CENTRE FOR ADVANCED STRATEGIC STUDIES

CASS

PROCEEDINGS OF SEMINAR

ON

INFORMATION WARFARE

24TH SEPTEMBER, 1997

CENTRE FOR ADVANCED STRATEGIC STUDIES

CENTRE FOR ADVANCED STRATEGIC STUDIES

PROCEEDINGS OF SEMINAR

ON

INFORMATION WARFARE

24TH SEPTEMBER, 1997

CONTENTS

Editor : S. G. Chitnis, Deputy Director, CASS

Address : **Centre for Advanced Strategic Studies**
Old Examination Hall Complex
Pune University Campus, Pune 411 007
Tel. No. 357516

PROCEEDINGS OF THE SEMINAR

Air Marshal (Retd) S. Kulkarni, Director, Centre for Advanced Strategic Studies (CASS) opened the Seminar and welcomed the distinguished guests. He welcomed all the participants of the Seminar.

The Seminar consisted of three sessions.The first session dealt with Electronic Warfare.The subject was taken by Gp Capt(Retd) G.M.Apte who had extensive experience in the IAF and AAI. Thereafter, the second session was taken by Dr. D.P. Bobade, Technical Director, National Informatics Centre, Pune. He talked about the current status of information technology in India. The last session of the Seminar was devoted to information warfare. This was eminently handled by Dr. G.S. Mani, Dean & Director, Institute of Aranment Technology, Pune and Sqn Ldr (Retd) Ajay Singh, Delhi. Sqn Ldr (Retd) Ajay Singh has extensively written on this topic in Newpapers and Journals.

The first two sessions were chaired by the Director, CASS where as the last session was chaired by Dr. Mani.

After each presentation sufficient time was devoted to questions and answers as also general discussion pertaining to that topic. This proved to be educative, thought provoking and lively. Therefore, summary of discussions has been dispensed with.

The seminar came to an end with the concluding remarks by Shri Ram Pradhan, President, CASS.

CENTRE FOR ADVANCED STRATEGIC STUDIES

INAUGURAL ADDRESS BY DR.BHATKAR

Air Marshal Kulkarni, Group Captain Chitnis, Group Captain Apte, Squadron Leader Ajay Singh.

I think some of us I am meeting for the first time and Dr.Bobade who is associated with me for years together in the IPAG and then in NIC, and dear friends.

This theme of information warfare was introduced to me just yesterday by Air Marshal Kulkarni and Group Captain Chitnis, when they came to me and asked me whether I could be associated with this seminar on Information Warfare. And I started asking myself this question of what is information warfare ? When it comes to the term warfare, I feel I am somewhat distant from the concept because I am speaking and advocating and meditating on how to go away from the concept of warfare. But then, this morning when I was contemplating on this term 'Warfare', I saw that the state of warfare is innate and integral part of our existence itself. Our biological existence in which of course our immune system is constantly fighting against the attacks of bacteria and viruses and many other things.

Our mental existence in which we are constantly discerning between what is good and what is bad, what is evil and what is auspicious and that state continues. How to discern between these two states? And our spiritual existence in which we are trying to go away from the evil and go to the concept of what is divine.

So this is the very nature of our existence. Conflict is the very nature of our existence itself. If you look at the whole ecology itself, you see the prey and the preyed systems, the big fish eat the small fish. The whole concept of this layer - the food chain is layered on the question of conflict, on the existence of conflict itself. And it continues in societies, it continues of course in institutions, societies and nations. Whole history is full of wars and conflicts and I think the wars envelop the whole world.

So, warfare is not something external to us. I think that it is an integral and innate part of the existence of human beings, the existence of the every being, the existence of societies and the existence of nations themselves.

Having accepted that, we must now ask the question; What is this Information Warfare? We are familiar with physical warfare and the warfare with weapons and we must perhaps make a distinction between warfare and the war itself not even the declaration of war. Warfare is essentially a hostility towards a perceived adversary. Perceived adversary - he may not be the adversary. You know in your own mind, who is your enemy and who is your friend.

And here I am reminded of one very interesting observation in Yoga Vashistha, in which Vashistha is teaching Ram, who is disillusioned when he sees the world when he goes out of his palace. And now Vashistha is explaining that what is this enemy and what is this friend and Vashistha tells him that it is all a concept of mind. It is only a mere concept of mind because the same person may be your dear friend one time, the same person at other time, in a different context, becomes an enemy.

This we see in our own life that we have remained dear friends for sometime, who, all of a sudden, become enemies. Same thing is true with the societies and nations and religions. So it is merely a concept of mind and if you alter your mind, Vashistha advises that, then the enemy will become your friend. You just have to change the nature of your perception and you change your mind.

So everything is really the mind itself and the mind can change by changing the context. And how it can change by changing how you are sensing, and particularly by information and knowledge. So I think the information on the enemy, I think the very concept of enemy is so profound, so philosophical, that the information can change. For example in institutions or in political systems you can see the fact that if you are given wrong information by your friend about somebody that this person is thinking about you like that, he is treating you like this in your absence,it is all information and your very concept about that person changes, particularly if you are in power.

We see that same thing is happening, how the information is used by the political parties to create different images in the minds of people to inflame our passions and emotions. This of course is well known, I am not trying to say anything different than that but we must try to understand the power of information. We all know that, how when US wanted Yeltsin to be elected as the President of Russia, how they articulated the whole policy of propaganda through the information technology medium, the television talking about the ills of communism or socialism and other things, and situations like that. This was continuously projected across the people as articulated policy and it really swayed opinions of Russians when some other forces were rising. I am just giving an example of that. It is a very well documented thing and was articulated by American media people.

Similarly as the great linguists who have been talking about that, what is it that is presented on the media today. All the newspapers, particularly the Western newspapers, the images about some countries which are created. For example the images of India created in the minds of Western countries or other advanced countries. This is essentially what is created by the media itself. The reality is something entirely different.

We experience information warfare in everyday life through the media. The opinions we form about people, societies, religions, states and nations is what we are told by the media and the media can present a very distorted picture.For example,advanced countries perceive India as a land of elephants, serpents, poverty,hunger and hopelessness. But this is not true ! This is a kind of Information Warfare of Western countries or other advanced countries. This is essentially what is created by the media itself. The reality is something entirely different. Interestinegly, studies have shown that experiences on television, computers, or Internet are perceived as real by the younger generation.

So this is the power of mis-information or dis-information or information pollution or whatever, or something like outside information warfare. How it is used. I have not read the books but I have read reviews of how the young generation or most of us who are glued to the computer today. We live more and more in the cyber world, that people see their experiences on the television, experiences on the computers, experiences on the Internet are as real as the real experiences themselves. It is very very interesting to see how they can alter our minds or alter our existence itself.

For example people have friends on the net who are as real and as dear as your physical friends. Perhaps more dear. I have experienced this with my own daughter when she has interest in such friends across the world and whom she has never seen. I myself have experienced that, in writing a book on mathematics, on abstract mathematics, when I was doing my Ph.D with a Professor in Lehigh University, Professor D.G.B Edlen. I wrote a book on abstract mathematics, functional mathematics, and I have never met him. I have never met him even till today. But I have published a book which is used here by research community in the field.

So this is very very interesting, particularly when you are talking about - as we are transforming from the industrial economy, from the industrial world to the - I think into the information age and see the studies, the strategic studies, and I feel that today we are talking about information warfare not merely in terms of aggression of the nations or the defence in a traditional sense that it has been understood.

But the warfares of today are, I think, the sociological warfares, the economic warfares or the technological warfares. I think I have been talking about it, and many many people, have been talking about it. Tomorrow's warfares or today's warfares are more and more knowledge warfares which have direct implications on the economic warfares.

For example, it is to be seen as to what happened recently in the trades and on the stocks or the economic developments of Malaysia and Thailand particularly, and we have also to face that sometimes, that mere creation of some sort of a dis-information in the minds of the investors who have been so strongly investing in Malaysia for sometime and earlier in Thailand and also in India, that what is happening ? That the Government is not really serious, Mahathir is not really serious about this liberalisation etc, and is oriented towards fundamentalism. You create a dis-information and suddenly people start withdrawing, led by Soros, the economy collapses, collapse of several hundreds of billions of dollars to fifty per cent of it overnight. Suddenly people get panicky.

Let us now look at the financial trading on the stock markets. The whole world has been recently shaken by what has happened in the stock markets. The economies of Thailand, Malaysia have been devastated. All this perhaps happened because of some disinformation spread by some investor Super Gurus. These Gurus spread the rumuor the fundamentals of the economies of Thailaind, Malaysia are very weak. And suddenly the investors started pulling out of the stocks and currencies. The result was catastrophies never anticipated by these nations. The tremors were felt all over the world. Such is the power of disinformation or the information warfare. Even a real war would not have caused such a economic devastation for these countries.

We also saw on the stock exchange. I know how the panics are created, in the minds of the people by certain dis-information, that something is going to happen or the political parties are going to fall, kind of just create some rumours and try to manipulate the economies, to manipulate the fates of so many industries. How it has become such a potent weapon.

Earlier I was thinking that information warfare relates to only what happens to electronic equipment. But I think it has become extremely important. Perhaps people are trying to get into the network or you are talking encryption or decryption technology or jamming your communications. This is information warfare. But this is one part of information warfare.

But more profound is the fact that you are playing on the beliefs and the knowledge of the perceived enemy. You wish to change his beliefs. You are changing his knowledge by giving some sort of a different kind of information - dis-information, wrong information and creating confusion in the minds of the people so that your objectives, I think, are not attacked. These are again the objectives of some people. I think nations do not, I think the nations are represented by their leaders. It is in the minds of some people that this is what should be done. I think the conflict between our neighbours are specially the conflict between the leaders of the people and not between the peoples themselves. The peoples have been manipulated over the years by the wills of the political leader.

Now, as we go on to really take up the issue of technology, information technology itself, we are living in the age of digital realities. It is very very important that we understand that 20th Century has gone, at the end of this century that we are going from the physical reality, of course the mental reality, the very existence, but we are going more and more to digital realities. What we perceive is of the computer.

For example many people and some groups do trading on computers and they are doing some simulations on super computers. Virtually they have become rich by millions of dollars on the basis of trading on the computer, on the screen. There are virtual friends, there are virtual enemies on the screen itself. They see that this has happened - this is the one with your feeling of richness or feeling of economic welfare or feeling that you have made billions of dollars overnight. It is on the screen. And that is what you are perceiving that you have lost next day so many billions of dollars, and I see that, I understand that people who do trade, who are very young. Very young people are allowed to do trading because you can't stand losing billions of dollars in the few hours time. People above 35 cannot stand that mental tension - the way it happens. And I have seen young guys just come out. They are allowed to do trading based on the computer simulation.

We are today developing model for doing those simulations based on neuro network, applying the laws of physics and it is very interesting to see what happens in trading. Of course it is a mad game of computers. Earlier we used to see what happens on stock exchanges when lot of it was done on computers. But now your see computer advisers. You now buy, now sell, now invest, not only for the stocks- but the derivatives are very very important.

How you change the other economies by just seeing, even creating right or wrong information, whatever, it is the truth. This is very very interesting strategic study we must do. Because tomorrow the existence of nations will depend on this. You look at Thailand. What has happened. Thailand, suddenly became a great country, you saw the economy rising with growth rate of eight per cent or ten per cent, and fall overnight, came to a desperate situation. Same thing in Malaysia, the panic which has occurred. I think the same thing perhaps occurred in a different way in Russia. Just create a concept of that openness and how the whole thing changes. How the Berlin wall collapsed ?

Strategic studies, I think, must understand this concept that tomorrow's weapons are not the weapons in the traditional sense but the weapons of this information, knowledge. beliefs, which are going to be altered, the paradigm shifts which are going to occur. Today we see that many many companies just disappear. Let me give you this example. I have been discussing sometime back with the biggest giant in telecom industry ITI. When you talk to the CMD of the Company, he is not aware that next year this company is going to disappear or perhaps going to get sick. So sick that it is for sale. Almost like the government bails it out because the paradigm shift has occurred, the information shift has occurred in the way the companies are run, or the way the chords are going to be different or the way the market economies are going to be of a different kind and you are not aware..

This is not only the case of India. I have been discussing sometime back and I have a personal experience of talking to very very senior people in ICL, which is the giant in Europe, and perhaps in U.K., which is perhaps the oldest computer company more old than the IBM even. They did not know that one day, the top people, that one day they will be gobbled-up and with the gobbling up of ICL, and Boom the entire information technology industry in Europe will be endangered and this happened and no one was aware of it because the paradigm shift has occurred.

Today, we are seeing the same situation in India. How the liberalisation framework has completely changed the whole game. How the industries should be organised, what should be the product mix, what should be the method of management ? All that takes place. So these are extremely strategic issues and this is going to happen more and more in the mental world. This is entirely the knowledge world, the products are now knowledge. The products are not material products, but the products are not bale products because we see that bales are being created by the company who started back yard, the largest bales are being created, many of them including Vodak or including Novel.

I think in the information technology industry one never had capital one simply had ideas and how to deploy these ideas into the real world. So this is the power of information. This is the information warfare. And of course this warfare is much more as we go on to the real war itself and this will play extremely critical role in the future. But please do not misunderstand, I think the nation should not understand that warfare is only the warfare in the conventional sense. We are talking of economic warfare, we are talking of knowledge warfare, we are talking of technological warfare.

Technological warfare the way Japan fights today by, I think, breaking the patents, what patent information comes to them that information is given to the industries in different way as I understand from many many books. The Japanese file the patents earlier than that and they protect their industries, and today, as you go to to WTO, and the patent information, you trap the knowledge itself and do not allow anybody to really leverage on that knowledge by trapping. I won't call it trap, but lock it before others.

This is the world we are creating. These are the conflicts we are creating in the tomorrow's world. And tomorrow's products are all information products, because they are biological products, bio-technological products, or material products. And even in the new materials which are totally based on the mano-technology, is based on total intelligence totally. They are simulated on computers created on computers with design properties.

So this is the goal and this is much more so as the whole world gets connected. I think today we are talking about ten or six million computers connected on the Internet and I think at least hundred million or sixty million computers connected on the Internet going to 100 million very soon. Where the world becomes totally connected. The net work becomes very very powerful and this whole thing is information pro and the economic activities occurring, knowledge activities occurring, distribution activities occurring, trading activities occurring on the net. And you can completely manipulate the people on the net itself. Manipulate the knowledge of the people. Let us talk about that the dis-propaganda done by very venerated magazines like Readers Digest etc. and very many people who believe what they read but which are not realities. We know that they are not the realities, the way Westerners are projecting India in the media. There are so many jokes about India on the net. We can see how pathetic and how funny they are.

So this is the world we are living in and I think we have to dwell on.

But this is the warfare and if you look at it, I feel that eventually the societies must understand the warfare in a much larger sense than warfare against - at the level of - we can talk in terms of the good and evil. We will have to have the spiritual upliftment. How do we annihilate the warfare within ourselves itself and how do we evolve the future societies and the future beings. That is the question of warfare and that will occur only through information and knowledge and that is why our thing - we could look at many many things - the path of Dnyanayoga or this talk of - that you create the information in your mind and what is the purpose of it and you change your very existence itself.

And I was dwelling on the concept of what Guru Nanak said sometime back that the NAM itself - or Namdeo said, many many people in India talked about it and they have said the name itself is the reality. The God is name itself. That is information itself is God. In a certain sense you talk about the knowledge of that. It is not the physical existence or it is not something else, that name itself and you get your liberation done only through that, the main concept of knowledge and information.

So this is the broader concept as I perceive it on the warfare side. And I am sure there are lot of people here who would enlighten you and there will be lot of discussion on this very new concept of information warfare which is very very important. And we will learn from this seminar. And I wish to congratulate and thank - it is a privilege for me to get associated with this seminar this morning and also providing me one opportunity to learn on this new term.

Thank you indeed.

Air Marshal Kulkarni:-

I would now request Group Captain Apte to speak on the Electronic Warfare. Group Captain Apte was a Technical Officer with the Indian Air Force. He has spent 28 years in the Air Force. He was associated with Electronic Warfare even while in the Air Force. After he left the Service, he was first with the Hindustan Cables and thereafter Member (Technical) with the Air port Authority of India. He has rich experience in this field and recently he spoke to members of our Centre on the Future Air Navigation Systems. I will now request Group Captain Apte to give his presentation on Electronic Warfare.

SESSION I

ELECTRONIC WARFARE

Main Speaker : Gp.Capt(Retd) G.M. Apte

(PAPER PRESENTED BY GP CAPT (RETD) G.M. APTE)

FROM 'HARD KILL' TO 'SOFT KILL' ON THE BATTLEFIELD

Homo sapiens set themselves apart from all other species in the animal kingdom because of their two distinguishing qualities. One is their ability to make and use tools, which includes weapons! The other is to organize into large groups, consisting of many thousands of individuals and use these weapons to wage wars against similar large groups of their own species ! Over the years, technological advances created a formidable array of weapons to choose from and, no wonder, soon the weapons themselves became targets, thus bringing in counter-weapons. With the sword came the shield, with the lance, the armour. With battleships came submarines and with aircraft, anti aircraft artillery. ABMs followed ICBMs and so on.

As the weapons became more complex, the emphasis during military conflict shifted from sheer muscle to tactics and precise control over weapons ; activities connected with mental power, the power of information processing ! War fever, which results in the human endocrine system preparing a person for 'fight or flight', diverting blood from the brain to the extremities, soon became a handicap and it became necessary to train modern combatants to keep cool and fight. Information Age had already arrived on the scene much longer ago than we tend to assume!

When Maxwell postulated the presence of Electromagnetic Waves composed of no matter but just oscillations of Electrostatic and Electrromagnetic fields, travelling at the speed of light in a medium of nothingness called Ether, it was thought of bordering on philosophy. An important milestone in the development of technology was reached decades later when Hertz demonstrated that the Electromagnetic waves predicted by Maxwell could in fact be produced at will. Little would Hertz have realized then the dramatic metamorphosis that this ability was to bring into our lives in times of peace as well as war. Electromagnetic radiation or EMR gave armed forces a global reach and that too at the fastest possible speed for information transfer, the speed of light! Logically, therefore, the initial use of Electromagnetic radiation was in Radio for the vital command and control communication with troops. Subsequently came the radio beacons to facilitate air navigation. Radar followed soon, providing effective surveillance of air space over land and sea. Armed forces became far more potent with EMR. Consequently, it was realized that interfering with the usage of EMR by the enemy was bound to give rich dividends. Thus was born a new form of warfare termed Electronic Warfare, or EW, in which armed forces strive to deny effective use of EMR by the enemy while ensuring its use for themselves. Very soon, application of Electronics no longer remained restricted to the transmission or reception of Electromagnetic waves but enveloped all the areas of control of machines and processing of information. Thus EW also enlarged in its scope, encompassing all activities for denial of effective use of Electronics (and not only EMR) by the enemy and its effective use by own forces.

The advent of Electronic Warfare brought in the concept of neutralizing hostile weapon systems through 'Soft Kill', a process which disables the weapon systems without physically damaging them, by interfering with the communication of information or with the internal processing of information. Thus, much before Information Technology came into being as a full fledged scientific discipline, information transmission and processing systems had already become a vital target system to be neutralized during war !

ELECTRONIC WARFARE BASICS

Electronic Countermeasures, or ECM, aim to deny the enemy effective use of Electronics. This is the offensive arm of Electronic Warfare. Electronic Counter-Countermeasures, or ECCM, ensure effective operation of our own Electronic systems even in an ECM environment, and hence represent the Defensive arm of Electronic Warfare for effective deployment of ECM in a tactical situation, it is necessary to know the characteristics of electromagnetic emissions emanating from hostile weapon systems such as radar. The EW systems which enable us to obtain such information are termed Eléctronic Support Measures or ESM. These form the Tactical Reconnaissance arm of Electronic Warfare. The information collected by ESM is normally for immediate use in the battle field, and modern ECM systems are automatically programmed on the basis of such information. There is however a need for in-depth probing of hostile systems in the longer term, even during peacetime, to be able to understand the behavior of each weapon system under various conditions realistically and thus to model the weapon system. The act of collecting such intelligence which leads to Modeling or Thumb-printing, is called Electronic Intelligence, or ELINT and is the Strategic Reconnaissance arm of Electronic Warfare. ELINT enables our forces to gain vital information on enemy's or potential enemy's Electronic Order of Battle.

Here a distinction needs to be made between ELINT and Signals Intelligence or SIGINT. The term SIGINT denotes intelligence activities conducted by eavesdropping on enemy telecommunications. The aim is not only to obtain parameters of hostile electronic systems but to gain information on all aspects of enmey's organization, order of battle, preparedness, operational procedures and so on which is then fed as an input component of the overall Military Intelligence apparatus. There could however be some commonality of hardware used for the purpose of ELINT and SIGINT.

ECM systems may or may not involve active transmission of Electromagnetic waves. If they do, they fall into the category of Active ECM, else they are termed Passive ECM. A large cloud of chaff deployed to create clutter on the radar scope to obliterate aircraft echo is an example of passive ECM while noise jamming of radio communications or radar is active ECM. Both active and passive ECMs are divided into two broad categories, which are Jamming and Deception. Both the examples of ECM just given fall under Jamming. Characteristic feature of Jamming is that the operator (or the processing function) of the victim weapon system generally becomes aware that the system is under the attack of an ECM. This is also termed 'Brute Force' ECM. The other category is 'Deception' which is far more subtle. When a known voice is perfectly imitated on a communication channel, the victim remains unaware of the presence of ECM. Or when an aircraft-like but fictitious echo is created on the radar screen, the operator is misled. That's deception. Deception is a highly economical weapon. It requires far less Radio Frequency Power and does not evoke retaliatory response as the enemy is not alerted. Deployment of deception however requires a more thorough knowledge of the targeted system.

ECCM may consist of an electronic circuit which gives a radar some measure of immunity against certain known ECM. Or may consist of hopping of the operating frequency of a communication link according to a predetermined secret sequence. There can be countermeasures against ECCM, which would become ECCCM or EC^{3}M and so on. We can thus think of a generic EC^{n}M!

BATTLE OF WITS

Consider the following scenario. A pilot on a bombing mission reaches the target area known to be protected by a radar controlled anti aircraft gun. The gunner acquires his target i.e. the aircraft and establishes a track, which is the electronic process in which a window in the form of a 'range gate' is set around the aircraft. In the meantime, the pilot fires a rapid deployment chaff cartridge. In a matter of milliseconds the aircraft has around it a cloud of tiny metal foils. Chaff cloud enhances the echo of the aircraft at the gun radar by many orders of magnitude. The chaff thus captures the Automatic Gain Control (AGC) circuitry of the radar receiver and thereafter, the gun actually tracks the chaff and not the aircraft. A few more tens of milliseconds later the chaff decelerates sufficiently while the aircraft forges ahead free of the chaff cloud and also free of the tracking by radar. The ECM has won the first round, or has it ? The high grade computer circuitry of the radar receiver however notices that the target (which actually is the chaff) has suddenly decelerated far faster than about 8 or 9 g which by far is the limit even for a trained pilot to withstand. The computer thus realizes that what it is tracking now is not a manned vechicle and could be an ECM. The computer looks at the history, picks up the instant of commencement of this sudden deceleration, disregards the track beyond this point and extrapolates the possible location of the aircraft from the immediate earlier history. This would enable the radar to pick up the aircraft again in a matter of a second or so and the ECCM capability of the weapon system would win the day! But may not be so! The pilot being well trained, jinks, that is takes a turn immediately after firing the chaff cartridge and after a while returns to his previous heading thus creating an off set between his actual course and the course the gun computer would recreate from historical information. The radar in this situation is unable to re-establish track on the aircraft. The pilot's maneuver, which in fact was an Electronic Counter Counter Counter Measure (EC^{3}M), won the day!

The above example tells us two important points. The first is, the weapons of electronic warfare may not necessarily be 'electronic' in nature. Thus, the pilots dodging maneuver is a physical activity but forms a weapon of electronic warfare. The second, and more important, fact that the example brings out is, like in any form of warfare, EW is a continuously played game of wits! He who deploys his available EW resources, whether offensive or defensive, in the right amount at the right place at the right time, wins!

PACKAGING OF EW HARDWARE

Manufacturers of EW hardware package it into systems that suit the platform of their deployment. Thus airborne suites are packaged according to their role and according to whether they are to be installed on transport aircraft, fighters or helicopters. All aircraft which are likely to be exposed to hostile weapon systems are provided with a light weight Self Protection EW suite which is most often carried internally. It consists of an ESM in the form of a 'set-on' receiver, which senses hostile radiation and programs an ECM package. The latter may be a chaff dispenser, an infrared flare dispenser, a low power jamming transmitter, an active deception device or a combination of two or more of these. Often the ESM system holds a library of information on hostile systems collected earlier through ELINT. In a formation of strike aircraft, some aircraft are specifically tasked to provide ECM suppression for the whole formation. Jammer transmitters in this case are more powerful, hence heavier and are carried in Pods as external stores. Podded configuration gives the Commander flexibility in allocating EW resources according to the threat preception of each mission. A very high degree of coordination is essential between strike aircraft and their EW escorts, therefore they are required to train together constantly during exercises in peacetime. ELINT function is carried out by highly specialized aircraft with high service ceiling, long endurance and highly accurate navigation systems.

In modern battlefield, EW is extensively used by all, Army, Navy and Air Force. The needs and priorities of each service are different. The choice of EW systems, their platforms and deployment philosophy depends on the particular application. Safeguarding own telecommunications while degrading enemy's communications has a very high priority for the Army in the battlefield. The highest priority for a Naval task force at sea is to conceal its location from the enemy at all times, hence Electronic Emission Security (which falls into the category of ECCM) assumes top priority. For an Air Force strike mission, countering gun and missile control radars and missile homing systems comes at high priority. Commanders are expected to utilize the EW resources placed at their disposal just as other weapons. The universally accepted Principles of War are applicable to Electronic Warfare as well. Of these, selection and maintenances of aim, concentration of force, economy of action and surprise are by far the most relevant to EW.

EMERGENCE OF ELECTRO-OPTICS IN THE BATTLEFIELD

The advent, in their solid state incarnation of three basic optical devices viz, the Laser, the Photo-diode and the Light

Emitting Diode (LED), has opened up a whole new range of electro-optical systems to make weapon systems more potent during the last three decades. In their wake, these have generated Electro-Optical Countermeasures (EOCM) and Counter-Countermeasures (EOCCM). Lasers are now used in the battlefield to mark targets and to obtain accurate range information. Systems on board aircraft use optical sensors to seek the marked targets and attack these with Laser guided weapons. As a defence against such a weapon, aerosol sprays are deployed around tanks at crucial phases of battle, to attenuate laser radiation and thus to serve as a passive EOCM. Alternatively Decoy Lasers can be deployed in the battlefield to misguide weapons providing Deception EOCM. Encoding of the marking laser signal is then resorted to as an EOCCM to make the marked target seeking system immune to such deception. And so the battle of wits continues in the Optical domain too!

Radiation from a laser is in the form of coherent electromagnetic waves, just as the signal from a radar, the difference being only in the wavelength. Hence deployment of EOCM and EOCCM is treated as a part of Electronic Warfare.

COMMAND CONTROL COMMUNICATION AS PRIME TARGETS

Electromagnetic Waves have given Commanders global reach, while high grade computing power has substantially extended their information processing power. The result of these developments is centralization of real-time battle control in Command & Control Centres, with their associated Communication networks. The resultant C^3I (Command, Control, Communications, Intelligence) apparatus has become a vital arm of war. Because of this very reason it has become a target system for suppression, with a priority higher than that for the actual wherewithal of war namely ships, tanks, gun positions, aircraft etc. Since C^{3}I depends very heavily on electronics (for information processing and for communication), what better weapon to use for suppression than EW or 'Soft Kill' ?

ELECTRONIC WARFARE IN THE SPACE AGE

Electromagnetic Waves exhibit different propagation characteristics in different regions of the frequency spectrum. However most of the important usage of EM Waves in Military applications, such as radar, microwave and space communication, air-ground communication and satellite navigation, takes place in the parts of the spectrum where EM Waves travel in straight lines. Curvature of the Earth thereofore restricts the use of ECMs only within the line-of-sight or radio horizon. As if to get over this handicap, Space technology has opened up the possibility of deploying ECM resources on satellites, geo-stationary as well as those in Earth orbits. Line-of-sight condition in this case is always available as long as the victim receiver is within the footprint of the satellite. Satellite is reasonably safe since attacking a satellite needs considerable planning, long gestation period and huge expense! Jamming from space can thus be considered as a Stand-off operation. Since a geo-stationary satellite subtends a constant elevation with respect to a ground based target system such as radar, a 'null' can set in modern radars to cancel the effect of jamming. Orbiting satellites on the other hand provide excellent opportunities to jam ground based targets at different and changing azimuths and elevations and from much closer distances (a few hundred km as opposed to about 35000 km in case of geo-stationary satellites). However the deployment of the ECM from Earth orbiting satellites is most productive only in certain favourable time slots. Space based systems can be effectively utilized for ESM, ELINT and SIGINT purposes during peace time as well and are believed to be already being used extensively by Space-capable nations! Space based ECM is a true strategic weapon of war as it can be brought to bear in theatre of war under centralized control from the Earth!

OPERATIONS WITHIN NOISE : THE NEW APPROACH

Those who deploy ECM, aim to achieve highest possible Jammer to Signal Ratio (JSR) of Radio Frequency (RF) power at the input to the victim receiver. And traditionally, the aim of the designers of communication networks and radars was to ensure that highest possible Signal to Noise Ratio (SNR) was attained at the receiver input by increasing the transmitter output as much as possible. (The term Noise in this case includes the jamming interference as well as any unintentional RF noise). High power radars and communication transmitters were in demand. Technology has of late reversed the trend. Advances in high speed digital techniques and solid state microwave transmitting devices have brought in a wholly new breed of radars and communication systems which operate at low powers ! Low power solid state radars transmit low power, coded pulses of long duration which are compressed after reception using matched filter techniques. This operation results in target detection even when noise predominates over the signal at the receiver input. In modern communication systems, signal in digitized form is mixed with pseudo-random digital sequences and such signal artificially spread over a bandwidth significantly larger than the original bandwidth is transmitted at low RF power, to be received correctly even in the presence of stronger noise, again by using matched filter technique. The race for deployment of higher power has thus been replaced by a race for superior ('smarter') tools for Information Processing!

ARTIFICIAL INTELLIGENCE PROVIDES A POWERFUL TOOL FOR EW

Progress in the field of Artificial Intelligence (AI) has come in very handy as a very powerful tool in many areas of EW. Modeling of hostile weapon systems is one such area. AI is particularly useful in SIGINT operations as well. Electronic systems today enable eavesdropping on literally several tens of thousands of speech circuits operating over Microwave Links, Satellite Links, UHF/VHF/HF radio and so on and so forth round the clock and round the year. The vast amount of tapes thus recorded have to be heard, so as to separate wheat from chaff. Highly trained humans are needed to understand the import of the on going conversation. The raw data generated is so vast and continuously accumulating day in and day out that no nation, however populous, can afford to train and deploy human power sufficient to do the task. Advances made by AI in Speech recognition and Language Understanding are of great help in making the task somewhat practical!

DEVELOPMENT AND PRODUCTION OF EW HARDWARE

Manufacturers of Weapon Systems are the ones who are in the best position to develop ECMs against their own weapons! For obvious reasons they do not indulge in this activity. In the post World War II years, international industries specializing in the manufacture and marketing of EW hardware sprang up all over the developed world. One of their important markets is the developing countries who do not have their own EW industry. The main risk in procuring equipment from these manufacturers is the lack of confidence in the equipment's efficacy against potentially hostile weapon systems, in the absence of 'EW Ranges', analogous to Firing Ranges. Further, the manufacturers' own Governments impose restrictions on exports of certain systems, or certain features of systems such as programmability, based on political and strategic considerations. Self-reliance is therefore not a rhetoric but utter necessity as far as EW hardware is concerned! A strong R&D base, establishment of simulation laboratories, proving ranges and a close interaction between defence forces and indigenous industry are the essential milestones in the journey towards self reliance.

CONCLUSION

With their superior intellect, humans over the ages created weapons and counter weapons. Ability to generate Electromagnetic Waves and the emergence of Electronic devices gave Commanders the ability to communicate with troops over large distances, process information fast and control operations remotely. Superiority in the battlefield depended on the ability to exploit electronics! Electronics became the target. Electronics for Information Transmission and Information Processing. This new target could be neutralized by 'Soft Kill', without the need for physical destruction. In their wake Countermeasures brought Counter-Countermeasures and so on, developing into Electronic Warfare. The new target system and the new soft weapons are the hallmarks of Electronic Warfare. These concepts, originating with EW around the time of World War II, were destined to grow in tandem with the galloping strides in the new field of Information Technology in a matter of a few decades and usher in the era of the War of Minds!

QUESTIONS / ANSWERS - GROUP CAPTAIN APTE'S TALK

Q.1 Is IAF using the satellites ? What's the role of Space Technology in EW ? How is a nuclear explosion sensed ?

A.1 There are two questions. One is specific about Indian Air Force which I am unable to answer.

Regarding space technology, I would like to convert it into a general question. The question was what part space technology is playing in the electronic warfare. The biggest handicap for electronic warfare is the line of sight. To jam a radar or to deceive a radar, you need a line of sight of that radar. Generally, except for HF, I am talking in a very general sense. Even for communication in micro wave link, you have to be in line of sight.

You get out of shackles of this line of sight the moment you have a resource in space. Space based ECMs and space based ESMs is a new vista altogether which is opened up with space technology. And therefore any country which has got its own resource in space will be foolish not to have ECM resource also in space. ESM resource in space. But this is something which is not made known to anyone. I would also not like to know what Indian Air Force is doing.

But no country would like to let out what actually is being placed there. But anyone who owns a satellite in space will have something that which can be controlled from ground and which can pick up what cannot be picked up otherwise, unless you go very close to the target to establish line of sight. Because there are side lobes from the radar and the satellites also. All are not geo-stationary and there are orbiting satellites which come at different elevations. So they can pick up radar emanations which go at the lower elevations also not at the side lobes but even main lobes. So even main lobe can be picked up.

But here by sending a satellite in space we are achieving the same. The space technology has changed the nature of the way in which you play electronic warfare and space resources are very useful.

Now the second question was about how intelligence is obtained on nuclear explosion. Now this is not very easy. There are many indications of a preparation for a nuclear explosion and those are the things which are put together and finally a conclusion will be arrived at that there has been experiment or plan for experiment. This is something physical on the ground. Something that comes as acoustic waves which are because of vibrations. Something which comes out as EMP, electro magnetic pulse which is associated with nuclear explosion. This is different area that EMP itself affects electronic system and therefore nowadays avionics is being made EMP hardened.

You need to harden electronics against that. You might have heard in the eighties. In the early eighties when a Tornado aircraft was lost over Germany and during investigation it was found that because it was flown above a high power HF transmitting station. It flew over that and the fly by wire system went hay wire and the control was lost and aircraft was destroyed, which was unintentional.

But radiation can do damage at a length and similarly the EMP also can be perceived at a distance, can destroy things too. But you have a liaison and the liaison can pick up the electro magnetic pulse which is associated with nuclear explosion. It is not associated with other explosions and that can come up even if the explosion is underground. That EMP can reach an object in space also. It can be picked up. So I do not know on what basis they have arrived at this conclusion. But it is a combination of so many things which must have made them to conclude that it was a nuclear explosion.

Q.2 Can the GPS accuracy be degraded ?

A.2 There are orthogonal codes which I mentioned. The signal is spread. The spread system technology is used in GPS. Now a satellite operates on two codes. One is a coarse acquisition code the other is a precision code. A coarse acquisition code is given to the whole world. That gives you a certain level of accuracy. Over that some inaccuracies are imposed by deceiving the clock. The clock which is an automatic clock on board the GPS satellite is made to dither. That gives error in your calculation and the other is ephemeris, the almanac of the satellite also is modified so that inaccuracies are introduced. These are two inaccuracies, out of that the dithering of the clock, can be removed if you create your own clock and synchronise it.

But this is an impracticable solution. Can't have it on each aircraft. The ephemeral inaccuracies can be corrected if you have your own system to track the GPS consulates. It has to be tracked very accurately and it has to be tracked by systems placed around the globe. And we do not have such systems around the globe. United States has. At Digo-Garcia they have, at Philippines they have sensors. In their own mainland they have sensors. But they have a reach around the globe. If we create a reach around the globe, yes it is possible to correct those errors which they introduce in the almanac.

Precision code is not made accessible. So that limits the accuracy again and it is not easy to break that code because it is a digital code, as I mentioned earlier. Having our own satellite, yes, that is the right solution and in that direction only we are going. Either our own satellite or having satellites owned by the world community. Civilian navigation satellites. So that is the direction in which the world is going.

Q.3 Should EMP cause any worry to us ?

A.3 This is what I mentioned as EMC. It creates a ripple in that section and then it becomes quiet. Electro magnetic spectrum does get affected and it results in a pulse. The pulse contains all frequencies. Just a single pulse in time domain is equivalent to having all frequencies from zero to infinity. So it will create interference in your radio set. It will create interference in your TV. It will create interference in all gadgets, on all frequencies. But that happens only just at that time. It does not remain. It dies down. It dies down in space. That is not a phenomenon which will bug us for ever.

The other parts are far more devastating. The radiation part. Physical devastation is far more than the devastation due to electro magnetic pulse. EMPs will affect the weapon systems in that area. Aircraft get affected and that is the worry. Nuclear weapon may get affected. Not the aircraft which were used in Second World War. Because today's aircrafts are dependent on electronics. They have to fly by wire and the more we are dependent, the more we become vulnerable. So from that point of view EMP is a worry for defence. But otherwise there is no need to worry. It won't affect the general public and not for any length of time. It lasts a few macro seconds.

THE STATE OF INFORMATION TECHNOLOGY TO DATE

Main Speaker : Dr.D.P. Bobde

(PAPER PRESENTED BY DR. D.P. BOBDE)

INFORMATION REVOLUTION - THE THIRD WAVE

Information Technology is the major technological development to grab imagination of the world today. This is likely to bring unbelievable changes in the way we live, think and transact our business.

According to Alvin Toffler humanity has undegone two major waves of changes. Each one of them had so much effect on the culture and civilization that it was inconceivable to the earlier generation. The first wave of change - Agricultural revolution - lasted for thousands of years. The second wave - Industrial revolution - took about 300 years and had similar effect on the society. Today history is more accelerative. It is likely that the third wave sweeps across the history and completes itself in a few decades. This is often termed as Information Wave, Electronic Era or Global Village.

GROWTH OF INFORMATION TECHNOLOGY

Though computer technology is the backbone of Information wave the revolutionary effect started when Personal Computers (PC) arrived.

IBM introduced PCXT, based on Intel 8088 micro processor chip in 1983. The processor speed was 4.77 MHz and the hard disk capacity was 10 MB. During the following year PCAT, based on 80286 chip was introduced. It had 6 MHz speed and the hard disk capacity was 20 MB. The next powerful PC, the 25 MHz, 80386 based PC was first introduced by Compac in 1986. Soon IBM and other clones followed. With this the power of Desktop became comparable with Mainframe. The hard disk capacity increased up to 300 MB. A couple of years later, 80486 based PC arrived with clock speed of 30 MHz increasing gradually to 80 MHz. Finally in 1995 Intel introduced its Pentium chip. Thus within a span of 12 years from 1983 to 1995 the processing speed increased steadily from 4.7 MHz (for 8088) to 120 MHz (for Pentium). The number of discrete devices packed into the chip (packing density) increased by many fold. 8088 had half a million devices while the pentium chip has about 3.5 million discrete devices packed into it. The hard disk capacity increased from 10 MB to few GB. The main memory also increased from few KB to more than 100 MB. The overall processing power has been doubling almost every 18 months.

THESE TECHNOLOGICAL BREAKTHROUGHS HAD THREE DISTINCT EFFECTS

- Computers became smaller in size
- Computers became powerful
- Computers became cheaper.

The shrinking size have changed computers from desk top to lap top to palm top. Power requirement also reduced. Computer became very convenient to handle.

PC which was initially considered as hobbyists' toy soon became an essential working tool. It quickly proliferated to variety of applications in business, education, R&D and defence.

ROLE OF NIC IN IT REVOLUTION IN INDIA

NIC is a decision support organisation of Government of India. Its main objective is to provide complete informatics services to Government and Government related organizations. Its activities are spread over areas such as CAD, GIS, Operation Research, Teletext, Customs & Excise Computerisation, Passport office, Immigration office Computerisation, RBI Currency Chest Operations etc. It has developed a few thousand databases in various subjects. In order to meet its object, NIC set up a computer communication network known as NICNET.

NICNET was set up in 1987, it has evolved over the time into a unique network of its type in the world. The network has about 1000 VSATs installed. There is no single VSAT which can meet the requirements of all sections of users. NIC being a total solution (Internet and Intranet) providing organization, it can not continue with single type of VSAT. The network has been upgraded to support a variety of VSATs namely CDMA, TDMA, FTDMA, SCPC, DAMA and receive only VSATs. The network uses state-of-the art technology in C-Band as well as Ku-Band. NIC has been pioneer in judiciously selecting latest and proven technology and making them operatinal in Indian conditions. For this purpose, NIC has large in-house R&D setup and it has patented a few products developed in-house.

NICNET has now been operational for over 10 years and has become an integral part of a large number of Government and Corporate organisations. It links all the District Headquarters, States/Union Territory capitals and the National Capital.

NICNET operates a low speed network using C-band transporder on INSAT 1-D, with a Master Earth Station hub using a 13 meter antenna in the heart of Delhi, and about 1000 Micro Earth Stations (Very Small Aperture Terminals-VSATs) connected to Intel-based PCs. NICNET facility vertically and horizontally, integrates the Indian Government at the Central and State levels, as well as the District Administrations.

NICNET INFO HIGHWAY

NIC has successfully operated its low-speed satellite-based, computer-communication Network since 1987. The capability and versatility of the network was successfully demonstrated for a variety of major applications including Result Processing and Dissemination for the General Elections and Assembly Election since 1991. The system has become an integral part for administration and monitoring of activities. The network also supports several Closed User Groups (CUG) for Steel Authority of India Ltd., Indian Farmers Fertilizer Co-operative Ltd., Central Excise, etc. Several users and organisations have also approached NIC for use of NICNET to connect their geographically distributed offices in the country.

With the increasing use of the network by both the Government and other organisations, the demand for data bandwidth has been gradually increasing. To meet this ever-increasing data transmission requirement NIC has established a powerful information highway.

As a part of this information highway, the network connects and provides services to several economically and commercially important cities/towns in the country. NICNET Info Highway, supports high speed communication, at 1 Mbps at each of the remote sites. It has the capacity to increase the speeds at selected nodes upto 2 Mbps without any major investment. Each remote station uses a 1.8/2.4 meter antenna. In addition, the remote stations have the necessary interfaces to support both synchronous circuits. Customers are able to directly dial into the system to access the services available on the network. The remote stations could be configured locally or from the Master Earth Station. These remote stations provide operational as well as monitoring information to the network control centre.

The Network Control Centre (NCC) has a Star Network Management System (SNMS) to monitor the network. The management software provides graphical information about all the links and also facilitates operations control at the remote sites.

INRERNATIONAL CONNECTIVITY

NICNET has been connected to the International Networks, through the Gateway Packet Switching System (GPSS) of Videsh Sanchar Nigam Ltd. Through this linkage, the network accesses several X.25 networks in the world. In particular it has been accessing the MEDLARS (MEDIcal Literature Analysis and Retrieval System) database located at the National Library of Medicine, Washington D.C., U.S.A. It also provides its users with international mail facility and the large number of public domain softwares available on UUNET.

To cater to many international needs NICNET has acquired another highspeed connection. It is connected to transit gateway of SPRINT at New York at 64 Kbps. This data link is in addition to the already existing gateway connection to GPSS. This increases the reliability and response time for NICNET users when they access international data networks. With the present gateway connections, NICNET users have access to almost any data network in the world. At present these connections are interfaced using X.25 protocols. NIC is converting NICNET into an Intranet. The present NICNET diagram is given in FIg-1.

NICNET, VALUE ADDED SERVICES

NIC provides total solution including networking services, value added services, Intranet solutions. NIC at present provides the following services :

1. Interactive communication for remote login, database access.

2. Sharing of expensive hardware/software resources available at a central place.

3. E-mail : NIC offers X-400 and smtp/uucp mail services. NIC has already set up a number of E-mail servers all over the country.

4. EDI : NIC provides EDI following EDIFACT standards.

5. Full range of Internet Services : NICNET is the class-B network of Internet. It has several hundred servers and created large number of home pages for different organizations. NIC facilitates Home Page Authoring and Content Hosting. It has a special division to handle such applications.

6. Video Conferencing and Multimedia Application : NIC has 6 studio based video conferencing centres at six major cities of the country. Delhi centre can have multi site conference with 4 cities at a time. Each studio can take about 10 persons at a time.

7. In addition, NIC has set up desktop video conferencing at 20 places and this number is being increased to 100 very soon.

8. Databases : NICNET supports several hundred databases on various subjects such as census, industries, educational institutions.

9. GIS : Geographical information system developed by NIC is used for district planning.

10. Emergency Communications : NICNET has also been used for emergency communication. When Earthquake struck Latur and Osmanabad districts of Maharashtra NIC shifted one truck mounted Mobile Earth Station with built in power supply to Omergaon and the NICNET node was made operational from there within 24 hours. When other means of communicatins were paralysed NICNET was working and helping the Government to overcome the crisis.

QUESTIONS / ANSWERS - DR.BOBADE'S TALK

Q.1 Do our MP's use the system ?

A.1 Well I think there we have done something for parliament. We have put a server in parliament, and that system is called parlies system. You can access that system right from our office here. That system stores all the questions asked so far - not the current questions but if somebody wants any reference to old question it is completely available and many MLAs and MPs, they make use of that facility. But current questions, it takes time. We get the exact text and we sort it out and put it on computer. So it has its own cycle. So it is effectively working for all the past questions, but not current questions.

Q.2 Is it true that MP's have been given PC's ?

A.2 True. See it again all depends on individuals. There are some MPs who are effectively using it. You know there is a scheme under the Government of India that is called MP Lad Scheme which is called MP's Local Area Development Scheme under which one crore is given to every MP for local area development. They have been given lap top by the Department of Electronics. So every MP has a lap top today and there are some MPs who come and ring me up and ask, see I want to access using that lap top. Through our network they access various avenues. I have mentioned to you, the MP Dr.Jichkar in Nagpur. He has been extensively using it. And he has used that MP Lad scheme for introducing internet access for children. So it all depends on how you use it. What is your attitude. May be in case of many MPs, these lap tops are lying with their children and grand children. We do not know. So, it again depends on individual. But there are people who are using it also and slowly we hope it will change.

Q.3 Is NICNET accessible to all ?

A.3 Well, It is easier to access the NIC NET now. Because we are connected to Internet. It is available to any network which is connected to Internet. We are service providers to Government sector in the country. Therefore all service provided to private sector is given by VSNL. But Government offices and public sector we handle. I think that is the advantage of internet. Earlier NICNET was not able to talk to Urnet educational research network. This network was not then there. There were dozens of networks in the country but they were not able to talk to each other. But today the internetters are the backbone. Those who are allowed to go to internet. I think everybody, everybody can talk. Through our e-mail, for example, I send my mail to my son in IIT Bombay. It goes via internet. It goes all the way to internet and comes back to Bombay. But this is available. This is a matter of minutes and seconds. It goes. But it is available. We have sites. You see our home page. There is a parliament home page. You see the Indian constitution - all those things are available today.

Q.4 Do you generate information ?

A.4 That is another problem. See we are only custodians. We do not generate information. I will tell you an example. When we developed website here in Pune, we had written letters to all ministries of the State saying that if you want we are prepared to give a home page for you. You give information. I have not got it from any department so far. Nobody wants to give information. What do I do ? But there are some exceptions. Let me give an example. PWD had a global tender for the eight lane highway between Poona and Bombay. But they wanted to do it. So we suggested, you put it on our web site. Of course they were expecting lot of quotations from international bidders and all that. So we said you put it. Anybody can access and you publish it in newspapers also. And then they did it and then they could get a lot of response through our network. So as far as technically it is not a problem at all and those departments who can technically understand it, they will give it also. Problem comes when you do not want to give information relating to your department.. So it is very difficult to get information.

Q.5 Is it possible to maintain secrecy ?

A.5 The first question that you wanted was whether such kind of encryption was possible. Yes. It is possible but then you have to do it for yourself. Nobody can develop encryption for you because it will be known to me and once it is known to a second person, it will go to the third and fourth. So technically yes, but you have to have your R&D wing and develop that software and a code which cannot be broken down, and there are such things available. Banking is done on network. You see the people use it. If there is anything, you know, people can draw millions and millions of dollars and that could be danagerous. But it does not happen. So it is a very proven technology. But then you have to have your own encryption and decryption.

Q.6 Do we have the expertise ?

A.6 Yes, we have that expertise. See our biggest advantage in this country is that we have a lot of programmers. English knowing programmers. If you see in USA also many companies have employed Indians and they are doing wonderful jobs in very big companies. So it should be possible. Only thing you know because of security, see now we have a satellite based network. Anything which is broadcast by satellite is open information. Anybody can receive it and use it. But then as was mentioned earlier that you have coded in multiplicity but we are using that kind of thing in our network and then the company which has supplied us that, knows the code. They can definitely decode it. But otherwise you have to have similar set up and you have to know the code and everything and then only one can decipher it.

Q.7 What is the secrecy of the Web page ?

A.7 But why do you need to know secrecy of web page ? Web page is something you want to publicly open it. That is the most visible part of your activity. That is open information. After all if you want we can put it on websight. I do not think, I mean there is a problem in putting a web page for any department. But of course the information should be such that people should access it and use it. You just cannot put anything and then keep it a secret. See this security is from the point of view of what I think is no hacker should get into it and spoil your information. So there are what is called fire balls. You put it around your information so that people cannot get into your site and could spoil your information and change it. Those kind of technologies are also available.

SESSION III

INFORMATION WARFARE

Main Speakers : Dr G.S. Mani
Sqn Ldr(Retd) Ajay`Singh

(PAPERS PRESENTED BY DR. G.S. MANI AND SQN LDR AJAY SINGH)

DR.G.S.MANI

INTRODUCTION

A study of the evolution of conflict clearly indicates how military tactics and doctrine have always been dominated by the most potent weapon available at that time. If bows and arrows influenced strategies in resolving conflicts among warring groups in pre historic days, horses and elephants took their role in the days of kings and emperors. Similarly, later centuries witnessed emergence of battleships, aircrafts, and missiles as important tools influencing conduct of warfare. Today, when the world is on the brink of "Information Explosion", it is natural to expect that each warring group tries to use all the potency of information to their best advantage in the future battlefield. See Figure 2.

POTENCY OF INFORMATION

Information has always played a key role in the activities of society. Whereas transparency of information is considered a virtue in an open society, confidentiality of information is very essential during times of war. There are certain basic features of information, which are unique and deserve special attention. These are :-

Non zero sum value : Algebraically, assets or inputs to a system are represented by + ve sign and liabilities or outputs by-ve sign. If assets exceed liabilities, one stands to gain ; otherwise it is considered to be a losing situation. Using Algebra, one cansay that if X is the money with person A, who after giving away money Y is left with Z, then $z = x - y$ or $x - (y+z) = 0$. However,in case of information, even if some portion of information is given to others, one is not left with less information. Thus, the law of non zero sum is not applicable ;in other words, information can be given away and still be retained.

Knowledge about others information : By the same law, it is difficult to know which information is known to others. Special efforts have to be put in, if one has to find out about information known to others.

Stealing of Information : Again, on the same basis, it is also difficult to know if information has been stolen.

Easy distribution : With modern Information Technology tools, information is easily distributable across the globe at low cost. However, it is worth noting that distribution of information need not necessarily be synonymous with high technology. A classic example is the way in which certain types of rumours, especially scandals involving VIPs spread fast mainly through word of mouth.

Information Technology (IT) : Information technology can be defined in simple terms as the Science of Information accessing, handling, transfering and storing. Key vehicles involved are communication and computer systems. Newer dimensions have been added to these technologies based on recent advances in miniaturisation, networking and intelligent software. Figure 3 gives a schematic representation of the key aspects involved in Information Technology. Photonics, Satellite linkages and High Definition TV have added sophistication and elegance to IT, making it globally accessible.

The inherent virtues of information together with technology driven features have increased its importance in the likely future warfare. To quote US Director of Central Intelligence John M Deutch "We have evidence that a number of countries around the world are developing the doctrine, strategies and tools to conduct Information attacks."

FIRST MOVES TOWARDS INFORMATION WARFARE

The three drivers of Information warfare or INFOWAR are :-

(a) Superior understanding abilities
(b) Better discrimination, and,
(c) Customization

Superior understandig abilities : As advances in understanding of complex systems are increasing through computer based information processing, it is becoming easier to analyse and to target on to those sub-components of a complex system which play key roles. Just as the modern doctor has hot tools today to diagnose, identify and surgically operate much inside the human body, without even looking at it directly, it is possible to identify the most critical node of the enemy's defence system and attack it through electronic means. In fact, this kind of analytical capability exists today at many levels ; mechanical, economic, military and even social.

Better Discrimination : Increasing memory power and process capabilities have made it possible to achieve much better resolution than even before. It is simply the question of "more bits for better resolution". This capability of discrimination or the ability to focus on smaller and smaller components and get more intricate and pin pointed information becomes the foundation of the techniques of INFOWAR.

CUSTOMIZATION : In the past, mass production and low cost were intimately interconnected. But, the modern digital technologies and process control mechanisms have made it possible to achieve customization at low cost. Technologies which were not easily approachable earlier due to large distances have now become accessible through the IT tools operating at the speed-of-light. Thus, now it is possible to integrate these technologies together to develop customized products - products which are not only unique, but also are becoming cost-effective compared to the mass productionised items. Indications of mass production giving way to customization are clearly visible.

What all these mean, is probably the end of the all-purpose-mighty weapons, large volumes of high-cost war equipment, and heavy dependence on massive troops. We are moving towards highly customized, one-off tools against very specific, small but very important system or sub system. Thus, the role of sledge hammer is being taken by a delicate tweezer in the future battlefield scenario.

FURTHER MOVES INTO SOPHISTICATION

The purpose of war is to bring about behavioural changes in society. And the best war brings this change through minimum loss of men and materials and probably even without firing a shot.

In this context, INFOWAR will mean "influencing and changing what adversary believes and what adversary knows."

INFLUENCING BEHAVIOUR OF SOCIETY : Bringing about changes in the behaviour of society with specific reference to the adversary's society - means manipulation of their knowledge systems and their belief systems. Most actions and decisions taken by leaders of a society (interchangeably used in the place of nation) are based on what they know of or probably what they believe or think they know. Knowledge systems are based on observations, which are possible to be verified. They are not easy to be influenced or manipulated. On the other hand, belief systems need not be based on facts. Often they are individualistic in nature, and can be influenced through personal or collective consciousness. However, both systems can be targeted in Information warfare.

The techniques for influencing adversary's societal behaviour depends on manipulation of ideas, Information and finally even the reality. All these techniques can use modern IT tools very effectively.

Manipulation of ideas : Newspapers, magazines, video and TV have been the media through which ideas get formed in large bases of population, and affect their behaviour and attitude. In recent years we have witnessed how images are built or destroyed through these media. Build up of massive demonstration against nuclear warfare, environmental pollution and even abortion have been possible only through the idea manipulation campaigns. However it is worth noting that the modern technology such as cyberspace can been used to orchestrate and manipulate ideas in such ways as to spark new behavioural change in society. All this can be achieved through targeting almost the complete globe simultaneously with the goals set to be achieved in short time.

MANIPULATION OF INFORMATION : Whereas manipulation of ideas requires subtle implementation, manipulation of information can be more direct. This is one step ahead of the political campaigns or advertisement commercials in vogue now. It is envisaged that more powerful methods of subliminal communication would be available in near future wherein information targeting an unwitting public could be inserted into the news and entertainment media.

MANIPULATION OF ACTIVITY : At one time photographic images were taken to be proof of authenticity of information. Now with the kind of sophistication available in the image processing field, it is becoming increasingly hard to determine what really represents truth. Thus, truth which was intrinsically associated with this information medium is no longer valid. Also, the ability to manipulate reality has been advancing fast. Invention of cine moves was probably a first step in the "make-believe" direction, to which public was introduced a few decades ago. 3-D Holography and Laser imaging are technology areas of high sophistication through which manipulation of reality is possible in the coming millennium. At that time, it may be possible for all of us to "see" an object and swear of its physical presence, even if our intelligence inhibits this possibility.

Information warfare can be conceived to be in two modes - Reactive and Proactive. The reactive mode would focus attention on influencing public opinion through media influences, psychological campaigns and diplomacy measures. A pro-active or direct mode of operation would be through manipulation of electronic data bases, means of banking, trade or finance and even ATC, IFF and the like. Whereas the first is a long term mode, the latter may yield quick results.

TECHNOLOGY TOOLS AND MEANS OF INFOWAR

The goals of Infowar can be summarized under "Theft, modification or destruction of Information". The technology tools through which this war may be fought can be categorized under computer virus counter measures (CVCMs), sniffers, chippers and HPM devices. See Figure 4.

Computer - virus Countermeasures (CVCM) : Recent years have demonstrated that computer viruses are not only feasible, but can cause catastrophic disruption. Since most military systems are tending to become computer-based, the vulnerability of such systems to CVCM is a reality. Just as biological viruses can infect and affect functioning of biological systems, computer viruses can infect software in C^4I systems and propagate through connected networks. They can spread rapidly and can cause damage which often are difficult to eradicate. Surprisingly, the amount of programming code required for generating computer viruses is so small that many of them go undetected during early stages. As time passes, they spread through the network causing far-reaching and catastrophic effects on the victims, including loss of information, data and even software. In a tactical warfare setting, such CVCM could have a prolonged and devastating effect not only on military targets, but also on other important business and financial sectors. Technologically advanced societies, where most of the activities such as transfer of economic assets, on-line banking and shopping are through computer networks, are more prone to such countermeasures.

A major problem however is injection of CVCM into a system. Advanced military C^4I and weapon systems can be targeted through data or control links. In weapon control and guidance systems it may be possible to insert CVCM into the main antenna after suitably masking it as a credible signal. Sometimes, indirect coupling of viruses can be through maintenance and diagnostic tools. It has also been reported that computer virus guns, capable of remotely injecting viruses into enemy's computer system are already available. Such an approach, if deployed to penetrate on-board computers on a tactical jet aircraft, can cause obvious damages.

Several operational scenarios for deployment of CVCM are possible. One of them, more commonly known as Trojan Horse Scenario, makes the virus lie dormant upto a pre-assigned time or event, when it starts acting on the vital components of the target. Such an approach leaves the victim totally unsuspecting till it is detected, and helpless after detection. It is also possible to design the virus so that it can navigate itself for a specific piece of data or information and then transmit it back to specific location. This would allow deceptive exploitation of the critical data. The overload scenario on the other hand is based on uncontrolled malignant growth, which apart from slowing down the vital operations of the computer can also affect data management system. In networking environment, the virus can also be made to announce its presence, forcing the user to disconnect a part of the network for fear of spreading. In short, CVCMs seem to be very potent tools made possible through the advances in IT techniques.

Sniffers : These were originally designed to analyse and diagnose problems within a network. However, it is possible to use them to access secret codes and pass words. Passive sniffers, or current probes can be used for monitoring network activities while remaining extremely difficult to detect.

Chipping : This refers to the practice by which microscopic internal circuitry can be reworked by deliberate injection of virus.

Sometimes referred as Infobombs or Knowledgeable robots, they can navigate through cyberspace, target a specific chip and make it useless. Alternatively, the chip can be constructed to cease functioning when a specific set of commands is inputed.

HPM Devices : These are guns which can focus a narrow beam of high radio frequency energy towards the weak link of an enemy's electronic device. The target can be a microprocessor or other critical components and devices used in a tactical weapon. The vulnerable devices can be diodes in receivers or low power MOS logic chips or even semiconductors used in electronic ignition systems. Table I shows the single pulse fluence level and their likely effect. About 1-10 microjoules of energy when concertrated on an area of 1 sq. cm can cause bit errors which can result in catastrophic effects. This requires generation of power levels of the order of 10 GW within reasonable volume and weight limitations. Generally the sophistication of HPM devices are expected to be much less compared to conventional Electronic Warfare jamming devices but power levels will be large by many orders. Figure 5 shows conceptual domain of HPM and EW devices. The HPM devices can take many active roles such as Suppression of Enemy Air Defences (SEAD), disrupting enemy communication and platform self protection against air-to-air or surface-to-air missiles. Also weapons capable of delivering explosively driven narrow band pulse over a large target area, burning out the sensitive electronics within the radar receivers can be developed using HPM devices.

NEXT GENERATION WARFARE

It is impossible to predict the future, but all directions point towards a warfare which is closely associated with computer-mediated forms of communication. Information being the most potent medium, warfare based on manipulation of information will necessarily form part of the overall strategy. However, such information warfare will have no front lines, since strategic targets will lie every where. In fact, the situation may be so complex that it may even be difficult to know who is under attack by whom, or who is in charge of the attack. Spread of misinformation will dramatically complitcate all efforts in implementing conventional security measures. Means required to deploy mechanisms to achieve success in this senario will be less costly, since these will be mostly software intensive. Moreover, the complete warfare may be clean with no blood shed, with microwave and photon replacing the bullet and the missile.

While most of the aforementioned techniques and weapons of Information warfare seem to be futuristic, it seems to be true that Western world is serious in its efforts in establishing base for this new approach. In 1995, sixteen Infowar officers passed out of the National Defence University at Washington. They have been specially trained to counter-attack computer systems. Also, development of virulent strains of computer viruses is being carried out by US National Security Agency which are capable of remaining dormant till a predetermined time after which they can cause havoc. High power electromagnetic pulse generators fitted in suit case sized enclosures are being developed at Los Alamos National Laboratory. Hughes is expected to deliver a HPMSEAD weapon which can be deployed in 1999 on an aircraft over a target at a stand-off distance. However, in South Eastern Asian region, where communication and computer networking has not grown to the level of sophistication as in the West, Information Warfare is not expected to be an immediate threat.

SQN LDR (RETD) AJAY SINGH

The employment of high technology in the Persian Gulf War made it perhaps the first war in which information, as well as misinformation created a unique impact on the conduct of conventional armed operations. It elevated the status of information from being a raw material for intelligence to a level where it is now being accepted as a tool, or even a new medium for war fighting. The lessons learned from the Gulf War have led to a reorganisation in US armed forces. More specifically, these lessons also set into motion a conception that the nature of war was undergoing radical changes due to increasing use of the frontiers of technology such as computers and satellites in actual conduct of battle. The Tofflerian theory of 'three waves of warfate' gave further impetus to the idea that war would be fought on a different plane altogether involving exploitation of the information spectrum and the term 'information warfare' was coined to express this new form of warfare. Formalised by the Tofflers, Information warfare has become the latest buzzword in the Pentagon with some referring to it as a revolution in military affairs. The US Army has adapted itself to thses changes through a process of change called Force XXI, the efforts of which are evident on three axes : digitisation, force development, and redesign of the future Army.

THE NATURE OF INFORMATION WARFARE

As the US forges ahead with plans to fight a new kind of war in the twenty-first century, it may be useful to examine the concepts of information warfare. Information warfare, simply put, is war in the information spectrum. It involves all actions taken to exploit the information spectrum while denying its use to the enemy. Naturally, safeguarding the spectrum for one's own use constitutes an important part in the information war. Conceptually, it is akin to the conduct of electronic warfare that we know as war in the electromagnetic spectrum or air power in the medium of aerospace. Information warfare involves much more than electronic warfare since information activities extend beyond the realms of the electromagnetic spectrum. The main aim of information warfare is targeting the human mind of the enemy, by denying, degrading, delaying, disrupting, or manipulating the flow of information to it. Starved of the right information at the right time, the enemy would be forced to take incorrect decisions leading to inadequate action or even no action at all.

Information warfare as a concept is not new. Strategists such as Sun Tzu had spoken of the importance of knowing the enemy and one's self centuries ago in order to defeat an opponent's strategy before battle was joined physically. What is new is the seamless and integrated approach to the conduct of the information (or misinformation) campaign that has been taken to new dimensions by the advances in microprocessor and data transmission technology. In other words, it is a system of systems; a roof over concepts that have existed for some time. Information warfare should be seen as encompassing and integrating the activities of electronic warfare, psychological warfare and intelligence operations. The overall concept of information warfare can be seen as having three parts :-

Set of information warfare elements i.e., techniques and capabilities (which have mostly been available).

Comprehensive strategy for application of these elements.

Target and objectives.

The last two are representative of the difference in information warfare and earlier forms of warfare such as electronic warfare where only information was the target but not so much as part of a strategy of targeting the decision process.

TARGET MODEL FOR INFORMATION WARFARE

From these three parts, we can derive a generic model for information warfare, which is layered :-

Sensor attacks against physical elements that generate information.

Link attacks against the elements involved in the management of information.

Decision process attacks against the elements and process that interprets and uses the information.

METHODS OF INFORMATION WARFARE

Information warfare can be conducted both against a country's military forces as well as its society. Although the objectives of information warfare are same, the methods differ somewhat in these cases. Against the military, information warfare could primarily consist of :-

- Command and control (C2) warfare

- Electronic warfare (EW)

- Intelligence-based warfare (IBW)

Against society, the methods used may be :-

- Info-economic warfare

- Cyberwar.

Psychological warfare and computer hacking operations would be common features in war against the military or society.

The forces for conduct of information operations may be drawn upon from the military or civilian information technology experts. In fact with increasing manpower base in the IT (information technology) industry worldwide, one may expect greater civilian participation in the future information warfare landscape.

C2 warfare consists of attacks against the enemy's ability to generate commands, and hence is directed at the leadership and its ability to direct/control or the leadership and its links to the field. The specific targets within the C2 network would require an analysis before deciding on a particular approach. The leadership of a highly centralised C2 structure is likely to be more vulnerable, an example of which was witnessed in the recent Persian Gulf conflict. If, however, the enemy decentralises the C2 structure, C2 warfare may not yield the desired results easily due to the collateral channels being available. The important issue to look at would be the information flow channels in the C2 structure, since use of networked computers, cellular communications etc. would diffuse the command centres insofar as information requirements are concerned, and thereby reduce their vulnerability to C2 warfare. If the information flow is based on a non-hierarchical systems, the ability of C2 warfare to interfere with the command and control functions would be severely curtailed. A non-hierarchical system is one, which would allow data transfer directly from the dissemination agency to the user without the need to traverse intermediary nodes. Some data would still have to follow hierarchical channels, but this could be kept at a low and non-critical value. Therefore, the method to conduct information warfare through C2 warfare, would necessarily involve the identification of information flow channels of the adversary, assessment of its vulnerability to anti-C2 operations, while designing one's own C2 system on a non-hierarchical basis to safeguard the system against the enemy's C2 operations.

Electronic warfare reached prominence in the Second World War, but the techniques and equipment were refined further in the years which followed. It became a recognised fact that the ability to interfere with the enemy's electronic systems while safeguarding one's own gave a side the decisive edge in warfare. EW is a set of actions taken to deny the use of the electronic spectrum to hostile forces while retaining the ability to use it oneself. What this effectively means is to deny, degrade, delay or disrupt information to the enemy in order to create an inadequate or false picture, which in turn is manifested in an incorrect action on the part of the enemy. EW therefore, must also be seen as a subset of information warfare, since the objectives of EW are derived from the aims of information warfare. Anti-data flow operations are likely to see an increase in the area. The important aspect to identify would be the strengths and vulnerabilities of one's data flow architecture as well as that of the enemy in order to plan and prosecute effective EW operations within the aims of information warfare.

A crucial component in the conduct of information warfare is the availability of intelligence data. The quest to see the other side of the hill has always been present in the minds of military planners and technology has moved to fulfil this requirement. Advances in satellite technology and imagery systems has made available reconnaissance and surveillance capabilities for some time now. The incomplete link has been the dissemination of the data to the end-user in a short time-frame. It is now possible to integrate sensors, emitters and processors into a reconnaissance, surveillance, target acquisition (RSTA) and battle damage assessment (BDA) system. This facilitates intelligence-based warfare (IBW) as one of the methods of information warfare. Reconnaissance and surveillance functions are moving into the realms of omni-sensorial capabilities, that includes the collection and fusion of data through infrared, ultraviolet, seismic, visual, auditory, olfactory spectra besides others to give information which can be used to conduct information warfare operations. The manifestation of IBW was witnessed in the Persian Gulf conflict in 1991, in which JSTARS aircraft were employed to give real time data for conducting precision strikes. In the future, smaller and more powerful computers as well as sensors will permit the deployment of tactical intelligence systems on a much larger scale. These will be fed from space, air, and offshore and ground sensors through appropriate filtering and cueing systems. Psychological warfare operations can be directed against the military and/or society. When employed against the military, it could be in the form of anti-commander or anti-troop measures. The information media are used to create a sense of despondency and hopelessness amongst the military forces when engaged in battle or preparing for it. Although these operations have been carried out since centuries, there is a shift towards greater usage of the electronic media like the television, which is readily available to most at least in the preparatory phases. Even during times of peace information warfare through psychological warfare operations can be used with great effect against the society, especially so in a democracy where the opinion of the masses can be shaped by exploitation of the media. This phenomenon is also popularly known as the CNN factor. If the leadership of the adversary can be made to believe that war may result in international sanctions, no domestic support, destruction of the economy or defeat of the military forces, they are less likely to indulge in following a course of action that could lead to direct confrontation. Since the target of information warfare is the mind, it is natural that psychological warfare is a key method of conducting information warfare. From mass propaganda practised earlier, however, technology has allowed customised propaganda to be conducted. This entails targeting key personalities in vital decision making positions by collection of their psychological profile data and influencing them in various subtle ways. While the idea is not new, computers give the capability to collate data from multiple sources such as credit card purchases to after-dinner speeches. Additionally, the advent of DTH broadcasting, which will have about 500 channels, makes customised propaganda a feasible proposition. It is possible to target policy makers and policy shapers in a country by collecting data regarding their public statements and writings and then classify each into categories which would assist in assessing their responses to situations and proposals, something which was not practicable even two decades ago. It should also be recognised that, the more one uses the information media, the more is one vulnerable to the effects of information warfare.

Computer hacking operations is a term used to refer to the employment of techniques to destroy, degrade, exploit or compromise information systems both military and civilian. One of the prime weapons of hackerwar is the use of computer virus by insertion through a telephone line. The fact that the hacker may be sitting thousands of miles away does not make things easier for defence against this method of information warfare. All that is required to neutralise or degrade a sophisticated military computer network is another computer and a telephone line with a person behind it with sufficient perseverance and knowledge. While the actual warfighting computers may be secure, most of the others, which deal with crucial areas such as manpower and spare parts, may be linked to low security telephone channels, and are thus open to hacking operations. It is believed (by Pentagon experts) that the military's computers in the US are probed 500 times a day of which only 25 are detected and 2-3 reported to security officials. The toughest Pentagon computer to crack is supposed to be the first one after which nearly 90% of the other computers linked to the first one would recognise the intruder as legitimate. If hackers achieve such a capability, it will not be long before we witness the growth of professional, mercenary hackers who would work for the highest bidder. During the Persian Gulf conflict, according to Pentagon officials, a group of Dutch hackers offered to disrupt the US military deployment to the Middle East for as low as $1 million. Saddam Hussein did not accept!

Besides inserting viruses in computer networks, hackerwar could be conducted by intelligence agencies, some of which are considering insertion of microbes into the computer systems of potential adversaries, which would eat the electronic systems in order to degrade the computer system for a prolonged time period. Though the hackerwar picture looks rather dismal, in reality it may not be so. It is believed that computer systems can be guarded against hackers with more assurance than other systems can be guarded against physical violence. The point to remember would be that, physical attacks constitute the last instrument of state policy and therefore, by necessity would be infrequent as compared to hacking operations, which are not constrained to the same extent. Another issue requiring thought is that, hackers may be operating independently, without sanction of the state, which is a disturbing possibility.

Info-economic warfare is manipulating the banks and stock markets to ruin a country's economy through organised hacking operations by another country. War in cyberspace, or the world of computers is another method of information warfare, but one, which is a distant reality. Cyberwar, borders on science fiction, where info-warriors are expected to enter into combat in the net and virtual wars replace physical wars. The first step is using virtual reality used in simulation techniques to possibly create illusions or images of 'virtual troops' advancing on a particular approach while the 'real troops' follow another route and come in undetected.

IMPLICATIONS OF THE INFORMATION WAR

Information warfare as a concept is still at a nascent stage and the ideas relating to information warfare are still evolving. There is a new focus on the missions of the military forces, which in turn has an effect on their equipment, doctrine and training. An issue, which merits thought, is the role information warfare will play in shaping the military's force structure. The question basically is whether the need for 'conventional' forces as we know them today would reduce if the war will be decided in the information spectrum. The answer is not simple, as a number of factors have to be considered. The determinants will include the level of sophistication and availability of own information warfare capabilities versus the pereceived adversary. Another issue which needs attention is identification of the challenges and opportunities that the developed and developing countries face in the information warfare scenario and how best to cope with them working within the embryonic stage which exists today.

Developed nations, notably the US, are moving towards integrating information warfare as part of their war fighting doctrines. For their military forces, this means faster transition through the information technology revolution. There is no doubt the technology will be absorbed without major problems, but the crucial point is the time it will take for information warfare doctrine to fructify into one that can be used to fight a war. Developing countries, which do not have an advanced information technology base, will be in no position to lay down elaborate information warfare doctrines to fight full-scale information wars. It is, however, important for them to understand information warfare as it gives an opportunity for relatively small, weak and under-equipped military forces (in the conventional sense) to upset more advanced countries through intrusion of their information systems. This requires, as a first step, computer literacy at least in their military forces, in order to stay abreast of the developments in this core field of information warfare. Secondly, efforts should be made to develop technologies that serve to infiltrate into the information systems of other countries and give adequate capability to cause damage.

QUESTION & ANSWERS - THIRD SESSION

Question 1. Do we have the capability to wage such a War ?

Answer 1 by Dr.Mani - Unfortunately, I think the wherewithal to answer this does not exist. I am not here as a government spokesman. However, I think the way I do look at things is Indian scenario. As rightly pointed out by Ajay, we should have an offensive policy which is much better as far as this aspect is concerned. And I personally believe the capability for taking on an offensive role is available with you. The software techniques are available in country. What is required here is brainware. I think brainware is sufficiently large in our country. We have to think of unconventional methods. Of course we have always been thinking in terms of unconventional methods and I think this is our strong point. But coming to the defensive, I think there is nothing much to defend. We are really not net-working here,It is not much to be talked about, unlike in USA. USA must definitely talk about it. They are definitely much more vulnerable than our country.

Q.2 Is there any agency which looks at this in a comprehensive manner?

A.2 By Dr.Bobade - I don't think there is any agency to my knowledge which is looking into it in a comprehensive manner. But you are absolutely right that management of information is a major challenge for the government. How do you manage information that is readily available?. We have to learn the methods of management. I think it is a very complex situation which has to be addressed. At the moment I do not think anybody can do it.

CLOSING REMARKS

SHRI RAM PRADHAN

Ladies & Gentlemen. I am aware that we have passed the normal lunch time for most of us and I do not wish to make any long speech. But I thank the presence in the hall of so many of you. I think this is the biggest audience that the Centre for Advanced Strategic Studies has attracted so far. It shows not only your interest, but the subject itself and those who have participated in the subject. And I would like to first thank all of you for coming here and participating. I have just a couple of observations to make.

In the Centre for Advanced Strategic Studies, we have been examining various issues relating to different areas, and, relating to various economic and other situations. But we decided to go and become somewhat modern or forward looking and this subject was chosen from that point of view. And I think today's discussion has shown that if we have to look ahead, this is the subject which requires greater attention. As I think Dr. Mani has rightly said, we may have war but we may not have any physical war. He was talking in general terms. There will be limited physical wars. They will continue. But real warfare is going to be how to ċapture the minds of men and women. And this is going to be a universal problem.

In the old days it was said that the wars are born in the minds of men. I think it has something very substantial. Of course in the Centre for Advanced Strategic Studies perhaps we may have greater attention to warfare in the traditional sense what we call warfare, but really warfare is to be seen in the wider context and again I am referring to Dr. Mani. It is a kind of social warfare. Warfare for ideas, warfare for manipulation of reality, manipulation of information. I think he hit very correctly on those three words to describe the situation.

And I just want to mention two things which have happened in last two or three days which show that both nationally and internationally this information technology is being used.

Only four days back, I think the President of China, delivered his address to their National Assembly. Commenting on that, yesterday or day before yesterday, there was a piece as to which direction China is taking. And the commentator said, ' you know it is like a cavalcade. Clinton, Yeltsin and the President of China were going in a cavalcade. Clinton turned right. President Yeltsin's cavalcade follows. He turns right. And when the President of China is approaching the square, he asked his guide, philosopher and God, Deng. Deng you are not there, what do I do ? He said, show the signal to the left but go right. So this is shaping the minds of the whole nation. Show a signal in one direction but do what is in the interest of the nation.

Second example was yesterday's Clinton's speech in the United Nations. I think that speech is a speech for the next century and I think it was very wisely crafted and drafted speech. I have been in the UN myself for several years and have never heard the Chief of the State speaking. So I think yesterday's speech was crafted to address it to the next century and the American power and the American interest and the whole emphasis was how to capture the minds of men all over the globe.He did not talk in terms of normal warfare and issues like that.

So I am only suggesting that this requires some kind of study and attention even in the Centre for Strategic Studies.

Now before I end, I must thank Dr.Bhatkar who inaugurated the seminar, Dr.Bobade, Group Captain Apte and the last two speakers who always get squeezed for time - Dr.Mani and young Sqn.Ldr. Ajay Singh. And here we have a real problem.

Normally, when we started, our activities were spread over in two sessions. One before lunch and one after lunch. But we found, after lunch it becomes a bit difficult for people to focus or concentrate and therefore we decided to extend little bit into the lunch hour and try to finish. But I think there is one suggestion which Air Marshal Pratap Rao has made and which I wanted to also articulate.

Now that we have discussed this subject, and the subject is going to be for the future, we should try to break it up into various components.

I think some suggestions have been made by the young Sqn.Ldr. Ajay Singh and we should try to see as to how we can organise workshops to really bite into these issues and I think that is one of the points which comes when you talk of strategy. It is not merely talking in general terms.

And finally I must thank Air Marshal Kulkarni, the Director and Group Captain Chitnis, who are really carrying on the Centre and who have done an excellent organisational work.

Ladies & Gentlemen I thank you again and declare that today's seminar is closed.

Thank you.

INFORMATION WARFARE

SEMINAR : 24TH SEPTEMBER, 1997

(Venue : Shivaji Sabhagruha, Pune University)

LIST FO PARTICIPANTS

1.	Shri RD Pradhan	- CASS
2.	Air Mshl (Retd) YV Malse	- CASS
3.	Air Mshl (Retd) S. Kulkarni	- CASS
4.	Gp Capt (Retd) SG Chitnis	- CASS
5.	Gp Capt (Retd) GM Apte	- CASS
6.	Shri VL Date	- CASS
7.	Shri BG Joshi	- CASS
8.	Maj Gen (Retd) KS Pendse	- CASS
9.	Shri MK Ranade	- CASS
10.	Shri DJ Sathe	- CASS
11.	Air Mshl (Retd) Pratap Rao	- CASS
12.	Shri Sangram Sawant	- CASS
13.	Ms. Pillai S. Deepak	- CASS
14.	Ms. Ashwini Patil	- CASS
15.	Ms. Snehal A. Masurkar	- CASS
16.	Ms. Arpana A. Abraham	- CASS
17.	Wg Cdr (Retd) SD Karnik	- CASS
18.	Cmde (Retd) B. Karpe	- CASS
19.	Mrs. Bharati B. Karpe	- CASS
20.	Dr. Pramod A. Paranjape	- CASS
21.	Gp Capt (Retd) HK Kaushal	- CASS
22.	Amit Sepaha	- CASS /T
23.	Shri RD Misal	- CASS /T
24.	Lt Akash Kapur	- CASS /T

25.	Wg Cdr S Dev Gupta	- CASS /T
26.	Col R. Bhardwaj	- CASS /E
27.	Maj Raghavendra Sharma	- CASS /E
28.	Maj Keshv Aswal	- CASS /E
29.	Maj NG Railkar	- CASS /E
30.	Maj Sreesh Kumar	- CASS /E
31.	Lt Col PK Sharma	- CASS /E
32.	Lt Col D. Banarjee	- CASS /TS
33.	Maj NCS Grewal	- CASS /TS
34.	Maj DS Bhati	- CASS /TS
35.	Maj AK Sinha	- CASS /TS
36.	Maj Gautam Deb	- CASS /TS
37.	Maj Satish Raj	- CASS /TS & D
38.	Dr. DP Bobde	- Direct NIC, Pune
39.	Sqn Ldr (Retd) Ajay Singh	- Delhi
40.	Dr. G.S. Mani	- Dean &rector, IAT
41.	Dr. Vijay Bhatkar	- Direct C-DAC, Pune
42.	Col KK Sharma	-
43.	Lt Col JS Bhamdare	-
44.	Lt Col HA Dalvi	-
45.	Gp Capt DN Ganesh	-
46.	Gp Capt MM Sharma	-
47.	Shri Rajeev Upadhye	-
48.	Shri BG Deshpande	-
49.	Col (Retd) YG Tambay	-
50.	Prof C. Ramakrishna	-
51.	Sqn Ldr P. Kulshrestha	-
52.	Sqn Ldr RN Jayasinha	-
53.	Flt Lt S. Philip	-
54.	Maj JS Yadav	-
55.	Maj PK Mehta	-
56.	Maj Virendra Singh	-
57.	Maj R. Deshmukh	-

58.	Maj HS Shanbag	-
59.	Maj AP Rao	-
60.	Lt Col DN Asija	-
61.	Maj JS Pansodkar	-
62.	Maj BPJS Bal	-
63.	Lt Col Gurinder Singh	-
64.	Lt Col BK Paliwal	-
65.	Maj Abhaya Raj Sharma	-
66.	Shri Rakesh Upadhyay	-
67.	Lt Cdr (Retd) SV Taskar	-
68.	Lt Cdr M. Chaturvedi	-
69.	Cdr Alok Bansal	-
70.	Lt Col S Kosili	-
71.	Wg Cdr (Retd) AT Thakur	-
72.	Flt Lt NP Praveen	-
73.	Shri D. Gangopadhyaya	-
74.	Flt Lt A. Srivastav	- IAF
75.	Fg Offr Ramesh Gupta	- IAF
76.	Flt Lt J. Venkatesh	- IAF
77.	Shri AN Chaudhary	- IAT
78.	Flt Lt NS Mohan Kumar	- IAF
79.	Flt Lt M. Panzing	- IAF
80.	Gp Capt (Retd) MG Vadgaokar	-
81.	Flt Lt S. Chaki	- AFIS
82.	Flt Lt MK Chopra	- AFIS
83.	Sqn Ldr AK Sakha	- AFIS
84.	Sqn Ldr Shri Krishan	- AFIS
85.	Flt Lt BS Bajwa	- AFIS
86.	Sqn Ldr JM Joshi	- AFIS
87.	Sqn Ldr AU Khan	- AFIS
88.	Sqn Ldr KA Kiran	- AFIS
89.	Flt Lt R. Ranjan	- AFIS
90.	Flt Lt MY Phatak	- AFIS

91.	Plt Offr C. Majumdar	- AFIS
92.	Plt Offr SM Manoharan	- AFIS
93.	Plt Offr VN Rao	- AFIS
94.	Flt Lt DN Roy	- AFIS
95.	Capt S. Bhattacharya	- AFIS
96.	Maj Gurinder Singh	- INF
97.	Maj SS Voltra	- INF
98	Lt Cdr R. Shukla	- MINTS
99.	Cdr KP Shashidharan	- MINTS
100.	Cdr N. Bhuri	- MINTS
101.	Maj M. Ravi	- MINTS
102.	Flt Lt KV Sant Babu	-
103.	Brig (Retd) SD Parab	-
104.	Shri Suhas Kadam	-
105.	Lt Col Pritam Singh	- Southern Command
106.	Col BA Patil	- HQ, Southern Command
107.	Ms. Pallavi Deshpande	- DDSS, Pune University
108.	Shri Rahul V. Patil	-
109.	Ms. Rajashree Nighojakar	-
110.	Shri Rahul H. Joshi	-
111.	Shri Prasad P. Rane	-
112.	Shri A. Krishnan	-

FLUENCE: MEASURE OF TIME-INTEGRATED POWER DENSITY

SINGLE PULSE FLUENCE LEVEL	LIKELY EFFECT
10^{-8} mJ/ CM^2	BURNS OUT DETECTOR DIODE WHEN COUPLED TO 3 METER ANTENNA
10^{-4} - 10^{-5} mJ/ CM^2	CAUSES BIT ERRORS IN UNSHIELDED COMPUTERS
0.04 mJ/ CM^2	CAN INDUCE " MW HEARING" IN HUMANS
100 mJ/ CM^2	CAN AFFECT NERVOUS SYSTEM
20 - 100 mJ/ CM^2	CAUSES HEATING EFFECT ON TISSUES

NOTE: mJ IS milli Joules

TABLE 1

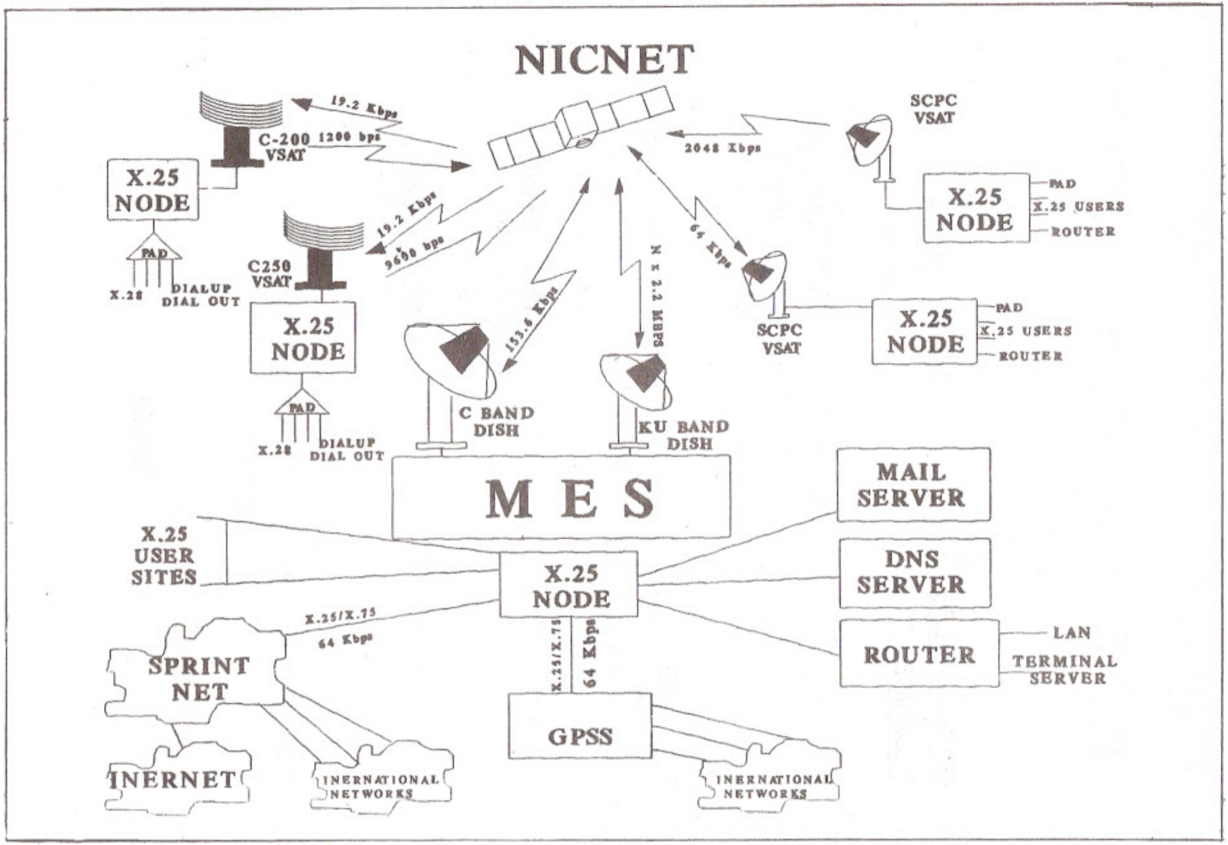
NICNET
19.2 Kbps
C-200 1200 bps
VSAT
X.25 NODE
PAD
X.28
DIALUP
DIAL OUT
19.2 Kbps
9600 bps
C250
VSAT
X.25 NODE
PAD
X.28
DIALUP
DIAL OUT
153.6 Kbps
N x 2.2 MBPS
64 Kbps
2048 Kbps
SCPC
VSAT
X.25 NODE
PAD
X.25 USERS
ROUTER
SCPC
VSAT
X.25 NODE
PAD
X.25 USERS
ROUTER
C BAND
DISH
KU BAND
DISH
M E S
MAIL
SERVER
DNS
SERVER
ROUTER
LAN
TERMINAL
SERVER
X.25
USER
SITES
X.25 NODE
X.25/X.75
64 Kbps
SPRINT
NET
X.25/X.75
64 Kbps
GPSS
INERNET
INERNATIONAL
NETWORKS
INERNATIONAL
NETWORKS

Fig- 1

" WARS THROUGH AGES HAVE DEPENDED ON MOST POTENT WEAPON AVAILABLE AT THAT TIME"

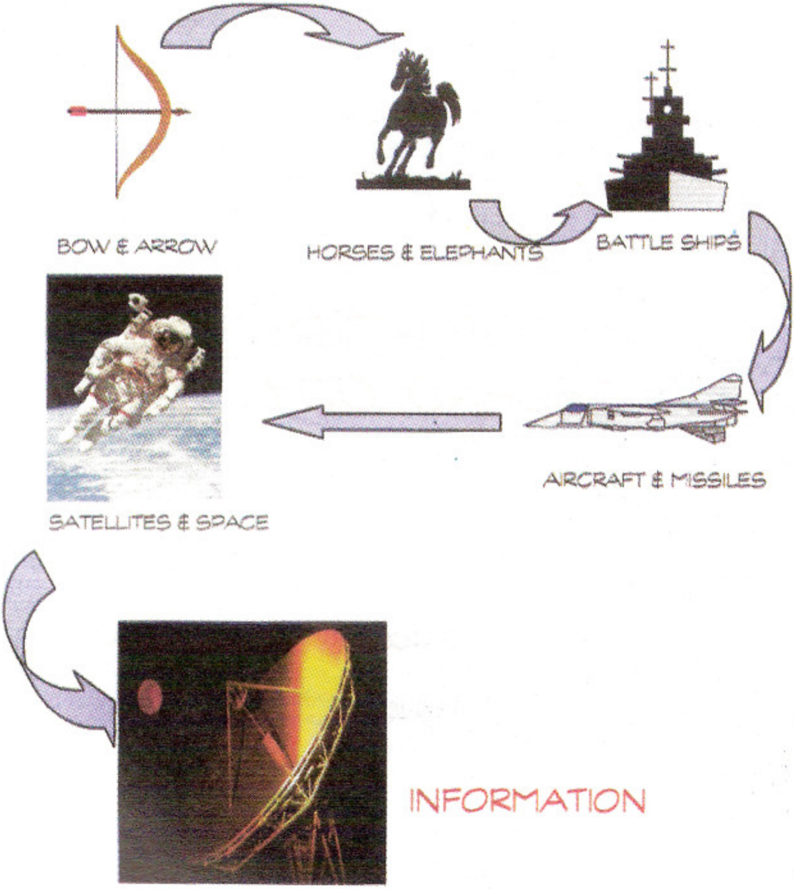

Figure 2

ELEMENTS OF INFORMATION TECHNOLOGY

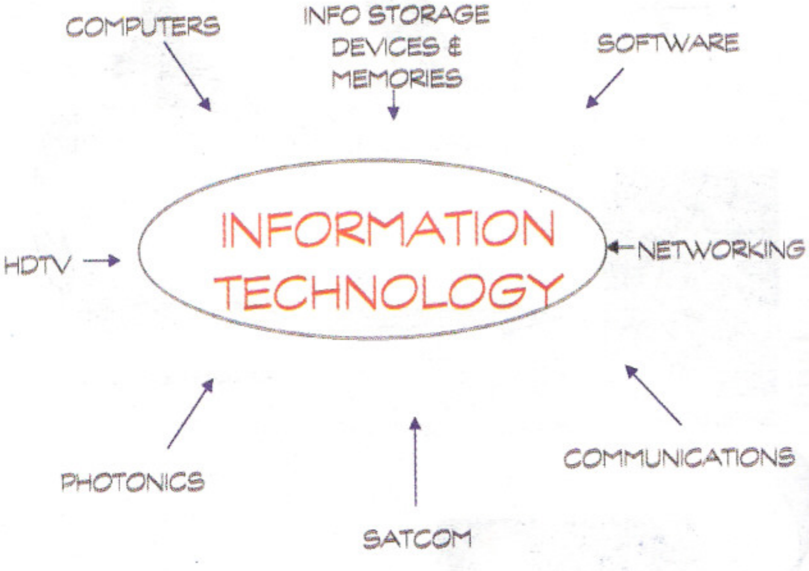

FIGURE 3

TOOLS, MEANS & GOALS OF INFOWAR

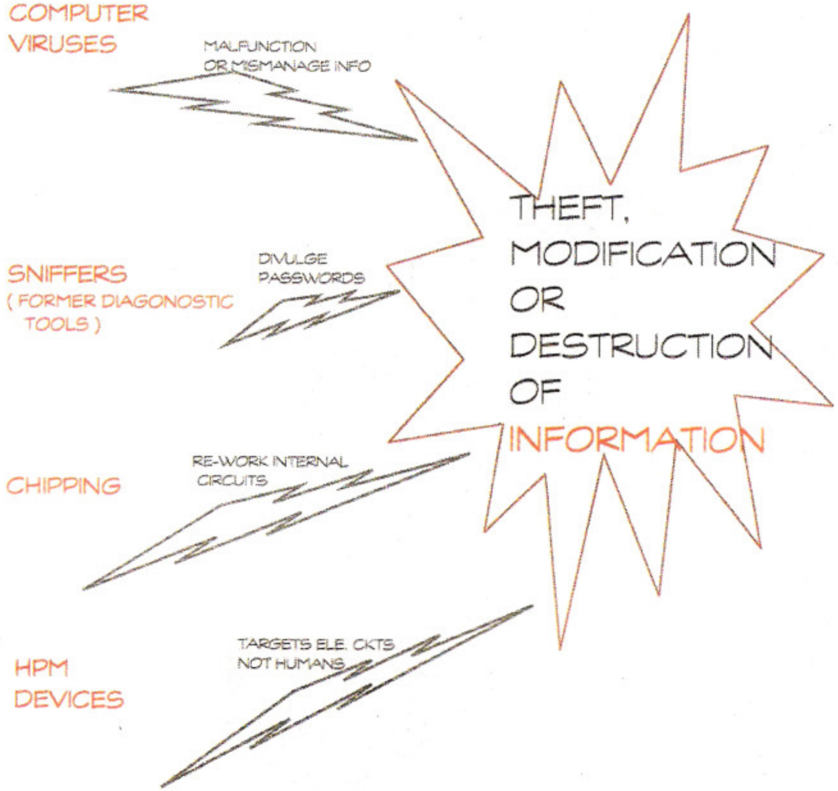
COMPUTER VIRUSES
MALFUNCTION OR MISMANAGE INFO
SNIFFERS (FORMER DIAGONOSTIC TOOLS)
DIVULGE PASSWORDS
CHIPPING
RE-WORK INTERNAL CIRCUITS
HPM DEVICES
TARGETS ELE. CKTS NOT HUMANS
THEFT, MODIFICATION OR DESTRUCTION OF INFORMATION

FIGURE 4

CONCEPTUAL DOMAINS OF HPM AND EW DEVICES

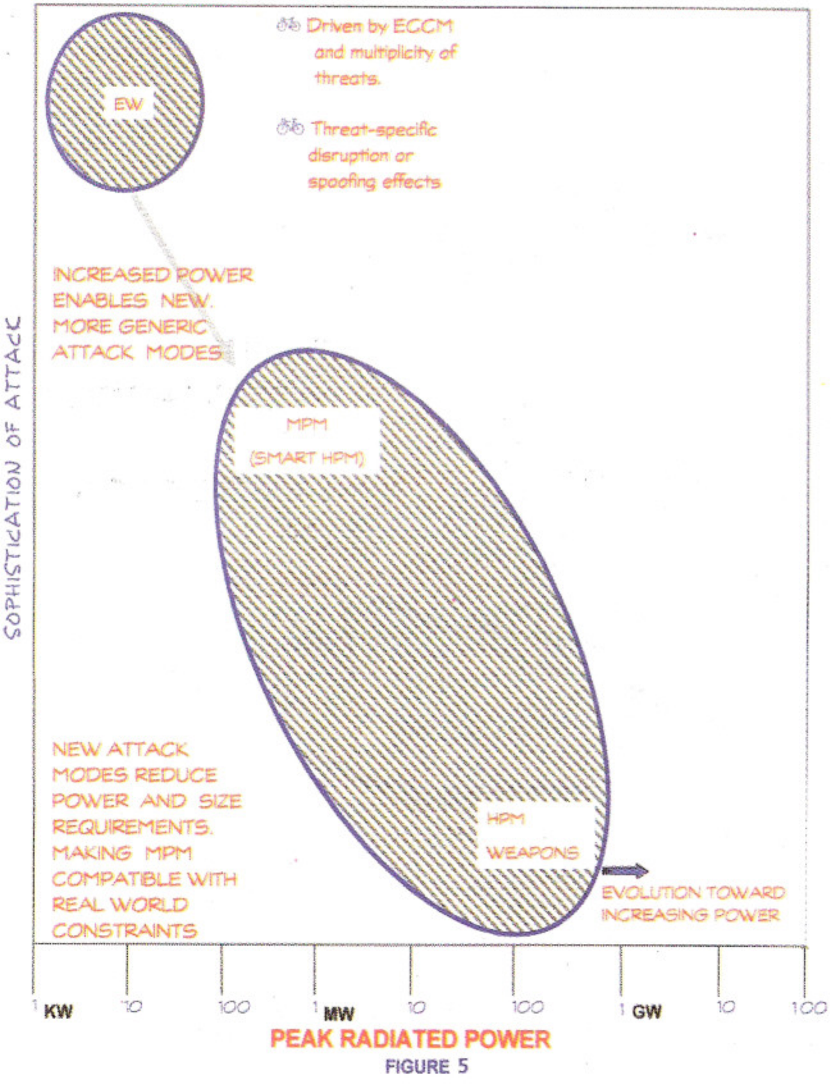
EW
Driven by ECCM and multiplicity of threats.
Threat-specific disruption or spoofing effects
INCREASED POWER ENABLES NEW, MORE GENERIC ATTACK MODES
MPM (SMART HPM)
NEW ATTACK MODES REDUCE POWER AND SIZE REQUIREMENTS. MAKING MPM COMPATIBLE WITH REAL WORLD CONSTRAINTS
HPM WEAPONS
EVOLUTION TOWARD INCREASING POWER
SOPHISTICATION OF ATTACK
1 KW
10
100
1 MW
10
100
1 GW
10
100
PEAK RADIATED POWER

FIGURE 5

CENTRE FOR ADVANCED STRATEGIC STUDIES

The Centre for Advanced Strategic Studies (CASS), Pune was registered on 21st September 1992 under the Society's Registration Act, 1860, and as a Charitable Public Trust on 28th October, 1992, under the Bombay Charitable Public Trust Act of 1950. The Department of Scientific and Industrial Research, Ministry of Science and Technology, Government of India have accorded recognition to CASS as a Scientific and Industrial Research Institution. CASS has been granted exemption under Section 10 (23C) for AY 1992-93 to 1994-95 and under Section 35 (1) (iii) and 80G of the I. T. Act, 1961 till 31 March, 1997. This gives hundred percent exemption for income of the CASS, and to the donating institutions/ organisations, and fifty percent to donating / subscribing individuals.

The Centre aims at undertaking research and analysis of subjects relating to national and international security and development through seminars, discussions, publications at periodical intervals and close interaction with the faculty members and research students in allied disciplines in the Universities / institutions and the Armed Forces. It also awards research fellowships. It aims to generate and promote interest among the academicians and public in these subjects with a view to making them alive to national security concerns. It has received very valuable support from the University of Pune in all its activities, specially from the Department of Defence and Strategic Studies. It has held a number of seminars and group discussions. The proceedings of the major seminar are widely distributed.

ADDRESS :

Centre for Advanced Strategic Studies
Old Examination Hall Complex,
Pune University Campus,
Pune - 411 007

Tel. : 357516 (Off.)

CASS PUBLICATIONS

	SEMINAR PROCEEDINGS	Date of Seminar
1.	"Defence and Industry"	17 May 93.
2.	"Use of Force in Internal Peace Keeping"	04 Dec. 93.
3.	"The Emergence of China : Political, Economic and Military Implications for India"	22-23 Nov.94.
4.	"Human Rights : Law and Order in India"	30 Sep. 95.
5.	"The Emerging Security Environment in South East Asia with Special Reference to Myanmar : Political, Economic and Military Implication for India"	2-3 Dec.95.
6.	"Challenges to India's National Security And India's Defence Preparedness"	20-21 Apr. 96
7.	"Challenges of Comprehensive Test Ban Treaty Implications for India"	28 Aug. 96.
8.	"Preparing to Meet Challenges to National Security In the 21st Century - The Organisational Dimension."	30 Jan. 97.
9.	"Regional Security Environment To The North-West of India With Special Reference To Afghanistan."	21-22 Mar. 97
10.	"Information Warfare"	24 Sep. 97

	OTHER PUBLICATIONS	Date of Publication
1.	"The First SLK Memorial Lecture" by Shri P. Chidambaram, Union Minister for Commerce.	Jun. 95.
2.	"India 2020 : An Agenda for the Nation" by Maj Gen (Retd) KS Pendse.	Feb. 96.
3.	"India : The Nuclear Challenge" by Lt Gen (Retd) EA Vas, Maj Gen (Retd) KS Pendse, Dr. Col (Retd) AA Athale.	Mar. 96.
4.	"Second SLK Memorial Lecture" by Dr. P.C. Alexander, Governor of Maharashtra "Citizens Rights and Indian Democracy"	Jul. 96.
5.	"Third SLK Memorial Lecture" by Justice A.M. Ahmadi, Former Chief Justice of India "Changing Scenario of The Constitutional Values"	Aug. 97.

Printed at Kirloskar Brothers Limited, Printing Division, Pune 411 037.