INFORMATION WARFARE : CONCEPTS AND COMPONENTS

Major General Bipin Bakshi
VSM, Department Of Defence Studies ChaudharyCharan Singh University, Meerut.

Received: August 24, 2018 Accepted: October 15, 2018

ABSTRACT *In the new age of Hybrid Warfare, nations have shifted to use of Information Warfare as an unconventional method to impose their National Will on an adversary with apparent anonymity and without violating international laws on sovereignty of other nations. Information Security as an essential part of National Security is an important step towards waging the war in infospace, the Fifth Dimension of Warfare. The components of Information Warfare may constitute of electronic warfare, psychological operations, Cyber warfare, military deception and Operational security. A holistic approach to operationalising a combination of Psychological Warfare, Cyber Operations and Electronic Warfare, which are the established components of Information Warfare is the need of the hour. There is also an urgent need to integrate the Military, Academic and Civilian components of the nation.*

Keywords: *Hybrid Warfare, Information Warfare, Information Security.*

> *Russian concepts of information warfare have long frustrated the discrete distinctions of cyber, electronic warfare and information operations used within U.S. doctrine. - US Army Association*[1]

In human relations as well as international relations, competition, disputes and conflicts of interests are inevitable. These disputes have often escalated to violence in the past, to gain advantage, change regimes or resolve a conflict. However in the new age of Hybrid Warfare, nations have shifted to use of Information Warfare as an unconventional method to impose their National Will on an adversary with apparent anonymity and without violating international laws on sovereignty of other nations.

India is continuously facing challenges in the Information Warfare space on a regular basis be it concerning the collusive nature of transborder Proxy War and Hybrid Warfare or spread of radicalism and terrorist ideology. These challenges are all manifesting on a daily basis in electronic, print and social media and other means of public diplomacy. While access to the world wide web is supposed to be free and unfettered, it is actually controlled by a few "Haves" and all the other "Have Nots" are vulnerable to compromise of their information.

At the end of the second millennium, divisions in the global community are structured not only by imbalances in trade and technology, levels of poverty and ethno- religious divergence, but also by the degree of access to the information superhighway. As far back as 1995, inthe First Conference on Information Society of the G-7 states, a free-market approach was advocated. It was also mentioned in the conference that "the cyberspace age will widen the chasm between rich and poor, and between leading industrialised nations and the developing world." These words have proved prophetic and the chasm is now so vast that it is getting practically irreversible. The recent arrest of the Chief Financial Officer of Huawei Technologies in Canada is a pointer of the efforts of China to break the monopoly of the Information Superpowers on the one hand, while on the other hand it is indicative of the kind of extreme steps that may be taken to protect this supremacy.

Third World countries, including India, will have to struggle to offset the Information Advantage of the First World, since Proprietary Software that run Information Systems, control over multiple Aps running essential services and massive data gathering giants like Google and Facebook have colonized us in a Neo-Colonial way. The world is only now realizing that the Internet Giants are extremely powerful owing to the Information they possess as also the uncanny capability they have to influence opinions, decisions and outcomes of events. The Cambridge Analytica revelations and several other examples of the use of Information Warfare underline the potency of Information Superiority in the digital age.

[1]Colonel Liam Collins and Professor Aaron Brantly, *A Bear of a Problem: Russian Special Forces Perfecting Their Cyber Capabilities*, Association of the United States Army journal, article dated November 28, 2018, available at https://www.ausa.org/articles/bear-problem-russian-special-forces-perfecting-their-cyber-capabilities

We need to have a holistic understanding of Information Warfare along with a stated and declared policy, strategy and suitable structures to undertake info warfare campaigns in support of our National Interests. Including Information Security as an essential part of National Security is an important step towards waging the war in infospace, the Fifth Dimension of Warfare. Another equally important step is to study Information Warfare as a concept and analyse the components of this new dimension of warfare.

Information Warfare and Information Operations

Information is both the target and the weapon in Information Warfare that has taken the concept of information security into a new dimension. This is a battle that is fought in a virtual domain of infospace which makes it distinct from the physical domains of Land, Sea, Air and Space. One of the first prominent writers on the subject is Edward Waltz, a former Manager for Information Understanding Programs at The Environmental Research Institute of Michigan. In his seminal book published in 1998, he stated that Information Warfare covers three central aspects of conflict at the national level: Information Dominance, Information Protection And Information Attack[2]. There has been considerable evolution in the concepts and doctrines of Information Warfare since then as the ideas he mooted were put into practice.

Information Warfare(IW) as a concept, has been first developed and articulated under US Military doctrine, while it has subsequently been adopted by several nations in different forms. The Indian Army also has had officers in Information Warfare appointments since the early 2000s. As can be seen from the various doctrines and studies published in USA over a period of time, IW extends into the realms of Electronic Warfare, Cyber Warfare and Psychological Operations and these three major components are also a part of the Indian Army's concepts of IW. Cyber Warfare consists of Computer Network Attack, Defence and Exploitation, while Electronic Warfare has the functions of Attack, Protect and Support. Psychological Warfare has always been a part of the warfighting doctrines of all major militaries since World War I when loudspeakers were used across the battle lines to demoralise opposing troops.

In more recent publications of the US Department of Defence, a broader term of **Information Operations** has developed combining the use of technology that was already a part of Information Warfare, but giving added emphasis to the more human-related aspects of information use, including social network analysis, decision analysis, and civilian agencies that can complement the military effort in the Information Domain.

Various definitions exist for Information Warfare, with variations between nations practicing IW and also between definitions in the same country written at different times. One of the definitions being used currently by most writers in India is :-

> "Actions taken during peace, crisis & conflict to achieve info dominance over the adversary by degrading his info & info structures while protecting one's own".

Information Warfare : American Concepts and Components

The term Information Warfare can be traced to one of the first instances of its use by the Office of Net Assessment, USA where in the 1970s, Dr. Rona described the competition between competing control systems in the cybernetics field as "Information Warfare"[3]. Subsequently the US military has used the term **Information Warfare (IW)** for a considerable period before expanding it to include a wider range of activities in **Information Operations(IO)**. Daniel Kuehl explained the relationship between IO, IW and CNA(Computer Network Attack) in his paper published for a US Naval War College Publication in 2002, wherein he states that IW is to be performed primarily by the military in a specific conflict while IO involves the military and civilian agencies. By and large the activities envisaged in IW and IO are the same, with IW being practiced at the Military level in a specific conflict and IO at the National level across the Peace-Confilct – Peace continuum.

Daniel Kuehl, in his writings, has extracted three important definitions from the US doctrinal publications as under :-

- **Information Operations**: Actions taken to affect adversary information and information systems while defending one's own information and information systems.
- **Information Warfare**: Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

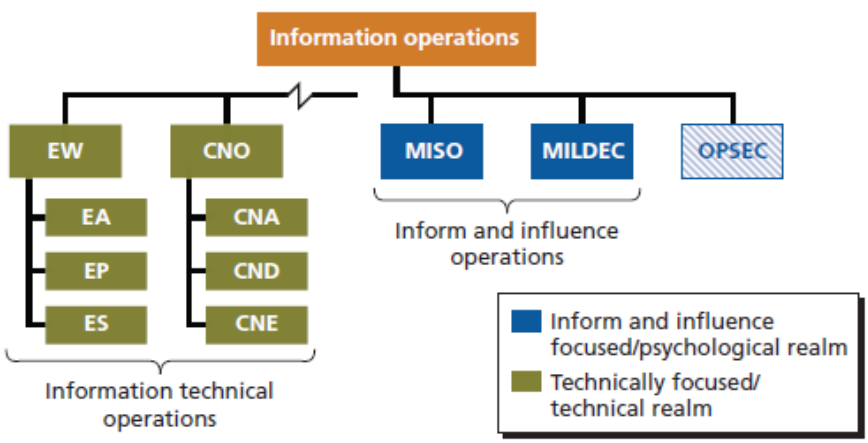
[2]*Edward Waltz, Information Warfare: Principles and Operations, Boston, Artech House, 1998 p.19*

[3]*Daniel T. Kuehl, Information Operations, Information Warfare, and Computer Network Attack : Their Relationship to National Security in the Information Age, US Naval War College Vol 76 publication 2002, p.36*

- **Information Assurance**: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Daniel Kuehl states that IW and IO can be described as the struggle to control and exploit the information environment, a struggle that extends across the conflict spectrum from "peace" to "war" and involves virtually all of the government's agencies and instruments of power[4] Early American publications specify the core capabilities of IW as Electronic Warfare (EW), Computer network operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC). PSYOP has now been renamed in the USA as Military Information Support Operations (MISO) and an elaborate structure of MISO units and organisations have been raised to execute these operations. EW consists of the functions of Electronic Attack (EA), Electronic Protect (EP), Electronic Support (ES), all of which deal with operations in the Electromagnetic Spectrum. CNO consists of Computer Network Attack (CNA) and Computer Network Exploit (CNE) in the field of Cyber Warfare.

A Rand study proposes separation of the functional areas currently defined in the IO definition into two realms: the more technical functional areas of EW and CNO as being related to machine targets and the operations in the psychological realm being related to people as targets. This segregation along with the proposed categorisation of activities pertaining to IO is elucidated below.[5]



This change in USA from IW to IO actually signifies the greater correlation in the American conceptual framework of warfare in the information domain to security related operations. This highlights the greater linkage that America provides between National Security and Information Warfare. Most other countries including India, still use the term Information Warfare which covers the same functions. There are also some variations in the terminology of the various components of IW used in different countries, and also the inclusion of Military Deception and Operational Security are considered to be RELATED FUNCTIONS rather than COMPONENTS of IW.

Military Information Support Operations[6] These are operations planned at the national level to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals in a manner favourable to the originator's objectives. In American parlance these operations are referred to as MISO.

Perception Management. The American Department of Defense (DOD) describes "perception management" as a type of psychological operation[7]. Traditionally, it's supposed to be directed at "foreign audiences," and basically it involves conveying (or denying) information "to influence their emotions, motives, and objective reasoning."Joint Publication 1-02 (Department of Defense Dictionary of Military and Associated Terms - April 2006) defines Perception Management as follows:

[4]Daniel T. Kuehl ,ibid p.37

[5] RAND ibid p. xxi

[6] US joint Chiefs of Staff , Military Information Support Operations, Joint Publication 3-13.2 updated 20 Dec 2011, pp vii , http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf

[7] Greg Guma, The evolution of perception management tactics , June 3, 2005 article in Towards Freedom site https://towardfreedom.org/archives/media/the-evolution-of-perception-management-tactics-0604/

Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, Perception Management combines truth projection, operations security, cover and deception, and psychological operations.

Information Warfare Concepts in other Nations

Russian Information Warfare. Russia has also developed capabilities for Information Warfare which include Computer Network Operations, Electronic Warfare, Psychological Operations, and Deception activities.[8] Russia views information warfare as a soft power tool to be used in both peacetime and wartime. In the Russian construct, Information Warfare is not an activity limited to wartime. It is not even limited to the "initial phase of conflict" before hostilities begin, which includes information preparation of the battle space. Instead, it is an ongoing activity regardless of the state of relations with the opponent; in contrast to other forms and methods of opposition, information confrontation is waged constantly in peacetime[9]. As per the Russian concepts, Information Warfare in the new age conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources)[10]

Synergy of Cognitive and Technical Aspects Instead of cyberspace, Russia refers to "information space," and includes in this space both computer and human information processing, in effect the cognitive dimension as also the cyber dimension. Within information space, Russian thinking includes linking the information-technical and information-psychological dimensions, the two main strands of Information Warfare, depending on the target of action and nature of attack or defence. It is here that there is a conceptual departure from the earlier understanding of Information Warfare which separated Cyber aspects from other Information Operations aspects, and the Russians have made great strides in use of the Information Domain owing to a very focussed approach to using the Cyber and Social Media in close synchronisation with the Cognitive Dimension for Information Dominance. UK has also merged the Cyber and Cognitive aspects into the concept of Information Manoeuvre.

The synergised application of Cognitive and Technical aspects in the Russian concept of operations in "Information Space" are described as under[11] :-

- **Information-Psychological Warfare** which is conducted under conditions of natural competition, i.e. permanently; and affects the personnel of the armed forces and the population of the adversary
- **Information-Technology Warfare** which is conducted during wars and armed conflicts to affect technical systems which receive, collect, process and transmit information

It may be seen that both US and Russian thinking on IW is beginning to connect Psychological Manipulation with use of Technology to jointly operate in the Information Domain for waging Information Warfare. While terminologies vary, the focus on use of various IW means to achieve Information Dominance and influence the outcome of peaceful competition as well as military conflict is evident. A study of Russian actions in Crimea has reinforced this synergy between Electronic Communication and Psychological Messaging. One study propounds that future Russian military adventures may include a far higher and frequent level of coordinated EW and Psyops. Much as conventional military communications are the vector by which orders and plans are transferred into action, civilian telecommunications are the vectors by which Psyops are conveyed[12]. The Russian concepts, strategies and structures reflect this skilful use of Military and Civilian infrastructure and manpower in a synchronised manner to achieve national goals. There is ample evidence of the success of the Russian approach in Ukrane, Crimea, Europe and America, so much so that American

[8]Ajir, Shelby Haas, & Bethany Vailliant, paper on *Russian Information Warfare & Implications for Deterrence Policy* , University of Nebraska at Omaha, 2017 p. 4 downloaded from https://stratcomds.com/wp-content/uploads/2018/04/UNO-Team-Paper-Russian-Information-Warfare.pdf

[9]Keir Giles, NATO Defense College Monograph, *Handbook of Russian Information Warfare*, DeBooks Italia ,Rome 2016 p. 4 , available at https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf

[10]Keir Giles, ibid, p. 6

[11]Keir Giles, ibid, p. 9

[12]Dr Thomas Withington, Article in Mönch Publishing Group, September 2018, available at https://www.monch.com/mpg/news/land/4117-analysis-bright-sparks.html

Information Warfare practitioners have started focussing a lot of effort to counter Russian IW attacks and also to design IW offensives against Russia.

IW Transformations in the UK – Information Manoeuvre Command

The United Kingdom has recognised the evolution of warfare from Air- Land- Sea Manoeuvre to Information Manoeuvre. They have created an Information Manoeuvre Command that intertwines three domains- Virtual, Physical & Cognitive for decisive advantage. Some of the key points from a presentation by the British speakers during a seminar[13] at Delhi in June 2018 and July 2017 are :-

- ✓ Information is the Lifeblood of the Battlefield
- ✓ Whoever wins in the Infospace wins
- ✓ Info Manoeuvre replaces Air- Land – Sea Manoeuvre

Rather than a Cyber Command they have created an Information Manoeuvre Command, recognising the need to integrate Cyber War with Perception Management and other digital interventions in infospace. This is something akin to the Chinese INEW, but the entire focus is on information dominance rather that segregating Cyber Operations from the actual aim of Information Warfare, that is domination of the Infospace.

Primacy of Information: UK has recognised that Information Warfare is not an isolated strand of warfare, it needs to be interwoven in a manner that the Physical supports the Virtual and vice versa. The Concept of UK Information Manoeuvre Command and its functioning was explained in detail during the seminar by the British speaker as under:-

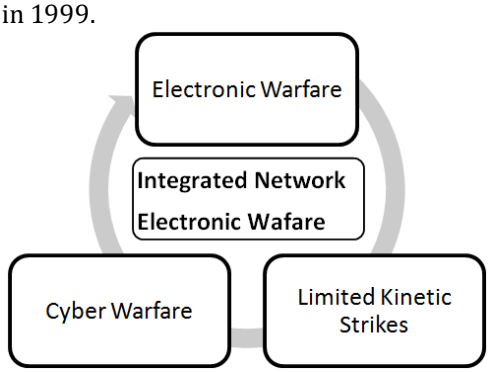
1 Purpose	All of Government Approach
2 Fronts	Home and Away
3 Dimensions	Physical, Virtual and Cognitive
4 Outputs	Understand, Communicate, Persuade and Protect

The Conceptual Construct of Cyberspace Operations in UK

It was seen that UK has no apprehensions in stating their Cyber Offensive capabilities in the international arena. On the other hand it is seen in our writings that we do not wish to disclose Cyber Offensive operations even in internal communication.

Chinese IW Concepts: Integrated Network Electronic Warfare

China has a unique concept of Integrated Network Electronic Warfare which goes far beyond the pure technical domain of Cyber and Electronic Warfare. It envisages the integrated use of Electronic Warfare, Computer Network Warfare and Limited Kinetic Strikes against key command, control, communication, computer nodes to disrupt the enemy's information systems and manipulate the perceptions of the target audience. The description aligns with Unrestricted Warfare as detailed in the book by the same name written by two Chinese Colonels in 1999.



Chinese INEW is an offensive concept which aims to take the initiative and effectively destroy the enemy's electronic information systems, break down his military and civilian communications, paralyse his decision making apparatus and manipulate perceptions of various foreign target audiences to facilitate the attaining of political objectives in the conflict.

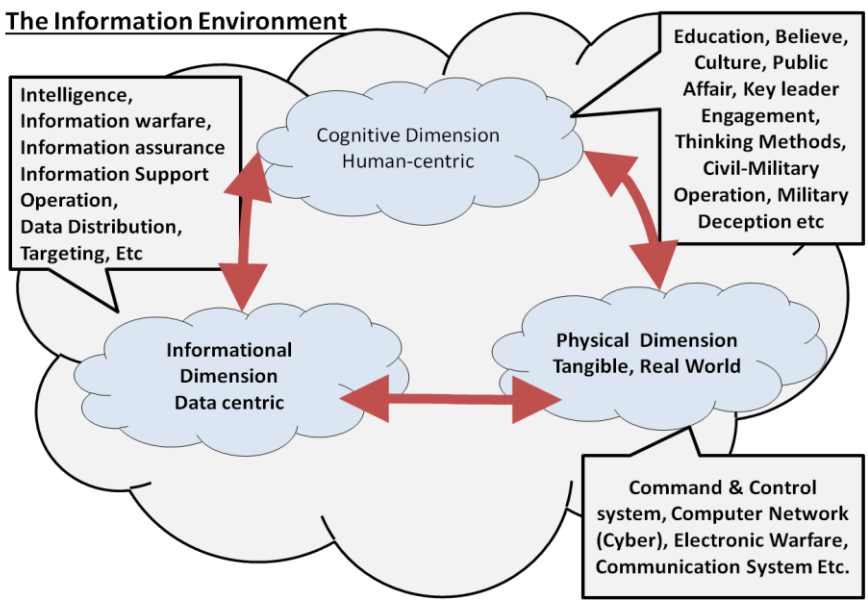
As the PLA has embraced the new operational construct that blends cyberspace operations with kinetic operations, they have created a form of "cyber-kinetic strategic interaction." The goal would be to blind,

[13] Seminar *CybertechIndia 2018* was held by Centre for Joint Warfare Studies, India in June 2018, attended by the author and reported in an article at http://www.defstrat.com/cyberspace-issues

disrupt or deceive adversary C4ISR systems while almost simultaneously deploying its formidable conventional strike, ballistic missile, and maritime power projection forces. The PLA envisions this operational concept as "integrated network electronic warfare," described as the "coordinated use of cyber operations, electronic warfare, space control, and kinetic strikes designed to create 'blind spots' in an adversary's C4ISR systems."[14]

The Western proponents of the technology focussed ideas of NETWORK CENTRIC WARFARE or NCW had broadly separated IW into the civil and military realms with only electronic and cyber warfare being assigned to the armed forces. Psychological manipulation was considered best to be carried out by a mix of military and civilian practitioners while kinetic strikes were thought to be a pure Force-on-Force activity. On the contrary, the Chinese INEW with its comprehensive approach advocates that all activities whether non- contact or kinetic, for disruption of adversary civilian networks, manipulation of public perception, and computer network attacks are also part of the military realm. However recent developments in the Western Nations point towards a closer conceptual integration between electronic and cyber warfare with psychological warfare and kinetic attacks.

It is essential to understand the correlation between the Information, Cognitive and Physical Dimensions that are closely synchronised in an effective Information Warfare campaign and all these three elements are an integral part of the Information Environment.



Elements of the Information Domain

As we can see from the above studies, Information Warfare is fought in the Information Environment that transcends Informational, Cognitive and Physical dimensions of both adversarial parties. Various studies and documents of military and non- military nature have made it clear that the new Hybrid War will be fought in a primarily Information Environment as described in the figure above. Recognition of these elements of the future wars, formulation of strategies and structures, as also establishing technological and Human Resource capabilities to wage this new warfare will be critical to warding off future threats to National Security. It is also essential to integrate efforts in these three related functions to achieve a common goal and our structures have to integrate suitably for this synchronisation. While the training and nurturing of talent in each domain may need to be separate at the practitioners levels, their integration needs to be done at an appropriate level where all elements are jointly applied to achieve info dominance, propagation of own narratives, and victory in the Info Battle.

Relationship Between PM and Psy Ops

The Integrated Defence Staff HQ of the Indian Armed Forces has published a doctrine that addresses Perception Management and Psychological Operations. The Indian Army has an existing doctrine on

[14]Maj Gen PK Mallick, VSM (Retd), *PLA in Electromagnetic Domain*, October 2017 Journal of India Foundation available at http://www.indiafoundation.in/pla-in-electromagnetic-domain/

Information Warfare, which also addresses Psychological operations. Perception Management and Psychological Operations address common issues, the latter being a precursor of the former[15]. The Joint Doctrine on PM and Psy Ops was released on 16 June 2010 to develop greater synergy among the three services— Army, Navy and Air Force and enhance joint fighting capabilities[16]. While this doctrine is likely to be made public soon as called for by the CIC[17] we are able to correlate from available information and writings that PM is a component of Psy Ops while some writers state that Psy Ops is a component of PM. To achieve the aim of Psy Ops, the technique used includes, but is not limited to, PM, as Public Information, Public Diplomacy and Military Psy Ops products are also required to execute Psy Ops at the National level. PM is one of the mediums used to achieve the objectives of Psy Ops.

Components of Information Warfare

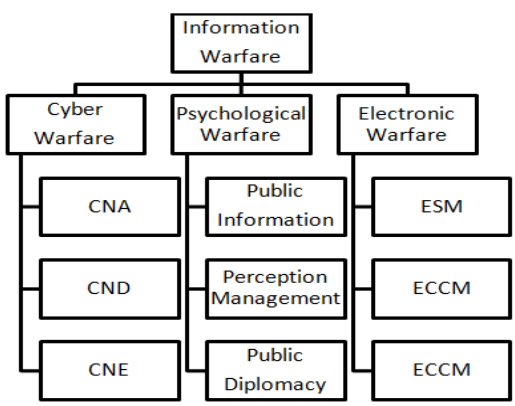
As has been analysed above, different nations use different terminology in the field of IW. After due study of these terms and processes, as also the current writing on the subject by Indian experts, we may propose the following components to be taken to comprise Information Wafare as pertaining to India's National Security.

Electronic Warfare . EW consists of Electronic Support Measures, Electronic Counter Measures and Electronic Counter Counter M easures.

Psychological Operations. Psychological Operations include Perception Management, Public Information and Public Diplomacy

Cyber Warfare. Operations in Cyberspace include Computer Network Defence, Expoit and Attack.

Military Deception and Operational Security. While these functions are often listed as components of IW in India as well as in USA, however both functions both require theuse of all the three main components of IW listed above and are related to standard procedures undertaken by all militaries since time immemorial. Moreover these two elements primarily relate to very specific military activities which are also linked to the three main components of IW. It is therefore felt that it would be prudent to exclude them from the components of IW.



Components of Information Warfare

The components of Information Warfare in the diagram are recommended to be adopted for further progress in this field, Having arrived at a conclusion about the components of Information Warfare that will be suitable for India's pursuit of Information Security in the evolving security environment we need to analyse the strategy and structures that will be needed for India's National Security in the Info Age.

A holistic approach to operationalising a combination of Psychological Warfare, Cyber Operations and Electronic Warfare, which are the established components of Information Warfareis the need of the hour. In fact, continuing to separate Cyber Security aspects from Psychological Warfare that is riding on social media and electronic media 24 X 7 in the interconnected world is a sure recipe for disaster for any nation,

[15] SK Chatterji, IDSA website https://idsa.in/askanexpert/Whatisthenewperceptionmanagementdoctrineforarmy

[16] SrimoyeePanditArticle in Jagran Josh, Doctrine on Perception Management Launched, 11 Oct 2010, https://www.jagranjosh.com/current-affairs/doctrines-on-perception-management-airland-operations-launched-1286792184-1

[17] Economic Times 05 Oct 2018. CIC Asks defence ministry to disclose 2 Joint operational doctrines available at https://economictimes.indiatimes.com/news/politics-and-nation/cic-asks-defence-ministry-to-disclose-2-joint-operational-doctrines/articleshow/66079637.cms

especially now that most nations like China and Russia have adopted a synchronised structure to wage Information Warfare.

The conceptual underpinning of Information Warfare needs to be a synchronisation between the Information-Technical and Information-Psychological Dimensions of Information Warfare to influence the Cognitive Dimension. There is also an urgent need to integrate the Military, Academic and Civilian components of the nation. Separation of all these elements is likely to result in a fragmented development of concepts, strategies and doctrines as also a sub- optimal execution of Information Warfare which will be detrimental to the future of the nation. With a number of adversaries or competitors adopting a more integrated approach to Information Warfare, those nations which choose to ignore this critical aspect are bound to face losses and defeats in peace, conflict and war, and will remain unable to pursue their National Interests.