INFORMATION WARFARE: ELEMENTS AND FORMS

RAKESH ARORA

Information has always been important to human beings in all their endeavours. Throughout history, individuals, groups and nations have strived to expand the information available to them and restrict that available to the adversary or competitor. Knowledge and the information explosion resulting from the industrial revolution and the requirement of its dissemination to the people at large gave rise to what was termed 'information overload'. Research in the fields of Information and Communication Technology (ICT) enabled the storage of large amounts of information, fast processing, and retrieval. These developments in the field of ICT brought about a paradigm change in the human capacity to handle information. Amongst other things, ICT brought about a quantum leap in efficiency in the core sectors of the economy like industry, communications, transportation, energy, etc. On the flip side, this increased efficiency made these sectors heavily dependent on the use of information and ICT.

This dependence, in turn, increased the vulnerability of the core sectors, and the society at large, to disruption in the flow of information. Information as an entity and its flow are more vulnerable and need to be protected like other national assets. Long recognised as one of the elements of national power, along with diplomacy, military and economic power, information

[*] Wing Commander **Rakesh Arora** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

Gaining and exploiting the relevant information is termed 'Information- in-War' and has been utilised extensively since ancient times.

has assumed greater weightage in the present society. This phenomenal rise in the importance of information in the late 20th century led military thinkers to treat 'information' both as a weapon and a target in modern conflicts.

Information has also been used in wars since historical times to gain decisive advantage over the adversary. Activities of intelligence gathering, surveillance and reconnaissance, essentially a survey of the enemy locations, therefore, have been important preoccupations of military planners and commanders. This aspect of *gaining and exploiting* the relevant information is termed 'Information- in- War' and has been utilised extensively since ancient times. The ongoing information revolution has catapulted *information per se* and *its flow* to such a position of prominence that these have become lucrative targets of attack in a conflict. Information Warfare (IW) deals with the aspects of attacking and defending information and the process/means of its dissemination. As the effect of disruption or denial of critical information is far greater than that obtained through physical attacks on traditional targets of war (viz. population centres, critical industry or roads and bridges), IW has become a favourite topic in the study of Effects-Based Operations (EBO).

This paper would endeavour to explore various aspects of information and its relevance as an instrument of waging war and a vulnerable target in conflicts. Evolution of various forms of IW will then be traced. The concept of IW as defined by the USA, Russia and China will then be compared and a suggested framework will be proposed for an Indian definition of information warfare.

WHAT IS INFORMATION?

Information, though it sounds trivial, is central to the concept of IW. Information in the simplest terms is generated by processing compiled data into a usable form. This data, however, is not there to be collected. The human mind experiences 'phenomena' and 'sensations' which form data. It is this data that, when compiled and processed through prior knowledge, becomes ‘information’.

Information, therefore, derives from the environment and the events occurring in it. It is also dependent upon observation and interpretation. This means that two persons can derive different information from the same environment, observing the same phenomena. In order to arrive at coherent information, a set of rules should be defined for observations and their interpretation. Defining rules becomes even more important when machines or computers are used to analyse the observed data. In the systems theory, the term information is used to denote data that are processed to be useful i.e. to be able to answer questions like “who”, “what”, “where”, “when”, “how much”, etc. US Army Field Manual 100-6 defines information as “data collected from the environment and processed into a usable form.”

Knowledge is information that has been tested and accepted as factual:

- Through cognition — the mental process that receives or develops unverified information (beliefs).
- Through assessment or testing to prove the information.
- By acceptance of the information as factual.

Information Functions

The activities of information acquisition, storage, processing, modification and, finally, dissemination are termed information functions. Interestingly these information functions are applicable to industrial enterprises as much as these are to the post industrial age ‘knowledge enterprises’. For example, when a pneumatic pump is set to cut off at a predetermined maximum pressure while filling an automobile tyre, it incorporates an information function regardless of the fact that the mechanism of cutting off is mechanical and not electronic. Similarly, an automatic answering machine attached to a telephone performs an information function when it announces the absence of a person after a given number of rings and records a message from the caller. Both these examples demonstrate the independence of information functions from the type of application and from the technology employed.

Extending the concept to military applications, activities of surveillance, reconnaissance, navigation and intelligence gathering have been conducted by militaries since the beginning of conflict. Since all these actions involve acquisition, processing and dissemination of information, they can be termed military information functions. Thus, information functions that enhance and support the employment of military forces may be termed military information functions.

Availability of quality information with the least possible time lag has always been high on the priorities of military commanders.

INFORMATION-IN-WAR AND INFORMATION WARFARE

Availability of quality information with the least possible time lag has always been high on the priorities of military commanders. The concept of (use of) Information-in-War refers to the activities of acquisition and exploitation of information about the enemy, his strengths, weaknesses, motivations, force structure, morale, strategies, tactics, etc. Acquisition of information in war, therefore, always precedes hostilities, and, in fact, can actually prevent hostilities. Examples of exploitation of superior information in war are available since the medieval period wherein smaller armies of local chieftains, armed with better knowledge of local terrain, routes, obstructions, etc., won many tactical battles against larger forces. Guerrilla warfare also demonstrated the tactical advantage brought in by the element of surprise and knowledge of local terrain. The Marathas of southwestern India under Chhatrapati Shivaji combined these tactics of guerrilla attacks with skillful diplomacy to great advantage against the vastly superior armies of Bijapur and later those of Mughal Emperor Aurangzeb. The advent of ICT in the late 20th century provided commanders with a potent tool for faster gathering and analysis of information relating to intelligence, surveillance, reconnaissance and actual combat operations. On the other hand, increased use of computers and communication systems has also added increased vulnerability to the activities of information gathering and processing.

Information Warfare (IW), on the other hand, targets the information and information exploitation mechanism of the adversary. It also aims at denying, delaying disrupting or otherwise manipulating the quality and quantity of information available to the adversary and corrupting his decision-making systems, including the human mind, while protecting own systems against such actions from the adversary. IW, therefore, views information itself as a separate realm, a potent weapon and a high value target, which can separate 'the head from the body'. In the absence of reliable decision-making systems, and fed with inaccurate and delayed information, even the best brains would make incorrect and arbitrary decisions. Psychological warfare and military deception, the earliest known forms of IW, aim at corrupting the decision-making capability of the human mind by feeding corrupted and inaccurate information to the adversary. Thirteenth century Mongol King Genghis Khan, who built the largest contiguous empire in known history, practised the art of psychological warfare when he asked each of his soldiers to light three torches in the night to give an impression of invincible numbers.

Since information is handled by automated electronic and computer systems, an attack on information can be conducted by attacking/ destroying or otherwise manipulating these systems.

Since information is handled by automated electronic and computer systems, an attack on information can be conducted by attacking/ destroying or otherwise manipulating these systems to disrupt, deny or corrupt the processing and flow of information. Examples of attacks on information handling systems are the bombing of the server or exchange room of a military installation (hard kill) or corrupting its software through hacking (soft kill). Similarly, defending the switching facility (through military means) is an example of IW, as is using intrusion prevention and anti-virus programmes to protect the facility's software.[1]

[1] Ronald Fogleman and Shiela E Widnall, "Cornerstones of Information Warfare", http://www.c4i.org/cornerstones.html, accessed on May 26, 2011.

TERMINOLOGY

Information Warfare (IW)/ Information Operations (IO) and associated issues have been defined and redefined many times in the last two decades by many countries. Although the USA was the first to articulate and publish definitions and doctrines on IW, Russia and China have been quick to follow with their own concepts of IW. Further, as each country colours the concepts according to its unique cultural and geo-political environments, how countries define IW/ IO and utilise the concept in their strategies and doctrines gives an insight into their strategic thought and culture, which could then be utilised in developing India's definition of IW.

For the purpose of this study, definitions of information operations, information warfare, information environment and a few other related aspects/elements as given in the US Department of Defence (DoD) Joint Publication 3-13 (JP 3-13, Information Operations, released on February 13, 2006) will be considered as the basic reference and other definitions will be compared with these for their relative points of agreement and departure. Definitions of a few other terms as per JP 3-13 are placed at the appendix to this paper for ready reference.

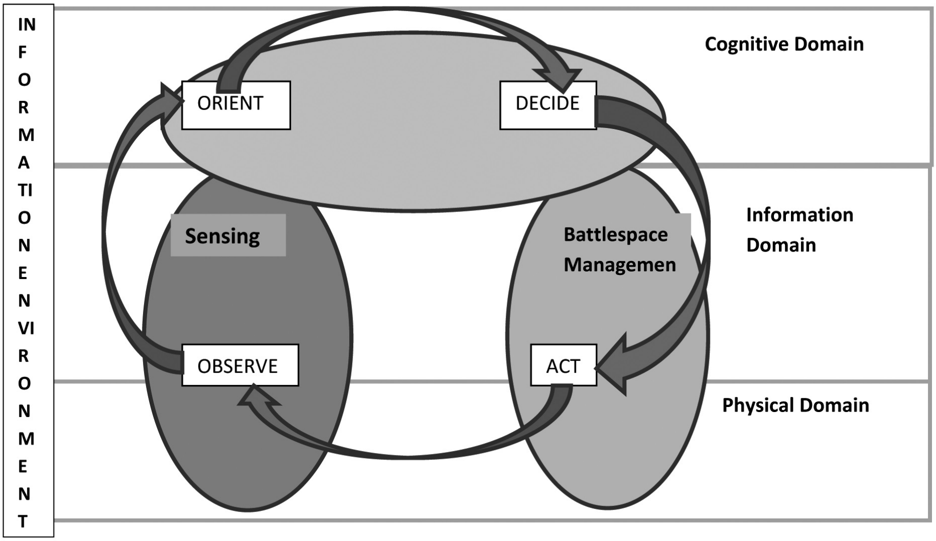
Information operations, according to JP 3-13, are described as the integrated employment of Electronic Warfare (**EW**), Computer Network Operations (**CNO**), Psychological Operations (**PSYOP**), Military Deception (**MILDEC**), and Operations Security (**OPSEC**), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own. There are five supporting capabilities: Information Assurance (IA), Physical Security, Physical Attack, Counter-Intelligence (CI), and Combat Camera (COMCAM), and three related capabilities: Public Affairs (PA), Civil-Military Operations (CMO), and Defence Support to Public Diplomacy (DSPD).[2]

According to the US Air Force (AFDD 2-5 of the year 2005), IO is, "Integrated employment of the capabilities of **influence operations,**

[2] Chapter II, *Core, Supporting and Related Information Operations Capabilities*, US Air Force Doctrine Document 2-5, January 11, 2005, pp. II-1.

electronic warfare operations, and network warfare operations, in concert with specified Integrated Control Enablers (ICE, to gather and exploit activities, earlier termed Information-in-War) to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own." It is pertinent to note that in this definition, capabilities of PSYOP, MILDEC and OPSEC have been included in influence operations and CNO has been expanded and renamed as network warfare operations.

The information environment is the aggregate of individuals, organisation and systems that collect process or disseminate information. As the information is acquired from the physical domain through sensors in the information domain, taken to the cognitive domain housing decision-making systems and the human (commanders') brain, the information environment includes all these domains. The decision, once arrived at, needs to be disseminated again through the information domain to enable actions in the physical domain. Superimposing these activities of the Observe, Orient, Decide, Act (OODA) loop on the physical information and cognitive domains, one gets a picture as shown below:



Martin Libicki lists seven forms of information warfare which according to him were identified by one or another expert as a defining example of such warfare.

All three capabilities of IO viz. influence operations, electronic warfare operations and network warfare operations operate in three different domains of the information environment. Electronic warfare operations work in the physical and information domains and their effect is felt in the cognitive domain as well. Network warfare operations focus on the information domain and aim at influencing sensors, hardware/software and humans. Influence operations focus on affecting the perceptions and behaviour of leaders, groups, and even entire populations. The means applied can be physical, informational or both.[3]

Advances in ICT provide opportunities to societies and militaries to transfer and process information at faster speed in the information domain. At the same time, it enables an adversary to affect that information. Essentially, the information domain continues to expand with the application of new technologies. The processes of observing, operating, deciding and acting can be utilised for attacking all types of targets, whether military, political leadership, command and control or even critical industries.

EVOLUTION OF US CONCEPT OF INFORMATION WARFARE

Early writings on the subject of IW in the US linked it to the Revolution in Military Affairs (RMA) and the evolution of the Industrial Society into the Information Society. Accordingly, information was thought of as a '*new tool for waging war*' across its spectrum, from the crisis situation right up to the restoration of peace. Thomas Rona, one of the early proponents of information warfare, defined it as, "The strategic, operational, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives."[4]

[3] Ibid.

[4] Thomas Rona, quoted in Martin C. Libicki, *What is Information Warfare (*Institute for National Strategic Studies, NDU, August 1995), p. 4.

Martin Libicki lists seven forms of information warfare which according to him were identified by one or another expert as a defining example of such warfare. These are Command and Control Warfare (C2W), Intelligence-Based Warfare (IBW), Electronic Warfare (EW), Psychological Warfare (PSYWAR), Hacker Warfare, Economic Information Warfare (EIW) and Cyber Warfare.[5]

Libicki further brings out the complex structure and problems in assigning its various forms to various directorates in the Pentagon as, "C2W was assigned to the operations directorate within the Joint Chief of Staff (J3), command and control systems for security was the province of the C4 directorate. Forms of IW that involved establishing systems of battlefield intelligence, reconnaissance and surveillance fell under the intelligence directorate (J2). Finally (future) information architecture would be associated with long-term planning in J5."[6]

Perhaps the first official definition of information warfare was given by Gen Ronald Fogelman, then USAF Chief of Staff, and Shiela E. Widnall, then Secretary of the Air Force, in their document *Cornerstones of Information Warfare* in the year 1997, "Information Warfare is any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions."[7]

The US Air Force Doctrine on Information Operations (AFDD 2-5 dated August 05, 1998) defined information warfare as, "Information warfare is information operations conducted to defend one's own information and information systems or attacking and affecting an adversary's information and information systems…Information warfare involves such diverse activities as psychological operations, military deception, electronic warfare, both physical and information ('cyber') attack, and a variety of defensive activities and programs. It is important to stress that information warfare is a *construct* that operates across the spectrum, from peace to war, to allow the effective execution of Air Force responsibilities."[8]

[5] Ibid.

[6] Ibid., p. 5.

[7] Fogleman and Widnall, n. 1.

[8] Foreword to the Air Force Doctrine Document 2-5, dated August 05, 1998, accessed online at http://www.dtic.mil/doctrine/jel/services_pubs/afd2_5.pdf, on May 27, 2011.

The subsequent doctrine on Information Operations (AFFD 2-5 dated January 11, 2005), further elaborated the concept of 'Information- in- War', which was now renamed as Integrated Control Enablers (ICE) — *to gain and exploit capabilities that are critical to all air, space and information operations.* The concept of Information Operations (IO) had by now also evolved to "*…gain a superior information advantage (information superiority)*". The activities of psychological operations, military deception, etc. defined as parts of information warfare in the earlier doctrine have been regrouped into capabilities like influence operations, electronic warfare operations and network warfare operations according to the effects achieved at the operational level. An interactive relationship between ICE (gain and exploit) and IO (defend/attack) capabilities has also been emphasised. The doctrine also recognises the need for mutual support between military operations and IO as it says, "(The) doctrine recognizes a fully integrated spectrum of military operations. Information operations, like air and space operations, ought to be effects-based. Both air and space operations can support and leverage information operations, just as information operations can support and leverage both air and space operations."[9]

However, the current definition of IO offered by the US DoD Joint Publication (JP 3-13 dated February 13, 2006), lists information superiority as its key goal. According to the doctrine, "IO are described as the integrated employment of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC) and Operations Security (OPSEC) in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own."

The evolution of the American concept of IW/ IO can be seen from the subtle differences in the successive definitions in the above documents.

While the first definition, given by the then USAF Chief of Staff and then Secretary of the Air Force in 1997, talked about denying or destroying the enemy's information and safeguarding our own, the second listed in the IO doctrine of 1998 goes on to list various forms of IW viz. psychological

[9] Ibid.

operations, military deception, electronic warfare and physical and information attack. It also stressed that infowar operates across the spectrum from peace to war.

Two subsequent definitions have omitted the term information warfare in favour of a broader concept of IO instead. The key goal of IO had now been identified as gaining superior information advantage or information superiority.

The key goal of IO had now been identified as gaining superior information advantage or information superiority.

AFDD 2-5 of the year 2005 also groups activities of psychological warfare, military deception and electronic warfare, etc. into influence operations, EW operations and network warfare operations, depending upon the effects generated at the operational level. Interdependence of Information-in-War and IO has also been emphasised as both are considered mutually supportive. This AFDD also considers military operations and IO as mutually supportive in that both can leverage each other for an effects-based approach.

RUSSIAN CONCEPT OF INFORMATION WARFARE

Economically (and militarily), Russia is not even a shadow of what the USSR was before its collapse in 1991. The Russian economy, society and state as a whole are in a process of transition from a Communist to a market driven democratic system. This transition, coupled with free exchange of information, makes the common citizen vulnerable to manipulation by glib marketing campaigns and exploitation by promises of quick economic prosperity. Today's Russian security experts believe that no other issue is more fraught with uncertainty than the current and future information environment. The apparent reasons for this thinking are many, some of which are:

- Citizens and decision-makers are now faced with a deluge of information from various religious, political and ideological sources, access to which was earlier forbidden. This, when the majority of the people are not clear about the ideological and political moorings of the state, could be a source of destabilisation.

The Russians attach great importance to the subject of information operations/ warfare, next only to that of nuclear weapons.

- Information, according to the Russians, has developed into an important strategic resource. Information technologies have influenced business practices, financial markets and even the capabilities of military weapons. Countries that enjoy information superiority may be more inclined to employ military force as they could now achieve military objectives without a significant loss of life. The Russians believe that the North Atlantic Treaty Organisation (NATO) intervention in Bosnia and Kosovo was successful because of their information superiority. This strategic importance and reach of information into all walks of life can allow some countries to dominate some others in the military-political realm.
- Finally, there are few legal constraints, even at the international level, which could deter information intervention or even attacks. This, in a way, encourages rogue elements and nations to attack other nations' critical infrastructure sectors that depend upon ICT, like the financial system, electrical distribution and even civil aviation and rail network, etc.

Because of all these reasons, the Russians attach great importance to the subject of information operations/warfare, next only to that of nuclear weapons. As information influences the economic, social, political and other components of national power, the Russians believe that information warfare is to be conducted during both peace-time and war-time. During peace, the term used in the Russian lexicon is the information security of society and the government in the psychological, scientific, cultural, and information production spheres. In its war-time usage, it refers to the attainment of superiority in the use of information protection and suppression systems, to include command and control, EW, and reconnaissance.

Adm Vladimir Pirumov (Retd), is perhaps, the most authoritative person to define the term so far. He was an instructor of electronic warfare and later was the Scientific Adviser to the President of Russia. He defines information warfare as follows.[10]

> "Information warfare" is a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemy's information resource, and also of protecting one's own information resource, in order to achieve assigned goals. An information resource is understood to be information which is gathered and stored during the development of science, practical human activity and the operation of special organisations or devices for the collection, processing and presentation of information saved magnetically or in any other form which assures its delivery in time and space to its consumers in order to solve scientific, manufacturing or management tasks.

His definition implies that information warfare is an activity that can be carried on in peace-time as well as war-time. For strict war-time scenarios, Pirumov offered a definition of information warfare in operations that aimed at gaining an information advantage which reads:[11]

> "Information warfare in operations (combat actions)" is the aggregate of all the coordinated measures and actions of troops conducted according to a single plan in order to gain or maintain an information advantage over the enemy during the preparation or conduct of operations. An "information advantage" assumes that one's own troop and weapon command and control components are informed to a greater degree than are those of the enemy, that they possess more complete, detailed, accurate and timely information than does the enemy, and that the condition and capabilities of one's own command and control system make it possible to actualise this advantage in combat actions of troops (forces).

[10] Timothy L. Thomas, "The Russian View of Information War," in Stephen J. Cimbala, ed., *The Russian Armed Forces at the Dawn of Millennium* (Chase Side, London: Frank Cass, 2011). Accessed online at http://www.csl.army.mil/usacsl/publications/RW.pdf on June 11, 2011.

[11] Ibid.

Military Definitions

Definitions provided by the Russian General Staff Academy treat IW in a psychological-technical and operational-strategic sense. The first applies more to the peace-time and the latter to the war-time use.

The first states,

> Information warfare is a way of resolving a conflict between two opposing sides. The goal for one side is to gain and hold an information advantage over the other. This is achieved by exerting a specific information-psychological and information-technical influence on a nation's decision-making system, on the nation's population and on its information resource structures as well as by defeating the enemy's (command and) control system and his information resource structures with the help of additional means such as nuclear assets, weapons and electronic assets.

And the operational-strategic version defined information war as:

> Within the framework of the execution of the operational strategic missions of offensive and defensive troop units, information warfare consists of the specially planned and coordinated-integrated actions of the forces and assets of intelligence and early warning, command and control, communications, deception and electronic warfare, whose purpose is to guarantee the achievement of the goals of operation (of its combat actions).[12]

However, there are many other components of IW that Russian published material, in both the military and civilian domains, addresses. These components offer an understanding far beyond what is included in the definitions above. Some of the topics covered in these writings are:[13]

Role of Federal Agency for Government Communications and Information (FAPSI): Since February 19, 1993, FAPSI has been entrusted with ensuring information security for government communication

[12] Ibid., p. 99.

[13] Adapted from Timothy L. Thomas, "Russian Views on Information Based Warfare," *US Air Power Journal*, Special Edition 1996, pp. 26-33.

and information. Four specific matters that have been assigned to FAPSI's jurisdiction are: special communications, including government communications, the cryptographic and engineering-technical security of encrypted communications, intelligence gathering activities in special communications field, and, finally, provision of special information to higher bodies of authority. In this regard, FAPSI fulfills many of the missions assigned to the National Security Agency in the USA. It has also been charged with fighting domestic criminals and hackers, foreign special services and 'information weapons'. According to Russian terminology, 'information weapons' are meant for gaining unsanctioned access to information and putting electronic management systems out of commission.

Computer Virus Warfare: The Russian military has been studying virus or software warfare as one of the most important aspects of future warfare. Virus warfare presents special problems at the strategic level as its use bears an impersonal imprint, is easily disguised as banal hooliganism or can hide itself as measures to protect the copyright and commercial interests of the firms for their own software. If virus warfare is successful, there may not exist a need to decide matters through violence. One Russian officer wrote, "There is no need to declare war against one's enemies and to actually unleash more or less large military operations using traditional means of armed struggle. This makes plans for hidden war considerably more workable and erodes the boundaries of organized violence, which is becoming more acceptable."

Information Component of Combat Potential: The increasing importance of information in command and control, and information support systems in the accomplishment of combat missions became amply clear to the Russians who observed war with great interest. An assessment by Russian observers credited US victory as coming from overwhelming superiority in logistics and in combat information support systems (C3ISR systems). Perhaps for the first time in recent history, the side with preponderance of weapon systems did not win. In the view of Adm V. Pirumov, "Information support predetermined the development of a new generation of reconnaissance equipment that led to more precise target location. Computer aided troop and weapon control stations were also made possible by applying information support technology." Pirumov estimated that the use of information technology increased the combat capability of the multinational forces by a degree of two. He also added, "All this makes possible the conclusion that the priority and weight of the contribution of information support to combat effectiveness in developed countries determined the dominant role of the electronic-fire concept of conducting warfare."

Information Accumulation, Processing and Integration: A Russian analyst, V. N. Medvedev, defined the dissemination of information in the armed forces as, "The process of the creation, broad-scale incorporation and application in various fields of activity of the armed forces under any conditions, of methods, systems, and means of obtaining gathering processing, storing and using information." This process is the key to informed decision-making. Fast reacting processors are mandatory to reduce the time required to decide and act. Therefore, timely gathering and utilisation of information is of extreme importance. Information accumulation, processing and adaptation are now as important, especially in the areas of reconnaissance and EW systems. Integration of such information obtained (and accumulated) to the command and control systems is critical to what Russians call '*combat system theory*'. The goal is to link this information to all the systems through a secure and stable data communication link, creating a synergy of effort where the overall effect is greater than the sum of the parts.

Perception Management: Disinformation is an old Russian technique of deception, often targeting specific people, and social groups. The purpose is to influence the consciousness and thinking of a person or a target group or even a nation. The erstwhile Soviet Union carried out disinformation campaigns through a well-oiled propaganda machine. One of their methods of getting people to do what they wanted them to do was through reflexive control. Reflexive control creates a pattern or provides partial information that causes an enemy to react in a pre-determined manner without him realising that he is being manipulated.

Russian Information Warfare Doctrine 2000: In September 2000, Russia published a very specific and important information-related document, the Information Security Doctrine of the Russian Federation. Signed by President Vladimir Putin, Russia's Information Security Doctrine presents the purposes, objectives, principles, and basic directions of Russia's information security. It defines information security as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." The doctrine declares that the "implementation of the guarantees of the constitutional rights and liberties of man and citizen concerning activity in the information sphere is the most important objective of the state in the field of information security." Some of the main points of the doctrine are:[14]

- First, the document discusses the national interests of the Russian Federation in the information sphere, including the protection of information resources from unsanctioned access.
- Second, the document examines the types of threats to Russia's information security. These include constitutional rights that protect one's spiritual life, information support for state policy, the development of the information industry, and the security of information.
- Third, the document identifies external and internal sources of threats to Russia's information security.
- Fourth, it outlines the state of information security in the Russian Federation and the objectives supporting it, discussing tension between the need for free exchange of information and the need for restrictions on dissemination of some information.
- Fifth, general methods of information security in the Russian Federation—legal, organisational-technical, and economic—are outlined.
- Sixth, the document discusses several features of information security: economics, domestic policy, foreign policy, science and technology, spiritual life, information and telecommunication systems, defence, law enforcement, and emergency situations.
- Seventh, the goals of international cooperation in the field of information

[14] Timothy L. Thomas, "Russian Information Warfare Theory: Consequences of August 2008," in Stephen J. Blank and Richard Weitz, eds., *Russian Military Today and Tomorrow* (Strategic Studies Institute, US Army War College, July 2010), p. 272.

security are discussed, such as the ban on information weapons and the coordination of law enforcement activities.

- Eighth, the doctrine describes the provisions of state policy regarding information security: guidelines for federal institutions of state power, and balancing the interests of the individual, society and the state in the information sphere.
- Finally, organisational elements of Russia's information security system are described; these include the President, Federation Council of the Federal Assembly, the State Duma of the Federal Assembly, the Government of the Russian Federation, the Security Council, and other federal executive authorities, presidential commissions, judiciary institutions, public associations, and citizens.

Anatoly Streltsov, one of the doctrine's authors, noted that the components of the doctrine provide for the constitutional rights and freedoms of citizens to obtain and use information, while providing for Russia's spiritual renewal, the development of moral values, patriotic and humanistic traditions, and cultural and scientific potential. According to Streltsov, "Currently (in the year 2000), Russia's information security does not fully comply with the needs of society and the state, lacking sufficient legal, organizational, and technical backing."

Information Security in Defence Sphere: According to the Information Warfare Doctrine 2000, information security in the defence sphere involves: (a) information infrastructure of the elements of military command and control, and elements of control of the branches of the armed forces and scientific research institutions of the Ministry of Defence; (b) information resources of enterprises of the defence complex and research institutions; (c) software and hardware of automatic systems of command and control of the forces and weapons, arms, and other military equipment furnished with computerisation facilities; and (d) information resources, infrastructure and communication systems of other forces and military components and elements.

Building Cyber Espionage and Hacking Capabilities: The erstwhile USSR nurtured teams of bright mathematicians, scientists, and computer programmers who could build stable algorithms to control guided weapons, spacecraft and allied systems. Russia has built on that legacy and tried to make up for deficiencies in hardware/microelectronics by building teams of programmers for computerisation in the civil and military arenas. Alongside, teams of patriotic hackers have sprung up, presumably with covert government support, who can attack and access most secretive files hidden behind firewalls and intrusion detection systems. Two news items, one of the Russian development of hacking capabilities and the second of the attack on US military computers would illustrate this point. According to a recent report in the BBC news website (March 11, 2010):[15]

> Mr Kaspersky has made his name battling the world's cyber criminals. The computer security guru says hackers in China and Latin America generate the greatest number of cyber-attacks. The most sophisticated come from his own country. "Russian attacks look more professional. The malware and design is more complicated and more technical," Mr Kaspersky says."I think it's thanks to Russia's technical education. Its graduates are probably the best."

And another report, again from BBC, stated, more than ten years ago (October 08, 1999):[16]

> Hackers, apparently working from Russia, have broken into US Government computer systems for over a year, an FBI official has said. The intruders stole "unclassified but still sensitive" information from US military computers, an FBI deputy assistant Director, Michael Vatis, said. Mr Vatis, also a Director of the National Infrastructure Protection Centre, told a US Senate subcommittee on technology, terrorism and government information that the intrusions appeared to have originated in Russia.
>
> *The Los Angeles Times* reported on Thursday that other officials had said some of the attacks had been traced to servers about 20 miles outside Moscow.

[15] Accessed online at http://news.bbc.co.uk/2/hi/technology/8561910.stm on June 15, 2011.

[16] Accessed online at http://news.bbc.co.uk/2/hi/americas/469006.stm on June 15, 2011.

It said the pattern of attacks suggested that they might involve someone working in an office: they took place on weekdays between 0800 and 1700 hours Moscow time, but not during Russian holidays.

This patriot band was probably responsible for the attack on Estonia in 2007, when its government and public websites were corrupted, and public services delivered through the internet were severely affected for days together. Similarly, during 2008, in the conflict with Georgia, Russian hackers could compromise even the Georgian President's site. One observer wrote on ZDnet.com (during end 2008), "The attacks originally started to take place several weeks before the actual 'intervention' with Georgia President's website coming under DDoS attack from Russian hackers in July, followed by active discussions across the Russian web on whether or not DDoS attacks and website defacements should, in fact, be taking place. The DDoS attacks are so sustained that the Georgian President's website has recently moved to Atlanta (USA)."[17]

China carefully observed the Gulf War wherein American dominance of Iraqi forces was primarily attributed to achievement of information superiority (and air superiority).

CHINESE CONCEPTS OF IW

China carefully observed the Gulf War wherein American dominance of Iraqi forces was primarily attributed to achievement of information superiority (and air superiority). It then started a process of theoretical reflection, analysing Western practices and amalgamating them with classical Chinese military thought, evolving strategies and doctrines to meet with likely future threats. Thus, the Chinese doctrine has evolved from that of people's war to people's war under modern conditions, limited war under high-tech conditions to limited war under informationised conditions. As will be seen, China's strategies, developed since the early Nineties have emphasised:

[17] Blog of Dancho Danchev on August 11, 2008, at http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

- Practical combination of IW and Maoist and Marxist military thought to guide IW issues under military constructs.
- Conducting 'people's war in the IW domain' by finding ways of using inferior equipment to achieve victory over the enemy's superior equipment, by attacking the enemy's weaknesses and vulnerabilities, and exploiting own strengths.
- Use of superior tactics to compensate for inferior technology.[18]

The Chinese way of conducting people's war in the IW domain is by converting millions of civilians, who understand and can use computers, into fighters who can eavesdrop on enemy computers or can disrupt their functioning by sending large amounts of useless data. Since it is difficult to discern where the attack originated from, the targeted country may not be able to apportion blame or retaliate. The internet can also be used for political mobilisation by sending a large number of patriotic e-mail messages and posting material for educating and influencing the masses.[19]

Primarily for use in the military domain as an asymmetric tool, the Chinese have defined IW as the sum of all information capabilities for breaking the enemy's will to resist by attacking the enemy's cognitive understanding and convictions, forcing it to give up all resistance and terminate the war. Xie Guang, the then Vice Minister of Science and Technology and Industry for National Defence, defined IW in December 1999 as: "IW in a military sense means overall use of various types (of) information technologies, equipment and systems, particularly command systems, to shake the determination of the enemy's policy-makers and, at the same time, the use of all the means possible to ensure that that one's own systems are not damaged or disturbed."[20]

Concept of Information Operations: The Chinese view IO as specific operations at the core of IW, in fact, a manifestation of IW on

[18] Wang Pufeng, "Challenge of Information Warfare," in Michael Pillsbury, ed., *Chinese Views of Future Warfare* (Washington DC: National Defense University Press, 1997), at http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinacont.html, accessed on May 26, 2011.

[19] Wei Jincheng, "Information War: A New Form of People's War," in Pillsbury ed., Ibid., Part Four at http://www.au.af.mil/ au/awc/awcgate/ndu/chinview/chinacont.html, accessed on May 26, 2011.

[20] As quoted by Vinod Anand in "Chinese Concepts and Capabilities of Information Warfare," *Strategic Analysis*, October-December 2006, p. 785.

the battlefield. IO can be defensive or offensive and can be conducted across all strategic operational and tactical levels. Various elements of IO, according to the Chinese military authors, are: centralised command and decentralised control, multi-dimension inspection and testing, timely decision-making and integration of military and civil actions. Maj Gen Dai Qingmin, then Director of the People's Liberation Army's (PLA's) General Staff, responsible for IW and IO, defines IO as, "A series of operations with an informationalised environment as the basic battlefield condition, with military information and information systems as the direct operational targets and EW and computer networks as the principal form. Various strategies have been outlined as the Chinese would wish to deploy superior strategies to compensate for inferior equipment and, in the case of IO strategies, may compensate for gaps in information about the enemy".[21]

In keeping with the concept of utilising civilians for IW, China has turned some of the 1.5 million reserve forces into mini-IW regiments. The People's Armed Forces Department (PAFD) has reportedly organised militia/ reserve IW regiments at district levels in many provinces. PAFD, in its exercises in the early 2000, practised the following 10 methods of IO to validate its concepts:[22]

- Planting information mines.
- Conducting information reconnaissance.
- Changing network data.
- Releasing information bombs.
- Dumping information garbage.
- Disseminating propaganda.
- Applying information deception.
- Releasing clone information.
- Organising information defence.
- Establishing network spy stations.

[21] Dai Qingmin, "Innovating and Developing Views on Information Operations," *Beijing Zhongguo*, August 20, 2000, article reviewed by Timothy L. Thomas in "China's Electronic Strategies," *Military Review*, May-June 2001, pp. 72-77.

[22] Ibid., p. 77.

Chinese Integrated Network Electronic Warfare: Half Cousin of Net-Centric Warfare? The National Defence White Paper of 2002 perhaps for the first time used the phrase Integrated Network Electronic Warfare (INEW), wherein it noted that in 2001, many PLA studies and exercises explored the features and patterns of an integrated network-electronic warfare. However, earlier in 2002, in an article in the journal *China Military Science*, Maj Gen Dai Qingmin (head of the 4th Department of the General Staff), explained the concept of INEW, parts of which contradicted the White Paper. For example, he stated that the concept placed more emphasis on active offence, whereas the White Paper emphasised a traditional active defence focus. Dai equated INEW with IO, which the White Paper did not, noting that it "serves as information operations theory with Chinese characteristics." This concept appears to be a half cousin of the popular Pentagon transformation concept of Network-Centric Warfare (NCW). While the American concept makes mention of developing and leveraging information superiority, the INEW objective, according to Dai is about seizing information superiority.[23]

IW, Dai argues, is composed of six forms: operational security, military deception, psychological war, electronic war, computer network war and physical destruction. Barring physical destruction, all these forms have been borrowed from the American definition of IO given in JP 3-13, referred to earlier.

INEW, according to Dai, refers to a series of combat operations that use the integration of electronic warfare and computer network warfare measures to disrupt the normal operation of enemy battlefield information systems while protecting one's information superiority—similar to the US definition of IO. While network war disrupts processing and use of information, EW disrupts acquisition and forwarding of information. The core of computer network warfare is to "disrupt the layers in which information is processed, with the objective of seizing and maintaining control of network space."

The depth to which this concept has been developed can be gauged by the minute details in which each element has been explained by Dai.

[23] Timothy L. Thomas, "Chinese and American Network Warfare," *Joint Force*, Quarterly Issue Thirty Eight, available at http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf, accessed on June 06, 2011.

The main targets of INEW are enemy military, political, economic and social information systems, making the attacks more effective than any traditional combat operation.

According to him, INEW emphasises integrating combat operations by merging command, forces, objectives, and actions. Command integration is its unified planning, organisation, coordination, and control. Forces integration means its use in a complementary manner; and objective integration is its simultaneous use against enemy Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), while action integration is its coordination to produce combined power. Dai listed the characteristics of INEW as its comprehensive nature, its integrated methods and expansive nature (battlespace), and the integrated nature of its effectiveness. Forces integration implies the synthesis of platforms with networks.

The main targets of INEW are enemy military, political, economic and social information systems, making the attacks more effective than any traditional combat operation. INEW also treats the battlefield as a system of systems replete with information-based systems. INEW, therefore, can be thought of as a means of participating in the system-versus-systems battle and attaining information superiority since systems are centres of gravity for a combat force. People and weapons become insignificant when not structured within a system. The concept is quite similar to the American idea of systems integration except that INEW emphasises ideology and philosophy as well. This concept also borrows from two transformations: the first being the change from EW to several forms and methods such as INEW: the second transformation emphasises both offence and defence, with priority on the development of offensive information operations equipment.

COMPARING AMERICAN, RUSSIAN AND CHINESE CONCEPTS

The USA had taken a lead in defining the concept of IO/IW and had influenced the thinking in both Russia and China. All three countries agree on the growing importance of information warfare/ information operations. Although the USA has discontinued use of the term information warfare in their current doctrine, both Russia and China continue to use the term in their writings. Ideas like information superiority, information dominance and command and control warfare find a place in the writings of all three countries. However, there are subtle differences in the definitions and views about IO and related concepts. Some of the salient points of differences are:

Peace-time Application: Russia and China treat IW in a more holistic manner i.e. a set of activities to be pursued during both peace and conflict, than the USA which defines it as an activity to be undertaken during times of crisis. The Chinese define four forms of IW: preemptive strike capability, asymmetric warfare, local war under informationised conditions and people's war.[24, 25]

Technology Vs. Strategy: Many of the Chinese concepts originate from the ancient Chinese *Secret Art of War: 36 Stratagems*, written over 2,500 years ago. Deception is one of the most important concepts that recurs many times in these stratagems e.g. cross the sea under camouflage; kill with a borrowed knife; conceal a dagger in a smile, etc. These stratagems are particularly applicable to IW which covers a long period of time and requires patience and perseverance, a trait that comes naturally to Asians and the Chinese in particular. Chinese military experts have criticised US doctrine for being much too technology driven and overlooking the 'strategy' dimension. Further, American doctrine focusses heavily on the information and information systems of the opponent, while ignoring softer psychological factors. The Chinese have emphasised affecting the opponent's psyche so that he loses the will and capability to fight.

The Russian view of IW also echoes many Chinese concepts in that it maintains that IW is to be conducted in both peace-time and during the build-up towards hostilities, and, in fact, throughout peace and war. Similarly,

[24] Weigung Shen, "A New Form of People's War," *China Military Science*, June 2006, accessed online at http://www.fas.org/irp/world/china/docs/iw_wei.htm, on June 07, 2011.

[25] Zhenxing, Pu Feng, "The Challenge of Information Warfare," *China Military Science*, April 1995, accessed online at http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm, accessed on June 07, 2011.

the peace-time definition of IW includes psychological/informational/ technical influence over the population and information resource structure to bring an end to the conflict situation.

Nuclear Angle: The Russian view differs from both the American and Chinese ones on one major issue, in that it talks of "defeating the enemy's control system and his information resource structures with the help of additional **means such as nuclear assets, weapons** and electronic assets". Neither the USA nor China has mentioned the use of nuclear weapons in its doctrine.

Types of Deception: All three countries consider deception to be a vital part of their IW effort. But there are subtle differences in the depth and the period for which it is to be used. The USA uses the term MILDEC as a core capability of IO in order to mislead the enemy's decision-making systems and the human (commander's) mind. The Russians, on the other hand use the term *maskirovka* (actions executed to deliberately mislead adversary military decision-makers about friendly military capabilities, intentions, and operations, thereby, causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission (definition by thefreedictionary.com) as an independent type of operational support to influence an adversary. This essentially covers the aspects of American MILDEC and OPSEC. It is conducted on a daily basis and on all levels.[26]

In the case of China, deception is the mainstay of the IW/IO concepts. This is the bedrock on which most Chinese strategies are developed.

Time Perspective: This is perhaps, the longest in the Chinese concept of IO, covering several decades as compared to the Russians. The US takes a much shorter time perspective as compared to both China and Russia, as it is related to specific conditions and conflict situations. For a longer term influence on strategic and political levels, Americans use the term s*trategic communication.* However, strategic communication is not included as either an element or a core capability of IO, though they are closely related.

[26] Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Operations,* report published by FOI, Swedish Defence Research Agency. Accessed online at http://www2.foi.se/rapp/foir2970.pdf, on June 07, 2011.

Information Superiority: The US Joint Publication 3-13 defines information superiority (or dominance) as a key enabler of the transformation and evolution of joint command and control. In fact, gaining information superiority is one of the key reasons for conducting information operations (as defined in the USAF doctrine AFDD 2-5). Russian analysts also agree that information superiority will be the main condition of victory in 21st century wars. Russian analyst Bogdanov, in an article in *Military Thought* (April 2001), wrote, "It will be impossible to achieve strategic and operational objectives in future wars without achieving superiority over the adversary in the information sphere."

Chinese literature defines information dominance (*zhixinxiquan*) as the ability to defend one's own information while exploiting and assaulting an opponent's information infrastructure. This information superiority has both technological and strategic components. On the one hand, it requires the capability to interfere with the enemy's ability to obtain, process, transmit and use information to paralyse his entire operational system. Till this point, the definition agrees with the American concept of information dominance. On the other, some Chinese writers have asserted that information superiority is not determined by technological superiority (alone), but by new tactics and the independent creativity of commanders in the field. This once again places much more emphasis on the strategic, personnel and organisation related components of the conflict, an idea that is central to Chinese theory of IW.

DEFINING IW IN THE INDIAN CONTEXT

Even though the Indian armed forces are capable of protecting physical borders, in today's Information Age, movement of ideas, information and knowledge needs to be regulated more than the physical movement of people. The Information Age has thrown up many new challenges that need to be addressed in order to maintain India's position as a leading nation in the world community. In the past, because of our weak patent laws and non-codification of traditional knowledge, many ideas and concepts were lost to the so-called developed nations that were quick to patent them in their own countries. Even the ubiquitous *Neem* has several properties and chemicals that have been patented abroad for their efficacy against various bacteria or as an antibiotic, etc.

Information exfiltration through computer hacking has emerged amongst the most serious threats to information security. Computer network attacks that have been traced to China have targeted India's core sectors, including the Information Technology (IT) sector, in one instance even taking away a lucrative contract from a third country.[27] China has even tried to penetrate various Indian government servers, including those at the National Security Adviser's (NAS') office. One such attempt on December 15, 2010, was admitted by the outgoing NSA Mr M. K. Narayanan when he said, "This was not the first instance to hack into our computers." The attack came in the form of an e-mail with a PDF attachment containing a Trojan which allows a hacker to access a computer remotely and download or delete files.[28]

The first step towards the development of the Indian information warfare concept, therefore, would be to define India's priorities and national interests in the information sphere. The information sphere would include all available information in both civil and military arenas, and accumulated knowledge whether in electronic, print or any other media or traditional knowledge passed down by word of mouth or execution methodologies unique to a particular area or community, etc. It also touches upon the cultural and spiritual lives of the people.

Information security, for the purpose of defining IW can then be thought of as "the state of protection of India's national interests in the information sphere defined by the totality of interests of its citizens, including NRIs, society at large, and the (Indian) nation-state." The importance of information, during both peace and war, necessitates formulation of IW concepts for the entire spectrum of peace, operations other than war, imminence of hostilities and full-fledged

[27] Josy Joseph, "Indian Infotech Sector is Main Focus of Chinese Spying," *DNA India*, December 15, 2008. Accessed at http://www.dnaindia.com/report.asp?newsid=1213993&pageid=0 on June 12, 2011.

[28] Richard Beeston and Jeremy Page, "China Tried to Hack on Our Computers, Says India's Security Chief M. K. Narayanan," accessed at http://www.timesonline.co.uk/tol/news/world/asia/article6991789.ece, accessed on June 12, 2011.

war. Taking the necessity to include both offensive and defensive elements into consideration, a proposed Indian definition of IW could read like:

> Information Warfare is a form of competition between two or more sides, consisting of both nation-states and non-state actors, involving use of special means (informational, cyber, psychological or technical) and methods of influencing the other party's information resources, and also of protecting one's own information/ knowledge resources, in order to achieve assigned goals and broader national interests.

CONCLUSION

An evolving concept like IW/IO needs careful definition of all its elements and forms due to the enormity of issues related with it. Its amorphous nature that encompasses technological and non-technological activities gives it the characteristics of a science as well as an art. Its facets of formulation of rules and procedures for the purpose of intelligence gathering, surveillance and reconnaissance, etc. and their analysis fall within the realm of science. On the other hand, the finer aspects of crafting persuasive or deceiving messages, depending upon who the message is meant for, generating relevant knowledge and managing its flow to the relevant persons and disrupting that of the enemy, keeping the morale of own forces high while demoralising the enemy forces require military strategists to be artists first and military commanders later. Information operations are seen as consisting of conduits of information, cutting across various disciplines like strategy, planning, command and control, IT, communication, personnel planning, etc. Therefore, their importance in the formulation of strategy also needs collective and collaborative effort on the part of the armed forces and civil wings of the government dealing with geo-political considerations.

Developing a relevant and current definition of IW for India is all the more important as this forms the first step towards formulating a policy and doctrine of IW. An IW doctrine, once prepared, would need a review, say every three years to integrate changes in technology and geo-political situations.

Appendix A

SOME BASIC DEFINITIONS OF IO RELATED TERMS AS PER US DOD JP 3-13 (INFORMATION OPERATIONS)

Information Operations Information Operations (IO) are described as the integrated employment of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

Core Capabilities IO consists of five core capabilities which are: PSYOP, MILDEC, OPSEC, EW and CNO. Of the five, PSYOP, OPSEC and MILDEC have played a major part in military operations for many centuries. In this modern age, they have been joined first by EW and most recently by CNO. Together, these five capabilities, used in conjunction with supporting and related capabilities, provide the Joint Force Commander (JFC) with the principal means of influencing an adversary and other Target Audiences (TAs) by enabling the joint forces freedom of operation in the information environment.

Supporting Capabilities Capabilities supporting IO include Information Assurance (IA), Physical Security, Physical Attack, Counter-Intelligence, and Combat Camera. These are either directly or indirectly involved in the information environment and contribute to effective IO. They should be integrated and coordinated with the core capabilities, but can also serve other wider purposes.

Related Capabilities There are three military functions, Public Affairs (PA), Civil Military Operations (CMO), and Defense Support to Public Diplomacy, specified as related capabilities for IO. These capabilities make significant contributions to IO and must always be coordinated and integrated with the core and supporting IO capabilities. However, their primary purpose and the rules under which they operate must not be compromised by IO. This requires additional care and consideration in the planning and conduct of IO. For this reason, the PA and CMO staffs particularly must work in close coordination with the IO planning staff.

Appendix B

ABBREVIATIONS USED

IW	Information Warfare
IO	Information Operations
ICT	Information and Communication Technologies
EBO	Effects-Based Operations
US DoD	United States Department of Defence
JP 3-13	Joint Publication 3-13 (Information Operations)
CNO	Computer Network Operations
EW	Electronic Warfare
PSYOP	Psychological Operations
MILDEC	Military Deception
OPSEC	Operations Security
IA	Information Assurance
CI	Counter-Intelligence
COMCAM	Combat Camera
PA	Public Affairs
CMO	Civil Military Operations
DSPD	Defence Support to Public Diplomacy
USAF	United States Air Force
AFDD	Air Force Doctrine Document
C2W	Command and Control Warfare
EIW	Electronic Information Warfare
J3	Joint Chiefs of Staff