ELECTRONIC WARFARE IN THE 21ST CENTURY

SANJAY PODUVAL

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after changes occur.

—Giulio Douhet

The electromagnetic (EM) spectrum has increasingly emerged as the invisible weapon in war. Those who have learnt to exploit and appreciate its strengths and weaknesses have always emerged victors. Little did the pioneers of the radio beams know the effect these invisible weapons would have in future conflicts. Formidable as they are, the military use of the electromagnetic spectrum is a "necessary evil" much like friction and gravity, at times, unwanted, but one cannot actually do without them. Electronic warfare (EW) is the control of the EM spectrum which implies unhindered use by friendly forces and, at the same time, denial of its use by the adversaries.

EW has introduced another dimension in war. From its humble beginnings of interception of communications in the second Boer War, it has constantly changed the way wars have been waged through its period of evolution. It has by no means reached the end of its evolution, and in the future, it will be fought more in intangible spaces to gain information dominance before shifting its focus to the more conventional means of attacks. All this because warfare is now changing from platform-centricity to net-centricity, as evident in the recent conflicts.

* **Wing Commander Sanjay Poduval** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

EW has introduced another dimension in war.

THE EARLY YEARS

Gugliemo Marconi developed the first wireless telecommunication set in 1901, and by 1905, the wireless sets had sufficiently advanced to be used in ships for long range communications. These sets were basic in nature and vulnerable to electronic espionage and started to impact command and control. A classic example of this was seen in the years preceding World War I. The French intercepted a long message transmitted to the German ambassador in Paris from the German foreign minister containing a declaration of war to be delivered to the French government. The French, who had already decrypted the code in which the message was sent, not only intercepted the dispatch but so garbled its contents that the German ambassador could at first make nothing of it, while the French gained valuable time to prepare.

The advent of radars in World War II extended the eyes of the war-fighter well into the enemy territory. The radar incidentally is not an instrument of EW; rather, it is one of the main targets of EW. During World War II, both the Allied and Axis powers extensively used electronic warfare, or what Winston Churchill called the "Battle of the Beams" to jam or deceive radar or navigation systems. The forerunners of electronic counter-measures were the jamming and deceptive tactics of the British against the navigational system of the Germans early in World War II. The Germans developed the successful Lorenz navigation system for landing at night or in poor visibility conditions and later adapted it for night bombing operations. The "blind bombing system" practically razed the city of Coventry. The British countered this with a system called MEACON (Masking Beacon). German planes attempting to get their bearing, received signals from the MEACON and obtained either no bearing or the wrong bearing. On several occasions, German planes were completely lost and landed on British airfields or bombed unpopulated areas instead of assigned cities[1].

Later, electronic warfare helped in providing the battlefield commander with vital tactical intelligence. The importance of electronic warfare was particularly

[1] Mario de Archangelis, *Electronic Warfare Wars* (New Delhi: Ritana Books, 1996).

demonstrated at the battle of Gazala-Bir Hacheim (Tobruk)[2], in June 1942. In the battle which followed, Gen Rommel not only knew of British plans and of their numerical superiority in a general way, he also knew—thanks to his signal intelligence company—exactly where the British fighting units were deployed. World War II saw the birth of electronic counter-measures (ECM) and electronic counter-counter measures (ECCM), and electronic warfare started to influence technology. The focus of operations now was to intercept communication or deceive and destroy radars and their associated systems by carrying out SEAD (suppression of enemy air defence) and DEAD (destruction of enemy air defence) operations.[3] Control of the electromagnetic spectrum had assumed significance similar to command of the air, whereas in World War I actual brute force was used to subdue the enemy forces.

The Vietnam War of 1965 witnessed a boom in EW. It saw for the first time the appearance of Soviet missiles on the battlefields of Southeast Asia, signalling that the radars had acquired 'teeth' and had just become more potent. Electronic support measure (ESM) and signal intelligence (SIGINT) missions were extensively flown to detect the weaknesses of this system. This war also saw the introduction of unmanned aerial vehicles (UAVs) in combat in the form of the Teledyne Firebee which clocked over 3,000 hours over Vietnam in reconnaissance and electronic intelligence (ELINT) missions[4]. Radar warning receivers (RWRs) dovetailed with Shrike anti-radiation missiles (ARMs), which were primarily targeted against the Fansong radar of the surface-to-air missile (SAM) II system were also introduced. In 1971, realising the importance of EW, the Grumman EA-6 Prowler specially designed for EW was inducted into service.

The amazing victory of the Israelis over the Syrians in the Bekaa Valley conflict in June 1982 once again emphasised the fact that EW had entirely changed the way wars were fought and won. The innovative employment of UAVs in this conflict took EW to another level. UAVs were used for continuous surveillance and were actually tracking newly deployed SAM sites. UAVs since

[2] Air Vice Marshal J.P.R. Browne and Wg Cdr M.T. Thurbon, *Electronic Warfare*, Vol IV (New Delhi: Ritana Books).

[3] SEAD and DEAD operations *per se* are not a part of EW, they definitely are a consequence of it.

[4] Hank Basham, "RPV'S Make the Difference", http://www.airpower.maxwell.af.mil/airchronicles/aureview/1974/jan-feb/basham.html

then been employed in a number of roles such as jamming of radars, for target acquisition and designation, as decoys, etc. It brought to the fore the utility of these platforms for the dull, dirty and dangerous missions.

The logical next step was arming the UAVs, which actually was the result of lessons learnt during the North Atlantic Treaty Organisation (NATO) air campaign in Yugoslavia in 1999. The Predator UAV, in the course of the campaign, located many military targets but by the time the aircraft arrived on location, the targets were already gone[5]. After successful tests with the Hellfire-C laser-guided missile in February 2001, the armed Predator was successfully used by the Central Intelligence Agency (CIA) to destroy a vehicle carrying Al Qaeda operatives in Yemen on November 3, 2002. Since then, armed with Hellfire-C missiles, these UAVs have been used in Operations Enduring Freedom and Iraqi Freedom for efficient SEAD/DEAD operations[6].

Another important step in the journey of EW was the emergence of stealth. This was prompted by the increasing capability of SAMs, shooting down of the U-2 and a need to penetrate the radar cover undetected. Low observable technology applied to combat aircraft has allowed them to operate with relative impunity against sophisticated air defence (AD) with the aid of electronic warfare assets. The impact of stealth was realised in the 1991 Gulf War in which the F117-A stealth fighter flew over 40 per cent of the Allies' strategic bombing raids in more than 1,300 sorties, delivering more than 2,000 tons of ordnance without the loss of a single plane. They flew at the 'comfortable' medium and high altitudes beyond the range of ground based weapon systems—not one was even fired upon as the revolutionary plane flew into the aviation history books. In spite of its heavy use, the F-117 had a mission capable rate of 85.8 per cent for the war—4 per cent higher than in peace-time.[7]

[5] John McHale, "Unmanned Aircraft Armed and Dangerous," http://mae.pennnet.com/articles/article_display.cfm?Section=ARCHI&C=Feat&ARTICLE_ID=191669&KEYWORDS=UAV&p=32 .

[6] Chelsea Emery, Reuters, "Unmanned-Flight Technology Takes Off," ,http://www.usatoday.com/tech/news/ techinnovations/2003-11-17-drone-flight_x.htm

[7] From "White Paper - Air Force Performance in Desert Storm, Department of the Air Force, April 1991," http://www.pbs.org/wgbh/pages/frontline/gulf/appendix/whitepaper.html .

PRESENT DAY EW: WHAT IS DIFFERENT?

Conflicts since the Gulf War witnessed a growing integration of command, control intelligence, surveillance and reconnaissance assets. In the future, less expensive, more capable, lighter sensors will support networking on the battlefield. This will be possible mainly due to the breakthroughs in micro and nanotechnologies which promise compact systems having greater potential. The incredible advances made in the miniaturisation of increasingly 'intelligent' electronic equipment in the military technology revolution allow ends to be matched with means.[8]

The armed forces of the future will see the deployment of new types of weapons systems and architectures.

The armed forces of the future will see the deployment of new types of weapon systems and architectures. To achieve this, not only do we have 'intelligent' [global positioning system (GPS), laser-guided] munitions capable of 'localised' strikes of great depth, satellites capable of detecting and disseminating information of the smallest of targets, increasingly powerful electronic data and communications systems, we also have non-lethal weapons designed to paralyse men without killing them and incapacitate their equipment in the form of the active denial system (ADS) and directed energy weapons.[9]

Military is Changing

Commanders today at all levels can count on operating "24/7" on the global stage before a live camera that never blinks. This changed environment has a profound effect on how strategic leaders make their decisions and direct their commands. The impact of this kind of media coverage has been dubbed as "the CNN effect."[10]

Precision Strikes. The military now places a lot of emphasis on precision strikes i.e. the importance of bringing minimal forces in "harm's way," and

[8] Maurice Najman "Developing the Weapons of the 21st Century," http://mondediplo.com/1998/02/13warfare

[9] "Tuning Up The Heat: High-Power Microwave Weapons," *Jane's Navy International*, vol. 112, issue2, March 2007, p. 39 and http://www.irconnect.com/noc/press/pages/news_releases.mhtml?d=89438

[10] The term "the CNN effect" represents the collective impact of all real-time news coverage. Margaret H. Belknap, "The CNN Effect: Strategic Enabler or Operational Risk?" http://www.encyclopedia.com/doc/1G1-91564618.html

In the conduct of operations, it is more cost-effective to cause functional paralysis rather than complete physical destruction of the target.

precision targeting to destroy or neutralise only those elements involved in war- fighting. Rapid strides in technology in the second half of the 20th century have significantly enhanced the reach potency and precision of air power. Where only 20 per cent of the bombs fell within 1,000 feet of the target, today circular errors of probability (CEPs) have reduced to a few feet, as were seen in the decisive operations in the Gulf War 1991, Kosovo Operations 1999 and Iraqi Freedom 2003. Therefore, with regard to technology, the trend has been dominated by the use of precision guided munitions (PGMs) which are highly dependent on precise intelligence. They not only hit their targets, lowering the level of effort and minimising collateral damage, they also reduce capabilities that must be deployed. This has been enabled due to advances in satellite guidance and communications, computerised flight control systems and sensor technology.

Effects-Based Operations. In the conduct of operations, it is more cost-effective to cause functional paralysis rather than complete physical destruction of the target. The earlier war strategies were based more on annihilation and attrition, with the aim to render the enemy's armed forces ineffective. The same effect can be obtained quickly and in a more lucrative manner with fewer casualties following the effects-based operations (EBO) approach. An EBO is one where operations against the enemy systems are planned, executed and assessed in order to achieve specific effects that contribute directly to the desired military and political outcomes. In the future, the swiftness with which campaign objectives are achieved, minimum collateral damage and least casualties in executing campaign plans will play a crucial role in planning operations. It is in this region that information dominance, networking and EW will play a major role and achieve far better results since the outcomes hinge on focussed and accurate targeting.

Threats are Changing

The traditional concept of national security has undergone considerable changes.

Traditional combat techniques, accepted rules of engagement and concepts of firepower and manoeuvre are fast yielding to more unconventional forms that are aimed at neutralising force and weapon superiorities. The military has now got to deal with semi-conventional wars[11]: a state fighting a terrorist organisation which too is armed like a modern army. These non-state actors are difficult to target because they attack from within buildings in densely populated areas.

Today's non-state actors are sophisticated and, in many cases, less tied to conventional means of warfare. The United States is spending $500 million apiece for stealth bombers; a terrorist's stealth bomber is a car with a bomb in the trunk—a car that looks like every other car.

Networks are pervasive, throughout almost every domain of both our civilian and military sectors, and have commensurately evolved into critical vulnerable points.

Another area which is an attractive asymmetrical target to non-state actors is the network of various elements of power. Networks are pervasive, throughout almost every domain of both our civilian and military sectors, and have commensurately evolved into critical vulnerable points. At the most fundamental level, networking aims to accelerate engagement cycles and operational tempo at all levels of a war-fighting system. As a result, they are attractive asymmetric targets to adversaries who do not have force equality in the traditional sense.[12] The networked command, control, communications, computers, information, surveillance, reconnaissance (C4ISR) infrastructure that connects tactical, operational and strategic nodes is only as secure as its weakest link.

Technology is Changing

Technology leadership is shifting from the military to the civilian sector. The internet which began as a Cold War military technology in the 1960 to provide a reliable means of communication (even in the face of a nuclear strike) is now more

[11] Jasjit Singh, "Interpreting the Lebanon War of 2006," *Air Power*, vol. 1, no.2, Winter 2006, p. 33.

[12] Carl D. Porter, *Network-Cenric Warfare: Transforming the US Army* (Carlisle Barracks: US Army War College).

There are few geographical boundaries in the information infrastructure.

widely spread in the civilian sector. So is the case with networking and communication. This is because the technologies are simple, inexpensive and readily available and also due to the fact that the civilian sector is economically more lucrative and widespread. GPS too was initially conceived for the military, but over the years, though still managed by the US Department of Defence (DoD), it is more widespread in the commercial sector.

Information technology has also changed warfare, not in degree, but in kind, so that victory will increasingly go to combatants who manoeuvre bits faster than their adversaries. Perhaps the biggest effect of the changing technology on warfare will be the elimination of the concept of a front. Evidence that this revolution has already occurred is available from the recent Gulf Wars: smart weapons turned Saddam's strength (concentrated troops and tanks) into liabilities. Fortifications will tie armies down to fixed locations, making them sitting ducks for smart bombs, enabling adversaries to destroy the troops with precision-guided weapons.

Though easier said than done, cheap cyber weapons (e.g. computer viruses) can neutralise expensive kinetic weapons (e.g. missile defences) which are highly dependent on a networked system. The ability to collect, communicate, process and protect information is the most important factor defining military power today. In September 2001, the Al Qaeda used the global telecommunications net to coordinate successful attacks by small, stealthy groups who triumphed through information superiority (knowing more about their targets than their targets knew about them).

Geography is Changing

There are few geographical boundaries in the information infrastructure. According to Berkowitz, a senior RAND analyst, if fronts persist at all, they will live in cyberspace where info-warriors battle not over turf, but over control of routers, operating systems and firewalls. They only need to be connected to the cyberspace. The military can no longer create and control the battlespace as was traditionally done.

Time magazine of December 2005 carried an article titled "Long Distance Warriors" which described how USAF pilots, at the Nellis air force base outside Las Vegas, controlled the predator UAV flying over Iraq and Afghanistan at a distance greater than 11,000 km. In another instance, a Predator UAV tracked and killed fleeing insurgents who had attacked a US base in Iraq.[13] Target access points are, therefore, changing and may not be in geographical proximity to the target. Warfare is becoming increasingly network-centric.

Militarisation of Space

The offensive capability of space-based assets came to the fore when they provided target intelligence, secure communications, weather forecasting, GPS assisted navigation and all-weather precision targeting in the Gulf War 1991. Space today provides a cost-effective means to accomplish war-time missions in a technically superior manner and provides an effective means for obtaining information at a rapid rate. Space warfare involves dominating the "high ground" of space to deny its advantages to the adversary and to use it to implement one's own command, control, communications, navigation, reconnaissance, air defence, missile defence, warning, all weather precision targeting and weather forecasting. Space assets have become a key to the future digitalisation of the battlefield from where some of the fog and friction of war will be removed for the side dominating space.

The existing systems will see tremendous improvements in their capability and designs due to developments in the field of micro and nanotechnologies.

THE FUTURE

The existing systems will see tremendous improvements in their capability and designs. This will be possible mainly due to developments in the field of micro and nanotechnologies. Miniaturisation will result in an unprecedented level of

[13] n.6, p. 3, and Sally B. Donnelly, "Long Distance Warriors," December 2005, http://www.time.com/time/magazine/article/0,9171,1137653,00.html.

Protection against infrared guided weapons is the highest priority need in electronic attack and is an important deficiency that prevents efficient execution of operations at present.

integration—for example, the integrating of the radar warning receiver with the counter-measure dispensing system, making it into a single unit. Such integration will not only reduce the volume and power requirements but will also shorten the response time.

There will also be greater emphasis given to the development of counter-measures against infrared (IR) homing missiles, new age communication technology, radar-based systems, net-centric operations and space-based assets, as discussed below.

Infrared-Guided Weapons

Infrared weapons pose a serious and growing threat to forces and platforms in the air, on land and at sea. Inexpensive, portable missiles can be launched with ease and effectiveness against all airborne combatants. The threat of long range infrared guided anti-ship missiles is equally great, and formidable in both at-sea and littoral scenarios. Land combat vehicles are similarly threatened by frontal and top-attack munitions guided by infrared and multi-spectral seekers. Protection against infrared guided weapons is the highest priority need in electronic attack and is an important deficiency that prevents efficient execution of operations at present. The ever-increasing effectiveness of electronic warfare and the advent of anti-radiation missiles create the need for covert, radar silent operations. Therefore, sensors are required which are virtually immune to jamming, undetectable and yet capable of detecting targets at reasonable ranges. Infrared search and track (IRST) and electro-optical distributed aperture (EODAS) systems are being developed to automatically sense, alert the pilot and deploy adequate counter-measures to mislead or misdirect the missiles with or without his intervention as in the case of F-22 and F-35.[14]

[14] Ron Sherman, 'F-35 Electronic Warfare Suite: More Than Self-Protection,' http://www.aviationtoday.com/av/categories/military/845.html

Radar-Based Systems

Modern missiles travel at higher speeds, lower altitudes and have a smaller radar cross-section. These radar-based systems are becoming increasingly complex, adaptive to the environment, and difficult to intercept. They use a combination of homing methods to strike a target. This results in shorter reaction times and requires improved combat sub-system integration and greater automation for a proper response. New techniques are being developed to counter targeting and surveillance radars to deny acquisition of targets and, therefore, suppress subsequent active and passive homing threats. The development and induction of active electronically scanned array (AESA) radars is a step in this direction. These radars are programmed to act as transmitters, receivers, or radars.[15] The AESA system can work not only as a powerful radar, but can also do different tasks in parallel, such as a radar warning receiver, or jammer. The technologies for the development of millimetre wave (MMW) radars, ultrawide band (UWB) radars and spectral imaging systems such as hyper-spectral imaging (HSI) and multi-spectral imaging (MSI), which are under different stages of development, offer a range of possibilities for covert and silent operations.

The people's war of the past was conducted in tangible space but information wafare, in addition to occurring in tangibl space, is conducted even more in intangible space.

New Communication Technology

Another area of concern for electronic attack (EA) is the rapid development and adoption of new communications technology which has created deficiencies in the ability of forces to exploit and selectively disrupt these modern signals. Cellular and personal communications systems used by civilians and hostile forces and high-capacity digital, multi-channel networks associated with distributed information systems, pose particularly difficult technical challenges.[16] The ability

[15] V.K. Thakur, "Active Electronically Steered Array (AESA) Airborne Radar," http://kuku.sawf.org/Emerging+Technologies/2667.aspx

[16] "Joint Warfighting Science And Technology Plan," http://www.wslweb.org/docs/dstp2000/jwstppdf/13-EW.pdf

The ability to deny an opponent reliable use of his C4ISR systems is a critical aspect of electronic attack.

to detect, analyse, exploit and disrupt these signals is fundamental to the conduct of operations. In the context of EA, jamming transmitters and antennas used for command, control and communications (C3) signals require improvements in precise modulation selection and modulator control, linearity, efficiency, output power, and directivity.

Information Technology

Besides being used in the conventional manner, EW in the future will be more information-based, relying heavily on space and networking which is the crux of the discussion to follow. Conventional tactics effectively fused with space-based assets and high speed networks providing information superiority/dominance over the adversary will be crucial to victory in future conflicts.

The people's war of the past was conducted in tangible space, but information warfare, in addition to occurring in tangible space on the ground, at sea, and in the air, is conducted even more in intangible space, such as in electromagnetic fields. It is not only a battlefield in which guns and bombs proliferate, but also a "computer battlefield" in sheltered laboratories and control rooms.

The key technologies in information warfare are remote-sensing, communications and computer technologies. Key information weapons include precision-guided weapon systems, electronic warfare weapon systems as well as C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) which form the central nervous system and the network which interconnects all the components. These hardware and software items are necessary and essential to adapt to, and achieve victory in, information warfare.

One of the main steps, and something many nations are now trying to implement in becoming an efficient military at waging information warfare is bringing all branches of the military into an information network. Vital information and real-time communication may be shared on the network. One example of how much information dictates the waging of war in this information age is the surprise attack on Libya by the United States in 1986.[17] Before the attack, 18 electronic-warfare aircraft were sent to Libya to engage in powerful interference. Fighter aircraft were then sent to launch counter-radiation guided missiles to destroy Libya's air defence radar stations and, finally, fighter aircraft were sent to launch precision-guided bombs to attack five important targets. The information offensives in this raid included:

(a) Information reconnaissance to gain information on the targets of the raid and to study the targets in detail.

(b) Electronic interference to paralyse the opponent's communications and blind the opponent's air defence guided missiles.

(c) Information suppression by using counter-radiation guided missiles to destroy air defence radar stations.

(d) Information attack by using precision-guided warheads to attack pre-set targets.

During the Gulf War, the information offensives of the multinational forces were even more representative. In addition to the four types listed above, at least the following should be added i.e. extensive information operations were planned (but not executed) against the computer systems of Iraq's air defence system and stealth aircraft were used to launch precision-guided bombs against the communications buildings and command centres, to achieve information suppression. Therefore, the ability to deny an opponent reliable use of his C4ISR systems is a critical aspect of an electronic attack because it prevents the adversary from operating freely in the battlespace.

The combat personnel are not only the warriors who charge enemy lines for face-to-face struggles, but sometimes are the operating technical personnel who sit before computers and instruments.

One must not forget that electronic warfare is conducted by the people against the people. The combat personnel are not only the warriors who charge enemy lines for face-to-face struggles, but sometimes are the operating technical personnel who sit before computers and instruments. They stand at the first line

[17] Operation El Dorado Canyon, http://www.globalsecurity.org/military/ops/el_dorado_canyon.htm

in electronic warfare and in the resistance against C4I systems. Combat personnel must, therefore, be familiar with the technical and operational aspects of the weapons and equipment in their hands and must be very well trained in their operation. They must be able to understand accurately the combat plan and resolutely and flexibly utilise weapons and equipment to wipe out the enemy.

The growing importance of IT in warfare will also change the way intelligence agencies support conventional conflicts.

The wars of tomorrow will increasingly be fought in cyberspace. Thus, intelligence services will need an increasing proportion of tech-savvy talent to track, target and defend against adversaries' information technology (IT) capabilities. Cyber-wars will be played out on landscapes of commercial IT; intelligence agencies will need new alliances with the private sector, akin to existing relationships between nation-states, and they will have to confront awkward problems such as: performing intelligence preparation of cyber battlefields; assessing capabilities and intentions of adversaries whose info-weapons and defences are invisible; deciding whether there is any distinction between cyber defence and cyber intelligence; and determining who in the national security establishment should perform functions that straddle the offensive, defensive and intelligence missions of the uniformed services and intelligence agencies.

The growing importance of IT in warfare will also change the way intelligence agencies support conventional conflicts. New technology will collect real-time intelligence for fast-changing tactical engagements, but the communications systems available at present are far too slow for disseminating these high-tech indications and warnings. Faster means of delivering—and protecting—raw collection are being devised, so that real-time intelligence can be sent directly to shooters without detouring through multiple echelons of military intelligence analysts. Super-high-speed free-space laser communications links will be the technological cornerstone of future military satellite communications. The new transformational satellite communications system of the US—better known as TSAT—will feature 10-gigabit-per-second laser cross links between satellites, and between satellites and high-altitude manned and unmanned aircraft. To overcome the inability of lasers to operate reliably through the low-earth atmosphere (because of clouds, precipitation, dust and other obscurants), TSAT's data links to ground stations will be extremely high frequency (EHF) RF links able to move data as quickly as 2 gigabits per second. The eight-satellite TSAT constellation is to be fully operational in 2016.[18] A 1-gigabyte image from a space-based radar satellite would take 88 minutes to move over MILSTAR II[19], while on a TSAT it would take less than a second. In addition, TSAT will enable as many as 1,500 combat vehicles on the move to transit data, a capability not available at present. According to Berkowitz, future wars will not be won by having more troops, weapons and territory than an opponent, but by having more bits of information. The digital revolution has started occupying the centre-stage.

Network-Centric Operations

The faster we can gather, distribute, analyse and understand information, the faster we can decide, how and when to act in combat.

Network-centric operations are mostly about the application of various digital-electronic technologies to military roles and missions. In the past 20 years, many astounding technological advancements in radars, directed energy, communication, space exploitation, miniaturisation, data processing, etc have taken place, which have not only influenced every aspect of our lives but also altered the means of waging wars. Warfare can now be more efficient and effective. The integration of all these factors has essentially led to network-centric warfare (NCW). Networking is a mechanism which improves operational tempo by accelerating the observation-orientation phases of Boyd's observation-orientation-decision-action loop. This is achieved by providing a mechanism to rapidly gather and distribute targeting information and rapidly issue directives. A high speed network permits error

[18] John Keller, "Optical Links are Key to Next-Generation Military Communications Satellite," http://mae.pennnet.com/articles/article_display.cfm?article_id=202216

[19] MILSTAR-II is the tactical and strategic multi-service satellite system designed to provide survivable communications for US forces worldwide.

The increasing dependence of societies and military forces on advance information networks creates new vulnerabilities.

free transmission in a fraction of the time required for voice transmission, and permits transfer of a wide range of data formats. The faster we can gather, distribute, analyse and understand information, the faster we can decide, how and when to act in combat. The audacious second attempt on April 7, 2003, to decapitate the Iraqi leadership, amply demonstrates this. The strike was especially noteworthy for the way it saw information on the whereabouts of the Iraqi dictator, which emerged at very short notice, transmitted rapidly to Allied air planners and then to the B-1B. "We confirmed the coordinates and then it took about 12 minutes to fly to the target and release the weapons," said Lt Col Frank Swan, the weapons systems officer on the aircraft. The crew had previously been tasked with attacking an airfield in western Iraq.[20] This short-duration 'sensor-to-shooter loop' is a key component of 'net-centric warfare': the ability to transmit, receive and view data in real-time across the spectrum. Net-centric warfare was practised in an embryonic capacity in Afghanistan and honed in Iraq – as the B-1B mission demonstrated.

Networking has its greatest gains in combat effect during battlefield strike and close air support operations, especially against highly mobile and fleeting ground targets. In such an environment, where the opponent is continuously on the move, networking can produce spectacular gains since the bottleneck limiting force capability which lay in the flow of targeting information to strike aircraft is effectively removed. The deciding factor in the first Gulf War was the ability of US forces to fight effectively at night. This advantage multiplied in Operation Iraqi Freedom and the conflict in Afghanistan. It was possible because of better and more reliable communication systems and networks. Battlefield elements of the future – tanks, aircraft, ships, and soldiers – all will be nodes within one large networked force. General Dynamics and Lockheed Martin are designing and demonstrating technologies for a network-centric force on the move.[21] The aim is

[20] "What Went Right?," *Jane's Defence Weekly*, April 30, 2003, http://www.oft.osd.mil/library/library_files/article_63_Jane.doc.

[21] United States Army Signal Centre, http://www.fas.org/man/dod-101/sys/land/win-t.htm.

to provide war-fighters a secure, high-bandwidth, wireless communications network that will provide soldiers access to critical battlefield information, seamless connectivity and security across a host of platforms and points of presence. It will encompass intelligence, surveillance and reconnaissance systems, as well as 'netted' (integrated) weapons, future combat systems along with cell-phone systems for individual soldiers.

The increasing dependence of societies and military forces on advance information networks creates new vulnerabilities through means such as computer network attack and directed energy weapons. The inherent implication here is that the universal nature of networked systems is in and of itself one of the key vulnerabilities. Provision of digital wireless connectivity between combat platforms is a major technical challenge which cannot be understated. While civilian networking of computers can largely rely on cabled links, be they copper or optical fibres, with wireless connectivity as an adjunct, in a military environment centred on moving platforms and field deployed bases, wireless connectivity is the central means of carrying information and the area most vulnerable to interference.

The fact that military networks and civilian networks co-mingle provides another set of vulnerabilities which must be addressed, for example, during Operation Iraqi Freedom, US and Coalition forces reportedly did not execute any computer network attacks against Iraqi systems, even though comprehensive information operations (IO) plans were prepared in advance US officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to the financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe.[22]

EW in SPACE

Militaries all over the world increasingly depend on space systems for various

[22] Charles Smith, "U.S. Information Warriors Wrestle with New Weapons," NewsMax.com, March 13, 2003 http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml .

Space is emerging, as a distinct warfare area of its own. The effect may be to so dominate an adversary before the conflict starts as to make the conflict unnecessary.

force enhancements and application functions. Space force plays an increasingly critical role in providing situational awareness (e.g. global communications, early warning, precise navigation, imagery, signal intelligence, timely and accurate missile warning, weather and ISR, etc) to military forces. Therefore, space power is a vital element which provides the ability to be persuasive in peace, decisive in conflict and preeminent in any form of combat. Space systems are very extremely important to military operations and it is unrealistic to imagine that they will never become targets. The trend towards increased dependency creates both opportunities and vulnerabilities in future crises and conflicts. Just as land dominance, sea control and air superiority have become critical elements, space superiority is emerging as an essential element of battlefield success and future warfare. As space systems become lucrative targets, there will be a critical need to develop robust capability to ensure space superiority—just as they have been for land, sea and air dimensions. Historically, military forces have evolved to protect national interests and investments. During this early part of the 21st century, space power has all the makings of evolving into another and equal (to land, sea and air) medium of warfare. Likewise, space forces will emerge to protect these commercial and military assets.

In the future, comprehensive plans will be laid out to achieve space superiority throughout the range of military operations to beat these space-based defences. Satellites are the main focus of military space activities. Over 800 satellites orbit the earth, many of which have military uses, from reconnaissance to guiding weapons. They are increasingly used to provide direct support for military operations: for instance, during the 2003 Iraq War, 68 per cent of munitions were satellite guided (up from 10 per cent in the 1991 Iraq War). Space assets have become a key feature in the digitalisation of the battlefield where some of the fog and friction of war is removed for the side dominating space.

Space is emerging, as a distinct warfare area of its own. The effect may be to so dominate an adversary before the conflict starts as to make the conflict unnecessary, something Sun Tzu advocated nearly 2,500 years ago. Owing to the strategic importance of satellites in space, EW in space is aimed at jamming , sabotaging and destroying satellites to gain information dominance in future conflicts. The sphere of action of EW in space is not limited to anti-satellite operations but also has tremendous potential applications in:

- Detection, tracking and destruction of ballistic missiles.
- Misdirecting or hijacking UAVs, especially those linked via satellites.
- Disruption of global positioning systems.[23]

Space plays an important role in the C4I framework, therefore, limiting the adversary's use of space and precluding him from influencing friendly space systems is crucial to maintaining situational awareness because of the critical advantages it provides. There are various ways of disrupting satellite operations. They are mainly ground-based and include: jamming i.e. interrupting communication links between satellites and ground stations[24] by 'drowning out' the signal with a more powerful 'fake' signal or by targeting ground stations via physical attacks or computer hacking. Ground stations are considered more vulnerable than satellites themselves.

One of the recognised weaknesses of GPS is its susceptibility to jamming.

Several other techniques are possible although there is no evidence they have ever been used (except in tests):

- Low power lasers can disrupt satellite sensors and, according to some reports, over 30 countries may have this capability, although this figure is hard to verify.
- Nuclear weapons explosions in space: in 1962, the US high altitude nuclear detonation resulted in high radiation levels, destroying seven satellites within months.

[23] These programmes were called Suter 1 and Suter 2, and were tested during Joint Expeditionary Forces Experiments held at Nellis Air Force Base in 2000 and 2002. David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p. 34.

[24] "Chinese Lasers Blind US Satelites," http://politics.slashdot.org/article.pl?sid=06/09/28/126207.

- Use of ground or air-launched missiles: during the Cold War, both the US and Russia developed missiles for this purpose.[25] The Chinese also demonstrated this capability in January 2007.

In Operation Iraqi Freedom, commercial satellites provided 80 per cent of US data, compared with only 45 per cent in Operation Desert Storm in the early 1990s. Therefore, some commercial satellites perform a dual role. Many commercial satellites have only one ground station, leaving them particularly vulnerable. Military systems are usually better protected than commercial satellites, but the latter are increasingly used for military purposes.

Owing to its strategic significance, say Chinese aerospace experts, space electronic warfare has become the most important way to gain information dominance in future wars.

Today, most forces use GPS for navigation and there is an increasing trend towards using GPS guided weapon systems. Most of the expensive, cruise-type missiles in the US inventory such as the Tomahawk, conventional air-launched cruise missile (CALCM), and some land-attack versions of the Harpoon missile employ GPS for navigation purposes. One of the recognised weaknesses of GPS is its susceptibility to jamming. The GPS signals from the satellite arrive at the user's GPS receiver at a very low level, so the jammer has the advantage of being, say, half a mile away. Hence, it doesn't take much power to completely swamp the GPS signal in the receiver.[26] It has been shown that even low power GPS jammers are capable of jamming an array of sophisticated military equipment. These jammers are cheap and easy to manufacture which could render the GPS receivers ineffective, or worse still, cause serious damage by spoofing the system to receive wrong information and thereby directing the weapons to places unintended by the user. Electronic warfare in space will be focussed in overcoming these drawbacks by providing assured and secure down link frequencies.

[25] "Military Uses of Space," http://www.parliament.uk/documents/upload/postpn273.pdf

[26] Michael Puttré, "GPS Weapons are Transforming the Air-Ground Battle," http://www.mputtre.com/id17.html.

THE CHINA FACTOR AND IMPLICATIONS FOR INDIA

China: EW Developments

China is in the process of upgrading its EW capability through technology acquisition, reverse engineering and indigenous research and development. China views EW as a fourth dimension of ground, naval and air combat. It currently is engaged in an extensive programme to upgrade its EW technology equipment and training. The current inventory of EW equipment includes a combination of the 1950s to 1980s vintage technologies. China is seeking to procure state-of-the-art intercept, direction finding and jamming equipment. For this, it has established close commercial ties with electronic companies in numerous foreign countries.[27]

Given China's current level of progress in laser technology, it is reasonable to assume that Beijing would develop a weapon that could destroy satellites in the future.

Owing to its strategic significance, say Chinese aerospace experts, space electronic warfare — aimed at jamming, sabotaging and destroying satellites — has become the most important way to gain information dominance in future wars. Chinese experts in space EW note that the counter-jamming capabilities of radar systems have been continuously advancing. The air-space battlefield is said to be the quintessential battlefield for information counter-attack. EW satellites, travelling in geostationary orbits or 300-1,000 km orbits can conduct electronic reconnaissance and jamming in wide areas. EW aircraft in flight can execute high-intensity electronic killing of enemy long-range radar stations, command centres, and communications centres to paralyse their command capabilities and disable their firing systems. They can also directly launch anti-radiation missiles to totally destroy the enemy.

According to Chinese military scientists, high-powered microwave weapons have triggered "a new revolution in electronic warfare systems and technology."

[27] "Future Military Capabilities and Strategy of the People's Republic of China," http://www.fas.org/news/china/1998/981100-prc-dod.htm#5

Not only are they compatible for creating integrated systems with radar for low-power detection, target tracking and jamming, but their power can also be rapidly increased for destruction of targets and for inflicting damage on the electronic equipment of enemy targets. These weapons portend extremely wide applications extending to aeronautic, astronautic, warship, and battlefield weaponry. According to China, rapid advances are being made in the US' HPM and high energy laser weapons with some of them already entering applications stages. China may already possess the capability to damage, under specific conditions, optical sensors on satellites that are very vulnerable to damage by lasers. However, given China's current level of progress in laser technology, it is reasonable to assume that Beijing would develop a weapon that could destroy satellites in the future.[28]

China reportedly has considerable and growing capabilities for developing information technology and networks. Chinese officials state that future military plans call for China to focus on developing "new-concept" weapons, such as electromagnetic pulse (EMP) systems for jamming adversary networks and new satellites for establishing a unique GPS network for the Chinese military.[29] China has also networked its forces using the European "Galileo" space-based global positioning system. China's military thinkers believe that the first wave of warfare will develop from firepower attack and electromagnetic attack to satellite paralysis.[30]

Implications for India

The future battlefield milieu, with its devastating weapons, surveillance equipment, dynamic tactics and highly mobile and dispersed forces, will demand state-of-the art command and control architecture. In such an environment, the time available to the commander for decision-making is decreasing while the complexity and volume of information and penalties for error are increasing.

[28] Source Jane's Defence at http://www.aeronautics.ru/archive/research_literature/aviation_articles/Janes/topics/plasma_stealth/Directed%20Energy%20Weapons%20and%20Sensors.pdf.

[29] Mary C. Fitzgerald, "China Plans to Control Space and Win the Coming Information War," *Armed Forces Journal*, November 2005, p. 40.

[30] Mary C. FitzGerald, "China's Military Modernization and its Impact on the United States and the Asia-Pacific," http://www.hudson.org/files/publications/07_03_29_30_fitzgerald_statement.pdf.

Effective command and control is an essential ingredient of all operations, in both peace and in war. The emerging command and control systems are valuable assets for managing the entire battlespace, with the emphasis shifting from platform-centric operations to network-centric operations, which are emerging as significant force multipliers. The concept of network-centric operations is an important one if we are to expand our tactical capabilities to a significant extent. In order to exploit the full potential of our surface, submarine and airborne platforms, it would be ideal to have these elements networked. It will then be possible to have a complete picture of what each of our platforms can detect by means of their electronic warfare devices, conveyed through the medium of satellites. However, the complexity and cost of such networking is extremely high since it would require a high degree of networking among satellites, platforms, weapon systems, command and control centres and also the interoperability of various systems. This is a huge task and may not actually be required in the near future in our context. But of immediate importance would be to integrate various systems within a Service, operating in a theatre. Difficulties notwithstanding, net-centricity is imperative because it enables the capability of geographically dispersed forces to operate as one integrated force.

The need to provide balanced wideband, narrowband and protected communication systems to a broad range of users across diverse mission areas can be effectively met by a satellite-based network. Satellite communication and navigation services will form the backbone of this desired ability to conduct operations in both peace and war during the coming years. The satellite-based communication network should be capable of supporting joint C4ISR and providing effective back-up as an overlay network to terrestrial communication, mobile communication and maritime communication requirements of the Services in all kinds of environments, including the nuclear.

The Indian Air Force (IAF) is on its way to establishing the Integrated Air Command and Control System (IACCS) in a phased manner. This system will have the capability to integrate the air situation picture, received in real-time, from ground-based as well as airborne sensors, and would be available to the IAF commanders to initiate, monitor and control tactical air defence actions against any hostile intruder in our air space.[31]

India currently has in orbit three dual-purpose satellites—CARTOSAT-I, CARTOSAT-II and the technical experiment satellite—that are used by the country's space agency and the military. The plan envisages the linking of the airborne warning and control system (AWACS) (when procured), aerostat radars and low-level transportable radars of the IAF with them.[32]

The C4ISR system should have physical and electronic security, survivability and adequate redundancy so that C4ISR and network-centric operations (NCO) systems are protected against deliberate or inadvertent, unauthorised acquisition; disclosure, manipulation; loss or modification of sensitive information.

Secure communication and networking are undoubtedly going to play very important strategic and tactical roles, not just in electronic warfare but also in conventional battles and wars, as the US led wars in Afghanistan and Iraq have amply demonstrated. In line with this thinking, the Indian Army commissioned the Dhruva Satellite Communications Network in September 2006. This state-of-the-art secure satellite network has the world's highest V-SAT (very small aperture terminal) which is integrated with the Eastern Theatre Satellite Network, one of the densest satellite communication networks within the country. During the commissioning of the network, the Signal Officer-in-Chief Lt Gen Davinder Kumar, VSM and Bar, stated that operational necessity, self-reliance, security and information assurance were the keys to provisioning of this high end technology, fully secure satellite communication network for the army. The network has been integrated with the army's terrestrial network to increase its range and efficacy with a view to meet the challenges of the digital battlefield of tomorrow.[33]

Elements like fighter aircraft squadrons, radars, Command Headquarters along with the existing Air Defence Ground Environment System (ADGES),

[31] "Integrated Air Defence System," http://164.100.24.208/lsq/quest.asp?qref=16570.

[32] "Aerospace Command," http://www.domain-b.com/aero/June/2007/20070611_military.htm.

[33] "Satellite Network for the Indian Army," http://www.expresscomputeronline.com/20060918/market12.shtml.

communications networks, etc are being modernised with asynchronous transfer mode (ATM) technology using fibre optic media.[34]

Although radar and communications systems remain the key targets of EW, systems such as the GPS, network links, etc have emerged as important objectives to an EW campaign.

In the era of information warfare, net wars, cyber warfare and the nuclear backdrop, C4ISR systems should have physical and electronic security, survivability and adequate redundancy so that C4ISR and network-centric operations (NCO) systems are protected against deliberate or inadvertent, unauthorised acquisition; disclosure, manipulation; loss or modification of sensitive information. The low cost of entry (for example, a laptop connected to the internet), and the ability to operate anonymously, are factors that make cyberspace an area for asymmetrical operations for potential adversaries. Countries like China, Russia, Cuba, Iran, Iraq, Libya, North Korea, and several non-state terrorist groups are reportedly developing such capabilities. In case of a local breach of network security, there should also be a provision for dynamic allocation of computing resources while, at the same time, isolating the affected system. In its quest towards becoming a network enabled force by 2009, the Indian Army is developing a computer emergency repair team[35] which is tasked with analysing computer intrusion incidents and providing solutions for such problems.

While Chinese military experts have applauded the "brilliant" performance of the US GPS in recent high-tech military operations, they continue to clarify its inevitable "Achilles' Heel" because the low altitudes of the GPS satellites and low power requirements of their receiver sets make them susceptible to interference, jamming or spoofing.[36] This is an aspect which is widely acknowledged, therefore, suitable standby/redundant systems must be incorporated to ensure smooth operations under these conditions. The Chinese

[34] Ravi Shekhar Pandey, "Communication In Defense: Securing The Frontiers," http://www.domain-b.com/aero/June/2007/20070611_military.htm

[35] Lt Gen Davinder Kumar, Signal Officer-in-Chief, Indian Army, "Information Warriors," http://mod.nic.in/samachar/feb15-06/h3.htm

[36] FitzGerald, n.30.

anti-satellite (ASAT) test signalled that satellites in space are no longer safe. The vulnerability of space-based assets is only going to increase after the US shot down their uncontrolled spy satellite before it entered the earth's atmosphere.

Therefore, we must be wary of putting all our eggs in one basket. In view of this, India is already on the way to develop its own navigation system GAGAN (GPS and geo augmented navigation) for the civil aviation and Indian Regional Navigation System (IRNSS). India has also signed the GLONASS (Global Navigational Satellite System) agreement with Russia which is an alternative to the US GPS. Another thought is to enter into collaboration with other friendly countries to use a common satellite system for a variety of purposes. This would in some measure restrain any country from disrupting satellite services since it would affect others as well.

CONCLUSION

EW has been important ever since military forces first began using radios and radar. It is the form of electromagnetic attack that is generally associated with the jamming of sensors, command and control, or communications systems that use the electromagnetic spectrum. Although radar and communications systems remain the key targets of EW, systems such as the GPS, network links, etc have emerged as important objectives to an EW campaign.

The proliferation of new sensor and communication technologies in recent years has been so profound that warfare has now transcended from being terrestrial to outer space. Satellites are playing an increasingly important role in achieving information dominance. Space power in the future will play a very major role in deciding the outcome of conflicts. Security of space-based assets will, therefore, have to be accorded the highest priority.

The synergistic employment of space-based assets and robust networking for information dominance will be important elements of success in future conflicts. Disruption of any one of these by hard kill or soft kill will have far-reaching effects on the outcome of operations. Moreover, the fantastic rates of increase in the ability to collect, process, classify and disseminate information to an ever-growing number of targets within an increasingly wide geographical radius at speeds that are hard to imagine implies that these information systems will be the targets of attack and there is a perpetual risk that the "weak signals" (those that count) could disappear in a "growing background noise." Adequate precautions against these are best taken during the design and implementation stages.

The war front, in the conventional sense, no longer exists. It is fluid and scattered. Therefore, the essential factor for success in the future will increasingly lie in the ability to provide secure links between the soldiers and commanders and the ability to increase the information gap between allies and adversaries.