not be freely available. The first step in this direction is to improve the quality of our project management organisations (PMOs) in all three Services. In order to make this happen, giving project based long tenures to EW specialists in PMOs is an essential prerequisite.

Information-Psychological Operations

This work has focussed briefly on the PSYOP, PA, MILDEC and SC functions. As stated above, an overall alignment and synergy is desirable amongst these four functions, which are recommended to be grouped under a separate stream of IW, termed as Information Psychological Operations (IPO). In order to develop IPO 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 IPO disciplines, most of which happen to be in very nascent stages, especially in the context of the complex 21st Century battlespace.

Concepts and Doctrine. A formal study of the IPO disciplines under discussion here has never been undertaken by the Armed Forces with any degree of seriousness. Limited exposure by way of short capsules on media management (PA) is being provided in some of the command oriented courses at different levels of service. Commanders and staff entrusted with IPO 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 IPO disciplines leaves much to be desired, especially in today’s information intensive world. It is vital, therefore, that 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. In addition, it is desirable to issue a similar doctrine separately for the Army which, in the context of our national security, has the most significant role to play in this area.

Cadre Management. Although trained manpower for the IPO disciplines is required by all the three Services, the numbers required are small. Also, presently there is no specialist manpower available with any of the Services. In view of this, it would be prudent to establish a new tri-Service line directorate for managing all the IPO disciplines. A suitably structured tri-Service training institute should also be established as a centre of excellence for the IPO disciplines. As a first step in this direction, a separate wing could be set-up at the Army War College. Broad recommendations for individual IPO disciplines are given out in succeeding paragraphs.

PSYOP. PSYOP demands staff as well as ground resources for executing operational tasks. Specialist training needs to be imparted for all personnel involved in PSYOP tasks. To begin with, cadre management at officer level could be based on providing repeated tenures, after suitable specialist structured training has been imparted. For lower ranks, creation of a specialist cadre is desirable. The strength of the cadre, the structure of execution elements and the nature of training to be imparted will emerge once concepts and doctrine in this important area have been developed. Due to its "black" content, this function is recommended to be kept firewalled from PA.

PA. The Defence PRO needs to be recast in such a manner as to rise up to the challenges of the Information Age, and in conformity with the operational needs of the Armed Forces. For this to happen, this resource should be placed under command of the Armed Forces for all purposes, or at the very least for operational deployment and training. Additional cadre may be recruited if needed. With respect to the IA, the ADG PI as an organisation should be formally sanctioned, and should carry out its tasks through PA Cells (re-cast PRO) at each formation Headquarter, down to the Corps Headquarter in the initial phase. The activities of these cells should be coordinated by the Operations staff at all levels. From considerations of credibility, these cells must carry out only 'truth projection', and be shielded from PSYOP functions.

MILDEC. MILDEC must necessarily be a function of the Operations staff at any Headquarter, since planning for military deception is inextricably linked to actual operational plans.

Officers specially trained in this discipline need to be posted to various Headquarter. However, raising of specialist units is not felt necessary for carrying out MILDEC tasks.

SC. Existing literature on SC in the military context is based on deployment scenarios for expeditionary forces, such as in Iraq, Afghanistan, Ukraine, etc. In the Indian context, SC of this flavour may not be so applicable. However, the basic principles of SC are relevant to CI scenarios prevalent in the Valley as well as the North-East. Such an umbrella concept would comprise of, in addition to PSYOP and PA, activities such as interaction with political and civil functionaries, *Sadbhavna* and Aid to Civil Authorities in the affected areas, sometimes referred to as Civil Affairs (CA). An important point to note is that, since PM as a term is perceived to have "black" connotations, it is felt that perception management of own populations as a function would be better covered under this umbrella terminology. Being a whole of government approach, close coordination with the Ministry of Home Affairs (MHA) as well as Ministry of External Affairs (MEA) is needed for effective execution of SC tasks. In addition to its relevance to CI operations, since our Armed Forces have a role in foreign countries as well by way of defence attachès, maritime diplomacy, participation in UN missions, etc., SC need to evolve with a tri-Services perspective. At this juncture, the only viable recommendation that may be made is to develop a formal joint services doctrine on SC. In the interim, the endeavour must be to continue making progress on development of the SC related IPO functions (PSYOP, PA).

IO vis-à-vis the Intelligence Function

It has been brought out earlier that the IW Exploit function is essentially the acquisition of intelligence using information weapons, specifically the ES and CNE sub-functions of EW and CO respectively. At the same time, acquisition of intelligence through Signal Intelligence (SIGINT) capabilities of Intelligence organisations also play out in the EM domain. SIGINT is the combination of Communication Intelligence (COMINT) and Electronic (or Non-Communication) Intelligence (ELINT) functions, which are essentially ES manifestations at the strategic level. Traditionally, it is HUMINT which has been the primary source of intelligence acquisition at the strategic level. In the wireless, networked world, however, HUMINT is gradually yielding ground to SIGINT and CNE for strategic intelligence collection.

In the Indian context, the Defence Intelligence Agency (DIA) at the tri-Services level, using the considerable SI Directorate resources at its disposal, is mandated to carry out SIGINT activities. It is but natural for the SI Directorate to attempt to develop CNE capabilities for acquiring strategic intelligence. However, in the scenario of a Defence Cyber Agency (DCA) and subsequently a Cyber Command being established, for the DIA to carry out CNE activities in parallel would amount to wasteful duplication of effort, and is hence not recommended.

The EW organisations are best structured to acquire tactical SIGINT through its ES function. However, in 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. This needs to be corrected by suitably modifying the existing command and control hierarchy.

In a similar vein, 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 EA by EW units on outbreak of hostilities. Here too, suitable organisational re-structuring appears to be warranted. While merging ELINT resources with the EW Groups would be an optimal solution, placing ELINT units directly under the Theatre Commands could be a good interim step in this direction. Further study in this area is recommended.

Conclusion

This work has endeavoured to analyse the intangible and multi-disciplinary arena of IW against the backdrop of a complex 21st Century battlespace, with the specific intention of suggesting effective and viable IW structures for the Indian Armed Forces. A conceptual understanding of the large number of disciplines involved and, more importantly, the interplay amongst them, is key to evolving optimum organisational structures. A large number of recommendations have been made, both in terms of doctrinal improvements as well as organisational re-structuring.

It is felt, however, that the key driver for bringing about the requisite transformation would be the conviction that the nature of warfare in this Information Age is changing in fundamental ways, which demands, even more than organisational changes, radically new models of HR philosophy, covering recruitment, training and career progression aspects. For this to happen, a change in existing mind-sets is essential, which by far is the greatest challenge. This work is primarily an effort to contribute towards addressing this challenge.

Endnotes

[1] *The Department of Defence Cyber Strategy,* Office of US Secretary of Defence, Washington, Apr 2015, pp. 5.

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

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

[4] Michael Connell and Sarah Vogler, Russia's *Approach to Cyber Warfare,* CNA's Occasional Paper, March 2017.

[5] Keir Giles, *Handbook of Russian IW,* Fellowship Monograph No 9, NATO Defence College, Nov 2016, pp. 9, 36.

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

[7] *Cyberspace Operations,* US DoD Joint Publication 3-12 (R), 05 Feb 2013, pp. I-2.

[8] Lt Gen (Dr) RS Panwar, *Cyberspace: The Fifth Dimension of Warfare,* Future Wars, Jan 2018, http://futurewars.rspanwar.net/cyberspace-the-fifth-dimension-of-warfare-part-i/.

[9] James Shires and Max Smeets, *The Word Cyber Now Means Everything—and Nothing At All,* Dec 2017, http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_ lost_all_meaning.html.

[10] 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/

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

[12] 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.

Compendium of Abbreviations

1.	ACG	-	Army Cyber Group
2	CC	-	Command and Control
3	CERT - Army	-	Computer Emergency Response Team - Army
4	CI	-	Counter Insurgency
5	CISO	-	Chief Information Security Officer
6	CNA	-	Comprehensive Network Attack
7	CND	-	Computer Network Defence
8	CNE	-	Computer Network Exploitation
9	CO	-	Cyberspace Operations
10	DCA	-	Defence Cyber Agency (upgraded version of DIARA)
11	DCO	-	Defensive Cyberspace Operations
12	DIA	-	Defence Intelligence Agency
13	DIARA	-	Defence Information Assurance and Research Agency
14	DIPAC	-	Defence Imagery and Photo Analysis Centre
15	DIWA	-	Defence Information Warfare Agency
16	EA	-	Electronic Attack
17	ELINT	-	Non Communication Electronic Intelligence
18	EM	-	Electro-Magnetic Domain
19	ES	-	Energy Source
20	EW	-	Electronic Warfare
21	HUMINT	-	Human Intelligence
22	IO	-	Intelligence Officer
23	IPO	-	Information-Psychological Operations
24	ITO	-	Information Technical Operations
25	IW	-	Information Warfare
26	MILDEC	-	Military Deception
27	NIB	-	National Information Board
28	NSA	-	National Security Advisor
29	OCO	-	Offensive Cyberspace Operations
30	PA	-	Public Affairs
31	PI	-	Public Information
32	PM	-	Perception Management
33	PMO	-	Project Management Organisation
34	PRO	-	Public Relations Organisation.
35	PSYOP	-	Psychological Operations

36	SC	-	Strategic Communications
37	SIGINT	-	Signal Intelligence
38	SSF	-	Strategic Support Force

*****This is the edited text of the 16th Major General Samir Sinha Memorial Lecture delivered by Lieutenant General RS Panwar, AVSM, SM, VSM, PhD (Retd), on 04 Apr 2018 at the United Service Institution of India, New Delhi. The complete text has been published as USI Occasional Paper No -3-2018.

[@] **Lieutenant General RS Panwar, AVSM, SM, VSM (Retd),** holds a PhD degree in Computer Science from the Indian Institute of Technology Bombay, and is a Distinguished Alumnus awardee of this premier institution. He superannuated as Commandant of the Military College of Telecommunication Engineering. His current areas of interest include technology driven future warfare, covering aspects such as Network Centric Warfare, Information Warfare and Artificial Intelligence based military autonomous systems, amongst others.

Journal of the United Service Institution of India, Vol. CXLVIII, No. 612, April-June 2018.