Disclaimer

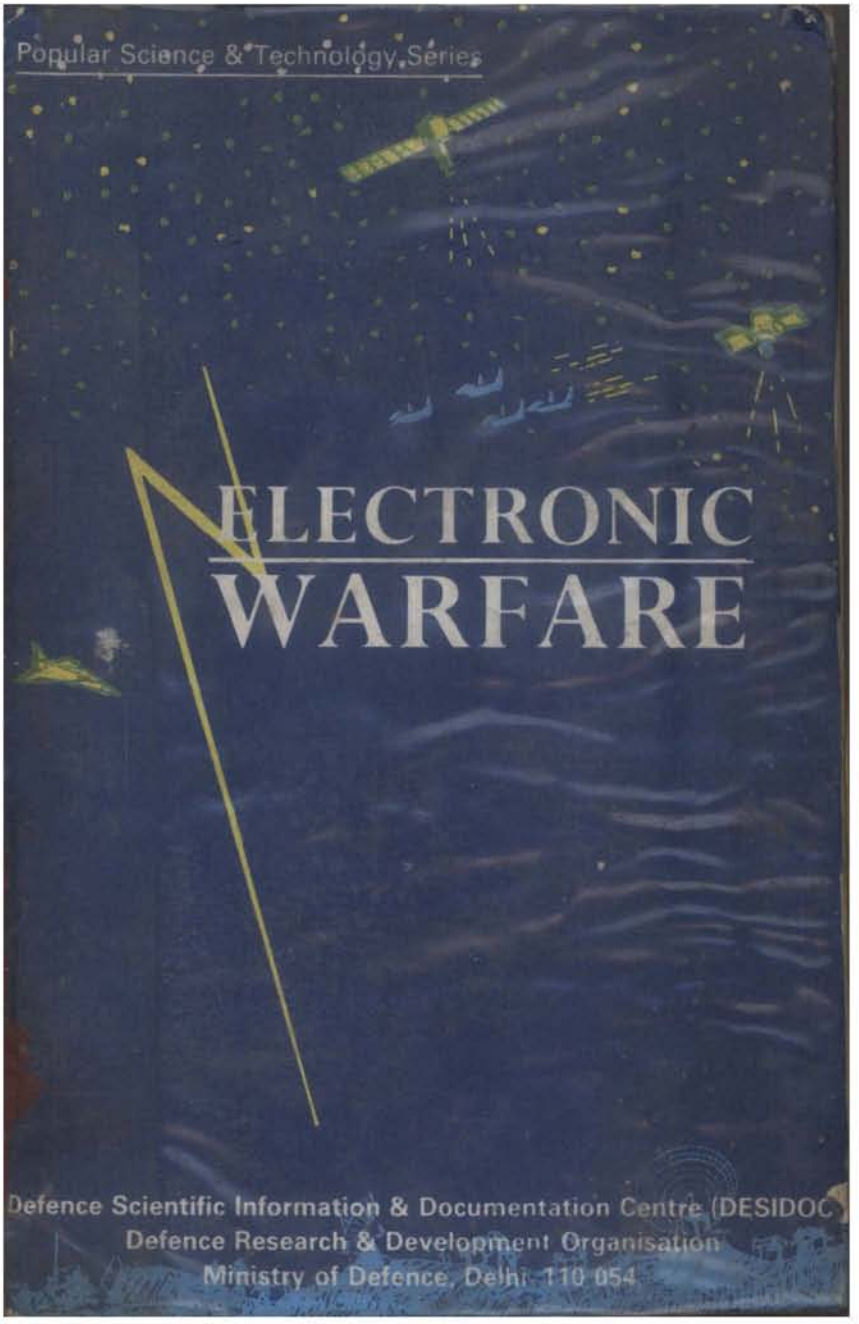
Popular Science & Technology (PST) series is being published by DESIDOC to promote the knowledge and understanding of the applications of science and technology in Defence among defence personnel, students, and general public. The contents covered in each of the titles are current to the year of publication.

This title Electronic Warfare was published in the year 1988.

For subscription details please contact:

Director
Defence Scientific Information & Documentation Centre (DESIDOC)
Ministry of Defence, DRDO
Metcalfe House, Delhi – 110054.
Tele: 011 – 2390 2527/29; Fax: 011 – 2381 9151

Popular Science & Technology Series



ELECTRONIC WARFARE

Defence Scientific Information & Documentation Centre (DESIDOC)
Defence Research & Development Organisation
Ministry of Defence, Delhi 110 054

Popular Science & Technology (PST) series is being published by DESIDOC to promote the knowledge and understanding of the applications of science and technology in Defence among Defence personnel, students and general public. Since the aim is to create awareness of current developments in frontier areas of science and technology among these groups, the presentation of material in the PST publications is lucid and generally in non-technical language. The text is supported by illustrations. Each issue of PST is devoted to a particular subject/discipline of current interest. PST is a half-yearly publication.

Electronic Warfare

Mohinder Singh
Scientist
Institute of Armament Technology
Pune

Defence Scientific Information & Documentation Centre
(DESIDOC)
Defence Research & Development Organisation
Ministry of Defence, New Delhi 110 054

Foreword

The high effectiveness and widespread use of electronic and associated equipment and weapon systems has led to the development of electronic warfare (EW) systems, to detect and counter these weapons. These developments are expanding in vareity, capability and sophistication. The use of infrared, electro-optic and visual techniques, including lasers, also occupies a special niche in the EW field.

The world has, so to say, become EW crazy. In advanced countries, the annual growth rate of the EW industry has been of the order of 20-30 percent and is being maintained at this level.Efforts are going on in a limited scale in developing countries like India and China to develop EW systems to meet their defence requirements. A country's EW capability has now become one of the vital elements which decides the outcome in the event of a conflict.

For obvious reasons of security, the techniques of EW (earlier known as the instruments of darkness) are known only to a few people working in the field. But today, with many complex features and dimensions, EW has grown into an important field. It needs popularisation among students and other general public who are interested to know how wars are fought today. Keeping this in view, DESIDOC had decided to bring out an issue on this subject under their Popular Scince and Technology (PST) series. The task of preparing the issue was assigned

to Shri Mohinder Singh, then at DLRL. He has covered all the important aspects of EW in this small volume.

I am sure that all those who are curious to know about the subject will find this special issue quite interesting and useful.

Hyderabad
June 1988

(K Swaminathan)
Director, DLRL

Preface

The ever increasing proportion of specialisation, complexity and performance of modern weapon systems is directly due to electronics. It is firmly believed by the defence community all over the world that electronics in general, and electronic warfare (EW) in particular, will dominate the battlefields of the future. The Yom Kippur War, the Falklands War and the Lebenon War bear testimony to this. The technological developments in area are so fast that by the time an EW principle or technique reaches the operational stage, it becomes obsolete. The ultimate aim of EW will be to attain an ability to paralyse the enemy before he attacks. In other words, it will be possible to win a battle before fighting it.

The present book covers a number of topics within the broad framework of the subject. The purpose of this book is to provide an overview of of the subject for those interested in the field. Throughout the book, the emphasis has been to provide an understanding of those fundamental principles of EW that have been discussed quite exhaustively in the published literature.

The work has been divided into six main chapters—History of Electronic Warfare(EW), Definitions and Concepts, Electronic Support Measures(ESM), Electronic Countermeasures(ECM), Electronic Counter-countermeasures(ECCM) and Future Trends in EW. Lists of antenna types and their applications, ECCM techniques and Companies manufacturing EW

equipment and their products are given in the Appendices. A Bibliography is included at the end.

I wish to thank all the people who provided indispensable encouragement, motivation and strength during the preparation of the manuscript. First of all, I feel greately encouraged by the keen interest of our Director General and SA to RM, Dr V S Arunachalam, for the popularisation of such a specialised but important topic. I am grateful to Shri V N Rao, Ex-Director, DLRL, Dr E B Rao, former Director, DLRL and now Director & Dean, IAT, and Dr A P J Abdul Kalam, Director, DRDL for their support and guidance. Shri K Swaminathan, Director, DLRL who assigned the job of compiling the manuscript of this publication to me. was the greatest source of simulation. I am immensely grateful to him. I am also equally grateful to all my other colleagus and friends who helped me in all possible ways, wherever required.

The immense contribution of my wife to the preparation of this work through tremendous help and cooperation was a great strength to me.

June 1988 Mohinder Singh

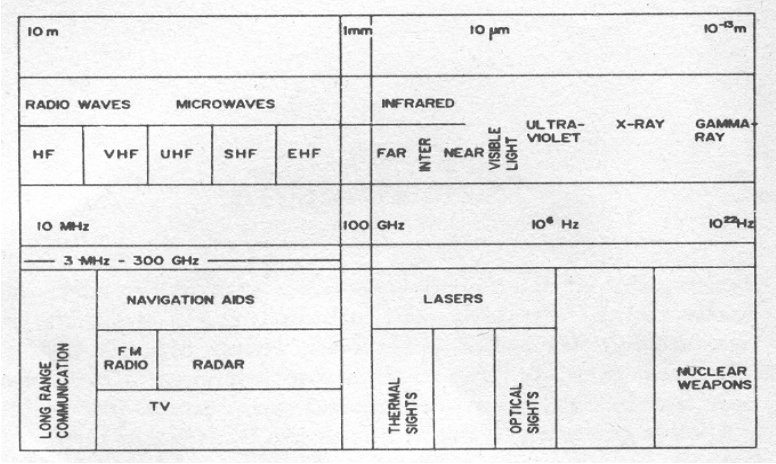
Contents

1. Introduction

Today, almost everybody is familiar with fighter aircraft, battle tanks, warships and submarines. A majority of people have seen them in action, either directly or via television or films. But there is another kind of invisible fight involving the use of radio and radar emissions which is always going on in the atmosphere. This silent battle of beams is commonly called *Electronic Warfare.* The battlefield of electronic warfare is global and its intensity varies according to different national perceptions of potential threats. In fact, electronic warfare is a catalyst towards the maintenance of regional and global balances which deter the outbreak of armed conflict.

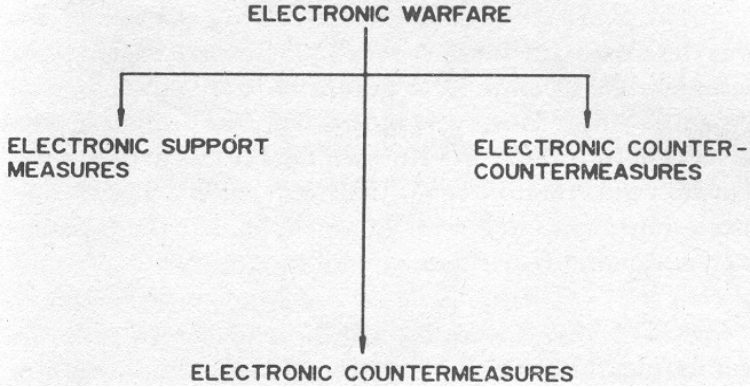
1.1 WHAT IS EW?

Electronic Warfare (EW) is not strictly 'electronic', i.e., it is not conducted using electrons; rather it is electromagnetic, and uses the entire range of the electromagnetic spectrum, as shown in Fig.l. Because of this, some people also call it *Electromagnetic Warfare.* During World War II, Sir Winston Churchill coined the words 'wizard war' and 'battle of beams'. However, the most accepted term for this field of applied science is 'Electronic Warfare'. Electronic circuits are, of course, used in EW equipment.



The basic concept of EW is to exploit the enemy's electromagnetic emissions in all parts of the electromagnetic spectrum in order to provide intelligence on the enemy's order of battle, intentions and capabilities and to use countermeasures to deny effective use of communications and weapons systems while protecting one's own effective use of the same spectrum.

EW involves a variety of concepts and definitions of many



terms which make the subject difficult to comprehend by laymen. Recognising this problem, the US Joint Chiefs of Staff issued a document, which embodied the basic terms of EW and their definitions. According to this, the field of EW is most commonly sub-divided into three categories: Electronic Support This Measures (ESM), Electronic Countermeasures (ECM) Electronic Counter- Countermeasures (ECCM). These are shown in Fig.2.

1.2 HISTORICAL DEVELOPMENTS IN EW

Electronic warfare is not new; it has been practiced in one from or another in every major conflict since the early days of this century; in fact, ever since radio communications were first used in war. Early techniques were often primitive and it was only from World War II onwards that EW gained an element of sophistication and maturity .

Before we go deeper into the study of electronic warfare, let us have a look at the historical development of EW and the strategic role it has played in key conflicts. is will help to highlight the importance of EW.

The first reported conflict involving the use of EW was the Russo-Japanese War of 1905, when Russian naval commanders attempted to jam radio transmissions from Japanese ships. However, in this war, the Japanese were successful in trailing the Russian fleet because they could transmit information about their movements and combat formations, without getting jammed, back to the Japanese high command for necessary action.

World War I saw the widespread use of radio for communication and transmission of combat information. In 1914, the Germans intercepted the communication system of the British forces. This communication jamming in practice is considered the first real action of EW, as electromagnetic energy had been used, not for communication, but for jamming enemy communications. It was also during World War I that both sides experimented with electronic deception in its the simplest forms, such as false transmissions, electronic the espionage, dummy traffic and other similar ruses for misleading the enemy. Direction-finding achieved great success in maritime operations during this war.

However, specialised EW equipment began to be developed only during World War II. Use of radar for war the operations was a major development of this period. Early sys in 1939, Germans employed *Luftwaffi's* LZI30 *Graf* up *Zeppelin* for locating British early warning radars. The rad Germans also introduced radio guidance techniques for their bombers during night raids on British military installations. Under pressure due to this constant threat of destruction, the British eventually developed a deceptive out. ECM called 'Bromide' against the German technique of eql dropping bombs on pre-located targets.

The sophisticated Wurzburg gun-Iaying German radars created a sensation in World War II. The British began to equip their aircraft with both noise jammers and passive ECM equipment as a countermeasure.Throughout the war, there was a fight between ECM and ECCM. Each side momentarily gained the upper hand in EW, only to lose it against a new countermeasure.

EW technology became progressively more specialised and sophisticated after World War II. During 'Vietnam War in 1965, Soviet SA-2 'Guideline' radar-guided SAMs (surface-to-air missiles) and 57 mm. radar-controlled AAA (anti-aircraft artillery) made their first appearance in the stormy battlefield, and the first SA-2 downing of a US fighter aircraft was recorded. The US found itself severely short in ECM and early warning equipment to meet this new challenge. To counter this serious threat, some crash programmes were started by the USA to develop an adequate EW capability to reduce the aircraft losses. Like the World War II, the Vietnam War also continued for many years. In 1971, one of history's heaviest barrages of radar-controlled AAA and SAMs were employed against US bombing raids over Hanoi and Haiphong. The US countered by deploying every available EW aircraft including the EA-68 *Prowler* , he first fully integrated tactical airborne jamming system. Thus the Vietnam War of 1965, which continued up to 1971, clearly demonstrated the conflict between radar and ECM and between ECM and ECCM.

The race of developing countermeasures against countermeasures continued to be directed to outmanoeuvre and outperform the adversary's equipment and ECM. The 1973 Middle East War (also known as Yom Kippur War or the Arab-Israel War) saw most of the latest Soviet SAM and AAA systems in action. Each side used a different region of the electromagnetic spectrum for target tracking and guidance. For the first time in modern warfare, a dense ground-based air defence E' system featuring the full spectrum of overlappling SAMs and AAA was thus encountered. In addition to passive communications monitoring, the Arabs employed a range E of ECM and ECCM measures. Poor ELINT (Electronic Intelligence) before the war led to the inadequate preparedness of the Israeli Air Force to counter the Arab air defences. However, after sustaining heavy air losses in the first few days, they managed to adapt countermeasures to suppress the radar- controlled SAMs and AAA. The 1973 war threw EW into the forefront of modern military thinking. It brought to surface the necessity of possessing a complete range of EW equipment, even in peace time, with an efficiently run Signal Intelligence (SIGINT) service. This war clearly emphasised that if one fails to control electromagnetic B spectrum and to gather intelligence, one may face F disaster.

In April 1982, the world saw another EW conflict in the Falklands War. On 4 May 1982, a British Type-42 destroyer, *HMS Sheffield,* was destroyed by a a sea-skimming French-built Exocet missile. The entire military world was shocked, for this type of warship was supposed to constitute the main fleet defence against air attack in cooperation with airborne early warning aircraft to detect low flying enemy aircraft. Unfortunately for *Sheffield,* there were no airborne early warning radars on board in operation on 4 May when the Exocet missiles were sighted close in. The Sea-Dart missile system on board *Sheffield,* designed to engage aerial platforms at a distance, was simply unable to get on target in time because of its slower reaction time. Assessing the war from the point of view of EW, several innovations were employed in ground combat. *Skeffield* lacked the latest EW equipment capable of countering technologically advanced western missiles like the Exocet. Argentinian forces made very little use of EW systems, except passive EW, like ELINT and ESM. Excellent organisation of command, control, communications and intelligence ($C^3$1) on the part of British forces contributed significantly to its success in the Falklands War.

In June 1982, another fierce EW battle, known as the Lebanon War, was fought between Israel and Lebanon in the Bekka Valley . By mid-june, Israeli forces reported the destruction of 86 Syrian aircraft, including Soviet-built 'Makoyan' MIG-23 fighters and five French-built ' Aero Spatiale Gazelle' attack helicopters. The Israelis reported that they, in turn, had lost only two helicopters and the Bekka Valley area had been destroyed by the Israeli Air Force without much losses. In this war, the Israelis made use of a special type of deception technique, called decoys (drones and RPVs, remotely piloted vehicles) to know the location and characteristics of enemy operating systems and weapons. Israelis had employed their 'Mastiff RPV (as well as drones) to ascertain the microwave radio frequencies used by the Syrian SAM- 65. Two Israeli Grumman, E-2C Hawkeye aircraft obtained electronic bearings of the Syrian missile radar system, allowing them to plot their exact location. Israeli aircraft then destroyed the sites with rockets riding a microwave beam to the SAM-6 sites. This led to a stunning defeat of Lebanese forces and an incredible victory of Israeli forces. Israeli Air Force played a dominant and decisive role In this war. What was the decisive factor? Electronic warfare.

The outstanding results achieved by the Israelis show that the new concept of real-time warfare, supported by accurate planning of EW actions, was the real key to their success. Another element which contributed greatly to the Israeli success in Lebanon was the coordinated use of AWACS (Airborne Early Warning and Control System) and ECM against enemy command, control and communications systems, called C^3CM.

The classic struggle between the lance and shield, the gun and armour, the missile and electronic systems, the countermeasures and counter-countermeasures will no doubt continue in the form of fight between radiation weapons and radiation countermeasures and between these counteremeasures and relative counter-countermeasures and so on.

Electronic warfare today is an utterly deadly battlefield, where victory or defeat may come in a matter of seconds, even microseconds. Thus, in this situation inadequate EW means certain defeat.

Many technological developments have come about as a result of military needs. An engineer was originally a person who designed and built military fortifications and equipment. But during the World War II, the intellectual forces of scientific research and development were deliberately and intensively applied to the conduct of war. Winston S Churchill was one of the first political leaders, with no significant background in science, to have engineers and scientists as advisors, to listen to them and utilise his political power to translate their scientific knowledge in to practical wartime technology .He was also the first leader to recognise EW as a vital phase of military operations.

Since the end of World War II, EW has been one of the best kept secrets with tecnical experts and armed forces. It is still in the interest of these two groups of people, though for different reasons, to keep EW developments hidden from indiscreet and unscruplous people. For a crew of military aircraft, a tank or a warship, an appropriate EW tactic which has been kept secret can mean the difference between the success and failure of their mission, or even the difference between life and death.

Therefore, there are strong reasons for keeping many aspects of EW secret. However, there are equally strong reasons for not only the armed forces and those concerned with National Defence but also the academicians, students and the general public being informed about the existence and general usefulness of EW. Upto World War II, Radar was the most secret weapon in the hands of military forces. The common man was interested to know about its capabilities. Soon after World War II all secrets of radar were thrown open to the public. It soon became a household word. It revolutionised the areas of research in the academic and specialised research institutions. Today, we have a great variety of radars performing thousands of functions for war, peace and public good.

With the same objective in view, an attempt has been made to make interested readers aware of the capabilities, limitations and applications of the diversified science of EW.

Much of the information pertaining to EW is still classified and can be expected to remain so. The basic principles, however, are easily derived and are easily derived and are unclassified. This text is thus confined to the discussion of general principles of electronic warfare and its multi-dimensional extension and growth to various areas of specialisations.

2. Definitions and Concepts

In this chapter, the general principles of EW are covered. The terms ESM, ECM, ECCM mentioned in Chapter 1 have been elaborated. Some of the major subsystems have also been explained.

2.1 EW DEFINITIONS

2.1.1 Electronic Warfare (EW)

Electronic Warfare is a military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent the hostile use of electromagnetic spectrum as well as action which retains friendly use of electromagnetic spectrum.

2.1.2 Electronic Support Measures (ESM)

Electronic Support Measure is that division of electronic warfare which involves actions taken to search for , intercept, locate, record and analyse radiated electromagnetic energy, for the purpose of exploiting such radiations to support military operations. Thus, ESM is an important source of EW information to carry out electronic countermeasures and electronic, counter- countermeasures. ESM involves, in general, gathering of EW information through Electronic Intelligence (ELINT), Communications Intelligence (COMINT) and ESM receivers.

2.1.3 Electronic Countermeasures (ECM)

Electronic Countermeasures are the actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum. Two major actions of ECM are jamming and deception.

2.1.4 Jamming.

The deliberate radiation, reradiation, or reflection of electromagnetic energy to impair the use of electronic devices, equipment. or systems is called Jamming.

2.1.5 Deception.

The deliberate radiation, re-radiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead the enemy in the interpretation or use of information received by his electronic systems is called deception.

There are two categories of deception.

2.1.6 Manipulative.

The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

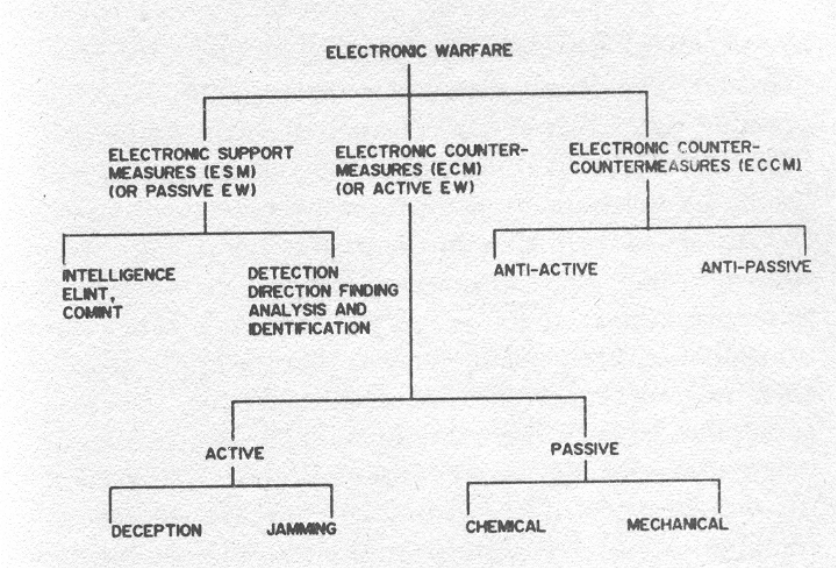
2.1.7 Imitative.

Introducing radiation into enemy channels which imitates his own emission.

2.1.8 Electronic Counter-Countermeasures (ECCM)

The actions taken to ensure friendly, effective, use of the electromagnetic spectrum despite the enemy's use of EW are known as ECCM.

As a matter of convenience and simplicity, the field of EW is discussed in terms of active and passive roles. Passive EW is the search for and analysis of electromagnetic radiation to determine the existence, source and pertinent characteristics of the enemy's use of the electromagnetic spectrum. On the other hand, Active EW is the radiation or re-radiation of electromagnetic energy so as to impair the enemy's use of electronic equipment/system, or to mislead the enemy in the interpretation of data received from his electronic systems/devices.



In general, ESM is Passive EW, ECM is Active EW, and ECCM may be either active or passive. Fig.3 shows the numerous divisions, sub-divisions and branches of today's complex EW tree.

2.1.9 RADAR AND COMMUNICATIONS EW

It is worth mentioning here that the above sub-division of the subject EW into ESM, ECM and ECCM is applicable to both Radar EW and Communications EW. However, there are some basic differences between the two. For example, in the case of radar, usually the transmitter and receiver are located at the same place, whereas in case of communications, the transmitter and receiver are located at separate places. Also, in the case of radar, there is a two-way range for transmission, whereas in the case of communications, there is only a one-way range for transmission. Another difference is that the radar usually uses no encryption for message security. whereas encryption is used in communications for generation of secure messages. Further, in radar EW, the radar system is jammed or misled by creating false targe.ts, whereas in communication EW, the communication system is jammed or misled by creating false messages.

2.1.10 OBJECTIVES OF EW

Electronic Warfare, whether it is radar-based or communications- based, employs the electronic devices and techniques for the following purposes.

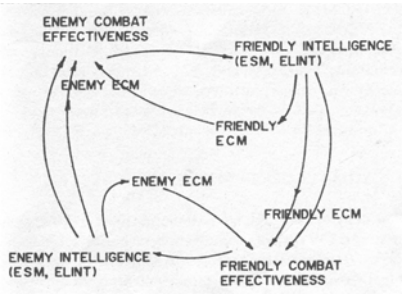
- Determining the existence and 'placements of the enemy's electronic aids to warfare
- Destroying or degrading the effectiveness of the enemy's electronic aids to warfare
- Denying the destruction or degradation of the effectiveness of friendly electronic aids to the warfare.

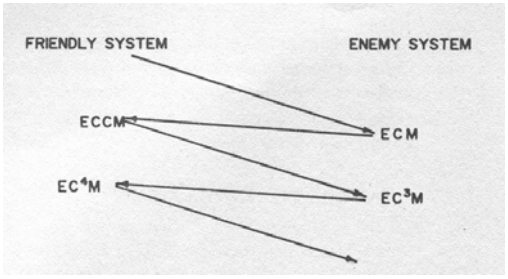
EW tries to achieve the above purposes by adopting the following procedures.

- Make full use of electromagnetic emissions released either intentionally or accidentally by the enemy
- Interfere with the enemy's use ofelectromagnetic spectrum in such a way as to render its use either ineffective, degrading or even dangerous for him
- Defend one's own friendly use of the electromagnetic spectrum.

2.2 INTERACTIVE ROLE OF EW

The role of EW is not static. It is a dynamic and closely inter- related interaction between ESM, ECM and ECCM and the Order of Battle, as shown in Fig.4. It is active as well as passive depending upon the nature of threat. For example, ESM may involve active radiation of a signal to determine the characteristics of the enemy equipment/system and ECM may require a passive reception of the enemy signals in order to decide what signal to counter. There is always an interaction between friendly and hostile electronic systems in an EW environment.





Also, ECM and ECCM are electronic equivalants of action and reaction of Newton's third law of motion. In combat-like situation, friendly forces always try to counter the enemy's electronic systems through ECM. This ECM, in turn, causes a counter-countermeasure (i.e., ECCM) to reduce the effectiveness of friendly systems/equipment, and this process continues ad infinitum. The ECM and ECCM process resembles a ladder-type advancement, as shown in Fig.5. There is always an ECCM for an ECM. One can never achieve unequivocal superiority through ECM.

2.2.1 SOME PECULIARITIES OF EW SYSTEMS

The design of a system is based mainly upon its objectives or needs. EW systems occupy a special position under the category of electronic systems, since their primary function is to be responsive to a potential threat or the enemy's immediate action. Therefore, the design philosophy of EW systems and their development cycle do not follow the traditional pattern set by other active weapons and electronic systems and subsystems. There are certain salient points of difference between the design and development of an EW system and other electronic systems, as indicated in the following

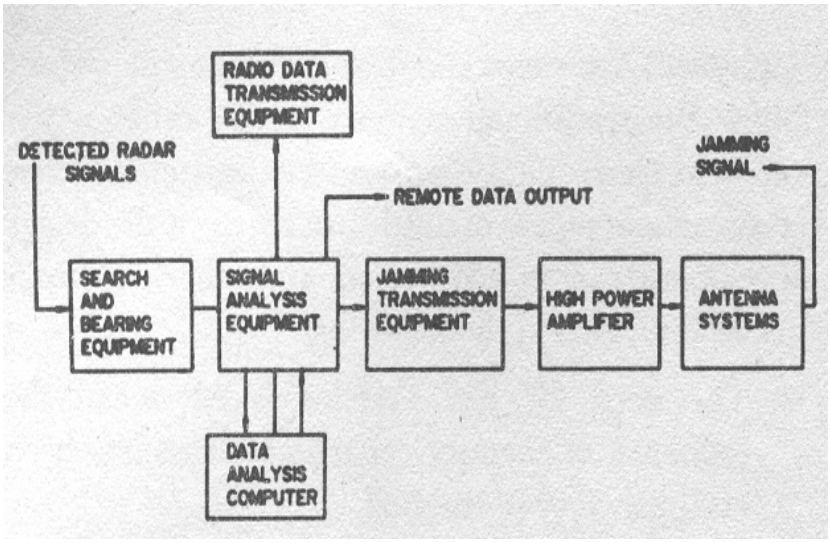
- The need for EW systems is felt when the existence of enemy electronic systems has been established or postulated.
- The features or characteristics of EW systems are determined when the features or nature of enemy electronic systems have been known or anticipated.
- The effectiveness of EW systems is established only when the enemy electronic systems are present, i.e., when the combat environment is either real or simulated.

- The future design of EW systems can only be predicted when the anticipated electronic environment created by the enemy is known.

Thus, the design of EW systems is mainly based on the electronic environment created by the enemy. Therefore, the information on enemy activity and its interpretation (i.e., intelligence) is key to the design, development and planning of EW systems.

2.2.2 A TYPICAL EW SYSTEM

From the above discussion, it is clear that an EW system is unique in its features and design. A functional block diagram of atypical EW system is shown in Fig.6, to give an idea about the complexity of the system. The following are the subsystems in atypical EW system.



2.2.3 Search and bearing equipment.

Consists of search and bearing receivers which cover a number of specific radar bands. The receivers display on a cathode ray tube (CRT) the selected signal, its.. frequency, type of transmission, true or relative bearing (i.e, angle of arrival of the signal) and the antenna rotation period (ARP), if desired.

2.2.4 Signal analysis equipment.

Comprises frequency counters and pulse/spectrum analysers and a video display unit. This equipment measures a number of parameters and their values present in the received signal. These include the pulse repetition rate (PRR), the pulse width, the period and the total harmonic content of each transmitted pulse. Facilities also exist to feed this

information to a remote data system, i.e., tactical indicator to display threat category, frequency of transmission, signal parameters and other relevant data.

Data analysis computer equipment. Comprises a multiplexer (MPX) and the central processing unit with associated memories. The binary coded decimal (BCD) signal data from signal analysis subsystem is fed to this subsystem for threat evaluation and/or storage.

2.2.5 Radio data transmission equipment.

Comprises a signal processor, pulse code modulation (PCM) encoder, pre-modulator and RF transmitter. This subsystem processes selected analog signals fed from the analysis equipment and converts them to a pulse code for application to the modulation circuits of a radio communication transmitter.

2.2.6 Jamming transmission equipment.

Comprises special wide-band and spot tuning microwave circuits operating a power output stage providing powers between 20W and 4OOW. It has the capability of transmitting amplitude modulated (AM) or frequency modulated (FM) noise signals or AM pulsed deception signals when the analog signals from the analysis equipment are fed into it. Some systems may radiate a combination of pulsed and noise signals. The jammer transmitter covers the same frequency band as the search equipment.

2.2.7 High power amplifier equipment.

Comprises a high-power, liquid-cooled, travelling-wave tube (TWT) amplifier, a high voltage modulator unit, and the power supplies and control equipment to operate the system. The frequency power output, modulation type arid levels are controlled remotely from the high power amplifier control unit. This type of subsystem is only fitted to those systems which can provide the excessive power and complex cooling facilities required by large travelling-wave amplifiers. The high-power amplifier equipment has the capacity to increase the strength of the jamming signal to at least twenty times that of the basic jamming equipment.

2.2.8 Jammer antenna equipment.

Comprises a ferrite circulator, high-power amplifier (when it forms a part of jamming antenna), main receiver, servo system, beam switching unit, oscillator, transmitter antenna, receiver antennas and antenna training motor. In this subsystem, the jamming signal is directed to the target by the antenna. A special jammer receiver, in conjunction with a servo system, keeps the antenna aligned on the selected target. When a high-power amplifier is not fitted, the output from the transmitter is applied directly to the transmitter antenna. If a high-power amplifier is fitted, the output from the jammer transmitter is applied to a ferrite circulator with one input and two output ports.

Video blanking equipment (not shown in Fig. 6). Comprises input processing amplifier, flip-flop circuit, pulse shaping circuit, pulse amplifiers and a video mixer. A video blanking system is used with most EW display units. The video blanking facility, by adjusting the blanking level, minimises the interference produced by radars and all jamming transmitters operating in the friendly EW systems.

2.2.9 SOME CONCEPTS ASSOCIATED WITH EW SUBSYSTEMS

As has been seen, an EW system is a very complex structure, consisting of many subsystems, components and devices. The electronic components and devices associated with the main subsystems are many and not all of them can be elaborated. However, to provide further insight into the subject, the details about some components of the main subsystems like antenna, transmitter and receiver and the associated concepts are given here. The basic concepts of radar, which forms an important element of EW systems, are also outlined.

2.2.10 Radar

'Know your enemy' still remains a valuable military maxim. Radar is the most commonly deployed long range electronic sensor. The acronym "Radar' was coined during World War II, and it stands for 'radio detection and ranging', the functions which it is supposed to perform. It can also work at night when there is little or no ambient light to illuminate the target.

Since World War II, radar has been found useful in a great variety of applications. Its ability to function in an all- weather environment at long ranges is unmatched by any other available sensor. It can be fitted to ground, ship, air and even space-based platforms. It is playing a key role as a sensor in a variety of forms in the modern weapon systems.

Radar is a complex system. A functional radar system consists of four basic elements-a transmitter, a highly directional antenna, a receiver and an indicator or display. The transmitter produces intense pulses of microwave electromagnetic energy at short intervals. The pulses are propagated outward in a narrow beam from the antenna, and strike targets at various distances. The reflected signals or echoes are picked up by the antenna shortly after the pulse is transmitted. The time gap between the transmission and the receipt of echo is directly proportional to the distance of the target from the radar, i.e., the farther the target, longer is the time before the echo is received. A device, duplexer, allows, the simultaneous operation of a receiver and transmitter, on differrent frequencies, using the same antenna. The noise produced in the system is reduced to minimum through special circuits so as to extract exact information about the target.

There are many types of radars today. They are classified according to their applications. Radars perform a number off functions like surveillance, tracking, guiding missiles, controlling weapons, detecting targets, etc. The various types of radars and their functions are given in Appendix I.

Generally, radars operate at narrow bands of electromagnetic spectrum because of operational constraints. The radar frequency bands range from 3 MHz to 300 GHz, but most of them operate in what are commonly called 'Microwave Frequency Bands', designated as L (1-2 GHz), S(2-4GHz), C (4-8 GHz), (8-12 GHz) and Ku (12-18 Ghz) bands. Very High Frequency (VHF), 50-300 MHz and Ultra High Frequency (UHF), 300-1000 MHz are generally used for long distance surveillance, because of their ability to provide over-the-horizon coverage. Search radars and tracking radars are most often found in one of the higher radar bands, with S, C and X bands being the widely used ones. The higher frequency bands like, Ku (12-18GHz) K (18-27GHz), Ka (27-40 GHz) and millimeter (40-100 + GHz) frequencies are finding increasing use in mapping, fire control, and missile guidance applications.

Some terms or concepts which are associated with radar and frequently quoted are radar cross-section, , radar clutter, radar signature, radar silence, and the radar warning receiver .

2.2.11 Radar cross-section.

Radar cross-section of a target plays a major role in its detection and location by radar. Radar cross-section, generally denoted by the Greek letter -sigma ( ), is the area a target would have to occupy to produce the amount of reflected power (i.e., echo) that is detected back at the radar. It depends upon several factors like physical size of the target, geometry of the target, radar frequency, viewing direction and the composition of the target.

Smaller the radar cross-section, more difficult is its detection. Thus by reducing the physical size of the target, using effective design in its geometry (i.e.,making curved surfaces), adopting proper viewing direction and using special surfaces with reduced reflectivity, one can reduce the radar cross-section of a target (say aircraft) by several orders of magnitude.

2.2.12 Radar clutter.

This is a major obstruction in the proper identification of a target by radar. Clutter actually arises due to radar returns from buildings, foliage, sea waves, clouds, plants, trees, etc.

2.2.13 Radar signature.

These are specific radiation parameters of a radar that distinguish it from all other radars, even of the same type. Radar parameters include power frequency, pulse repetition frequency (PRF), pulse length, antenna gain, antenna polarisation and antenna scan.

2.2.14 Radar silence.

Generally, it means there are no radiations emitted from the radar, and radar simply 'listens' in this mode. More specifically, it is an imposed discipline prohibiting the transmission by radar of electromagnetic signals on some or all frequencies.

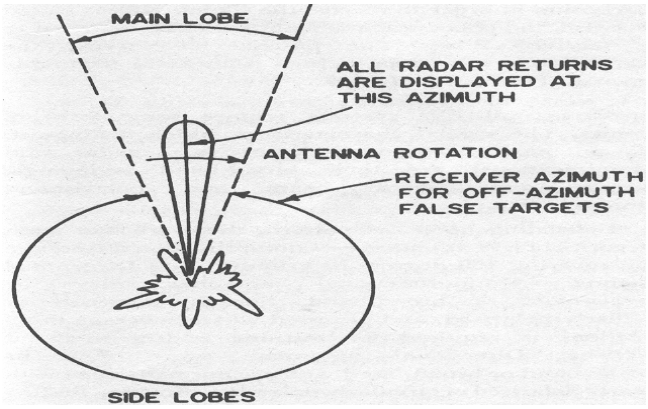
2.2.15 Antenna

An antenna is a device that can transmit and/or receive electromagnetic energy. In a transmitting antenna, electrons flowing back and forth in the conductor generate electromagnetic fields that propagate far into space. In a receiving antenna, passing electromagnetic fields cause electric current to flow back and forth in the antenna conductor at the same frequency as the field oscillations. Thus, antenna is a special kind of transducer, that converts electric current into electromagnetic energy and vice versa.

The performance of a system largely depends upon its transmitting and receiving antennas. If the antenna is badly designed or poorly located, system operation is seriously affected. Like the human eye and other optical systems, the radar antenna is deliberately designed to be more sensitive in a given direction than in the other directions. This serves to concentrate more energy on the target upon transmission, and to increase the receiver sensitivity upon reception. In other words, in a practical antenna, there are usually one or more preferred directions where power detected is usually more than power detected elsewhere. The factor by which a given antenna 's power density is larger than that of an isotropic antenna (no directional preference) in a selected direction is defined as the' Antenna Gain' along that direction. The maximum gain of an antenna is known as the 'Directive Gain' of the antenna.

Each antenna has its specific pattern. The directional characteristics of any transmitting or receiving antenna, when graphed on a polar coordinate system, is called the, Antenna Pattern'.An antenna pattern may have just one lobe, or it may have several lobes. The measure of the degree to which the output of a directional antenna is concentrated is called its 'Beamwidth'. Antenna beamwidth is usually specified in terms of horizontal direction, or azimuth, and can also be specified in the vertical plane. 'Bearing' generally refers to the direction of the antenna, such as azimuth or elevation or a combination of directions.

Different lobes may have different magnitudes. The strongest lobe is called the 'Main' or 'Major' lobe. The localised weaker lobes or peaks which lie outside the main lobe or beam are known as 'Secondary', 'Minor' or 'Side' lobes. Maximum energy of a signal lies in the main lobe or beam of the radiation pattern, as shown in Fig. 7.



There is another important phenomenon in antenna, called 'Polarisation'. The polarisation of an antenna is determined by the orientation of the electric lines of force in the electromagnetic field radiated or received by the antenna. Polarisation may be linear, or it may be circular. Linear polarisation, again, may be vertical, horizontal, or somewhere in between. In circular polarisation, the rotation can be either clockwise or counter-clockwise. The important aspect of polarisation is that if the transmitted wave is polarised, then each receiver must have a matched polarisation in order to receive the signal. Unless stated otherwise, the polarisation is assumed to be matched to the received wave. The practice of varying the polarisation in a random manner is an ECM technique known as 'Polarisation Diversity'.

Almost all EW systems require some form of antenna. The special characteristics which distinguish EW antennas from other types (e.g. radar and communications) are their broad-band wide-angle coverage and diverse beam and polarisation requirements.

Depending upon the pattern, there are two main categories of EW antennas-Omni-directional Antenna (one covering 360 degrees in azimuth) and Directional Antenna. Omni-directional antennas may be narrow-band or broad-band, linearly polarised or circularly polarised, and are used where coverage in all directions is required for warning and or intercept functions. Directional antennas, again may be narrow-band or broad-band, and are normally used with linearly polarised or circularly polarised, direction finding systems, high-gain intercept systems, directional jamming systems and radars. Linear polarisation is used when the antenna is of known linear polarisation and it is desired to optimise the gain of the system, or if polarisation analysis is to be performed. Circular polarisation is used when the polarisation of the other antenna is unknown or variable, or if polarisation diversity for any other reason is required. Circular polarisation is used for both the ECM and ESM functions.

There are mainly three types of EW antennas: Fixed Beam EW Antennas, ECM Phased Array Antennas, and Lens-fed Multiple Beam Array Antennas.

2.2.16 Fixed beam EW antennas.

There are several designs of fixed beam EW antennas. Each antenna has its characteristic radiation pattern. These antennas are mostly used for ESM and ECM applications.

2.2.17 ECM phased array antennas.

An array of an antenna is a collection ofantennas, usually dipoles, placed at equal distances along a common line of reference, known as array axis: A phased array is an antenna having a number of radiating antenna elements driven by some form of beam-forming network. The elements are fed with a certain relative phase, resulting in a directivity pattern that exhibits gain in some directions and little or no radiation in other directions.

The primary advantage of a phased array antenna in ECM applications is its ability to rapidly (i.e. within microseconds) and accurately point the jamming beam or beams at the victim radars within its spatial coverage angles. The pointing ability allows the use of narrow jamming beams, which magnify the jamming energy focussed on victim radars through increased effective radiation power (ERP). The phased array, 'thus, find valuable application in both airborne self-protection ECM systems and for stand-off EW jamming missions. The accurate beam pointing capability of phase-steered array is also commonly used to provide direction finding with high probability of intercept.

2.2.18 Lens-fed multiple beaIn array antennas.

In ECM phased array antennas, the beam-forming is done through phase steering using phase shifters, and the direction of the beam position is frequency dependent. In case of lens-fed multiple beam array antennas, the direction of each beam is fixed in angle and is made independent of frequency by using appropriate time delay steering in each element. These are used in self-protection ECM applications.

2.2.19 Transmitter

A transmitter is a device that produces a signal for communication purposes. A basic transmitter consists of an oscillator, a transducer, a modulator and a signal amplifier. The oscillater provides the carrier wave. The transducer converts audio and /or video information into electrical signal on the carrier wave. The amplifier boosts the signal level to provide sufficient power for transmission over the required distance. The amplifier output is connected to an antenna system for transmission. The design of a transmitter depends, to some extent, on its application.

2.2.20 Receiver

Any circuit that intercepts (i.e., reception of a signal by an unintended user) a signal, processes it and converts it to a form useful to a person, is a receiver. A receiver usually consists of five or six basic components- an,antenna or receptor, a front end/wide-band filter, an amplification chain/narrow-band filter, a detector, an audio and/or video amplifier and a transducer. When electromagnetic waves strike the antenna or other receptor, alternating current is set up in the conductors. It is then fed to the front end. The front end, wide-band, filter then provides amplification and some selectivity. This is then fed to the , amplification chain. The amplification chain brings up the weak signal to a

level suitable for operating the detector, which extracts the modulation information from the electromagnetic energy. This is then fed to the audio or video amplifier, which gives the detected signal sufficient amplitude to drive the transducer. The transducer then converts the detected signal to a form suitable for listening, viewing, driving a set of recording instruments, or a combination of these things.

The above-mentioned architecture is valid for a simple type of receiver. EW intercept receivers, on the other hand, have to function in a high signal density environment. Their key function is to search, intercept, locate and identify the sources of enemy electromagnetic radiations for the purpose of threat recognition and tactical employment of military forces and ECM equipments. EW receiver architectures are usually scenario-dependent, and hence there is no preferred general or universal architecture which is applicable for all types of intercept receivers.

2.2.21 LESSONS LEARNED FROM EW CONFLICTS

It is quite evident from the above discussions that in the intervening years between 194l and 1982, EW technology has advanced by giant steps. Nevertheless, those historic air combat operations in World War II over the English Channel revealed the same basic lessons as did the conflicts employing more complex systems at a much later time in history.

- No countermeasure is effective for ever. It is time-sensitive and time-perishable.
- Countermeasures are more effective when used in a 'surprise' mode, The wise battle planner should act accordingly.
- Men make the ultimate difference in an EW engagement. A good system with an unskilled operator will always lose to a marginal system with an alert, knowledgeable technician at its controls.
- Countermeasures, in themselves, are useful in military operations. Coupled with imaginative tactics, countermeasures are decisive factors for victory.

In conclusion,the ability of a nation to control the three 'R's (recognition, reaction, resolution) will tip the ECM/ECCM balance. One must 'recognise' surprises and correctly estimate their effect, 'react' immediately by alerting corrective forces to respond and 'resolve' the situation by a military/scientific group effort geared towards a dynamic solution-motivated mission.

2.2.22 ROLE OF R&D IN THE AREA OF EW

From the earlier discussion, it is clear that EW is a dynamic field. The mere possession of a certain number of ESM or ECM devices is not enough to ensure success in war. In EW what works today may not work tomorrow, and the developments in EW systems must always closely and appropriately follow developments in the threat. With the endless evolution of applied military technology, electronically-guided weapons are coming closer and closer to perfection and thus constant updating and refinement of EW equipment is required.

Computer, for example, is playing a key role since the last few years in the development of special threat-oriented integrated EW systems. EW and ECW techniques have now become so highly sophisticated that EW personnel must utilise the most modern computer equipment to assist them in complex battle operations.

The extremely dynamic and evolutionary character of EW, unfortunately, demands constant, heavy, financial expenditure. If a potential enemy changes the frequency of one of his radars or develops a new anti-jamming device or makes some important change in the IR guidance system of a missile, then the potential opponent has to modify or completely renew his own EW equipment. However, this is a necessary and worthwhile investment for the military forces. But, this investment must be made in peace time because the price to be paid once an unexpected war has broken out will be extremely high.It is, therefore, vital to have regular research and development facilities for scientific and technical research in order to develop the technology necessary to achieve and maintain superiority in EW which has now become an obligatory route to success.

The battles in Lebanon have proved beyond any shadow of doubt that the result of future battles will depend much less on the quantity of the aircraft, warships or tanks used than on their quality , which naturally includes new developments in the field of electronic technology like antenna, receiver, transmitter, signal processing and other associated technologies related to EW systems.

If there is a World War Ill, the winner will be the side that would control best and manage the electromagnetic spectrum best. So, this race of technology-win must be backed up by extensive and intensive efforts in R&D for the survival of the military forces and the security of the country.

3. Electronic Support Measures

As already defined, Electronic Support Measures (ESM) is that division of EW that involves actions taken to search for, intercept, locate, and immediately identify sources of enemy electromagnetic radiations for the purposes of immediate threat recognition and for tactical employment of military forces or assets, such as ECM equipment. The key functions of ESM are intercepting (which primarily involves detection, frequency estimation and direction finding), identifying, analysing, and locating sources of hostile radiations. ESM is for 'tactical' purposes that require immediate actions as contrasted with similar functions which are performed for intelligence gathering, such as Signal Intelligence (SIGINT}, which has Electronic Intelligence (ELINT), Communications Intelligence (COMINT) and Radiation Intelligence (RINT) as its constituent parts.

3.1 DISTINCTION BETWEEN ESM AND SIGINT

ESM is basically a 'tactically' oriented activity, whereas SIGINT is basically a 'strategically' oriented activity. So, the ESM function is reserved for real-time reaction which serves to differentiate between ESM receivers and ELINT or COMINT receivers, which collect intelligence data for subsequent or non-real-time analysis. SIGINT data generally focuses on producing intelligence of an analytical nature which is not as time-critical as ESM data. Top commanders of military forces are generally interested in SIGINT data. SIGINT is thus closely allied to ESM.

3.2 Distinction between ELINT, COMINT and RINT

3.2.1 Electronic Intelligence (EUNT).

This is defined as intelligence information that is the product of activities non in the collection and processing, for subsequent intelligence purposes, of potentially hostile, non-communications electromagnetic radiations which emanate from other than nuclear detonations and the radioactive sources.

3.2.2 Communications Inielligence (COMINT).

This is defined as intelligence derived from potentially hostile communications by persons other than the intended recipients.

COMINT receivers directed against communication transmissions are similar in concept to those designed to intercept radar transmissions (i.e., non-communication collection of electromagnetic data using ELINT or ESM nun receivers) except that a different approach is required to accommodate the communication signal structure. Communication systems generally operate on discrete channels, are relatively powerful, employ wide-beam antennas with poor side lobes, and use modulated continuous wave transmissions. To avoid jamming, encryption and frequency hopping (i.e., changing frequency randomly) transmissions are normally used. Also, in principle, COMINT does not distinguish between the categories of message intercepted, since the sophistication of

encryption may not be apparent until decryption decryption is attempted. Thus, the additional difference between COMINT and ELINT is the additional processing applied to the received signal in an attempt to recover the message.

3.2.3 Radiation Intelligence (RINT).

This is defined as intelligence derived from potentially hostile communications and weapons systems by virtue of their unintended spurious emissions, even when they are in a non-transmitting mode of operation.

In brief, ELINT is intelligence derived *about* the emitter, COMINT is intelligence derived *from* the emitter, and RINT is intelligence derived *about* and *from* the enemy electromagnetic radiation (i.e., activities) utilising *active* techniques.

3.2.4 IMPORTANCE AND PURPOSE OF EUNT/ESM SYSTEMS

Electronic reconnaissance (which covers ESM and ELINT functions) and its operational employment play important roles in view of the continuous increase in the number of radars and other electronic emitters, and because of the increasing complexity and sophistication of these weapons. Due to this dense operational signal environment, the function of intercept receivers has been extended from that of a single aircraft detection to the detection of warlike intentions of potential enemies, like battlefield surveillance, determination of enemy missile launchings, study of enemy production and industrial capabilities, political moves and covert data collection.

Study of operational environment also plays an important role in the design of intercept equipment for the detection, location, and recognition of a signal associate with a particular piece of radiating equipment. when a radar, a guided missile, a bomb fuse, or an ECM system is required to operate in an environment in which there are many electromagnetic radiators, then it is necessary to know the nature and amount of the interference that may be present in order to design equipment that can function properly.Two classes of information are Important for applying a suitable ECM against the enemy's electronic systems. The first category of information can be termed as strategic information, which include such things as technical characteristics of the electronic systems and weapons to be countered, the mode of operation of the system, and the nature of supplementary systems which can be employed by the enemy, This type of intelligence information is needed to make strategic decisions, such as whether one should attempt to counter the system and what characteristics are required for the countermeasure device. The second category of information might be and called as tactical information, which include such things the as whether the enemy is using a certain electronic system or weapon, the frequency of operation of the system and whether the enemy is shifting his frequency as a result of jamming employed. The strategic mission primarly involves protection of a country's national assets from attack while a tactical mission involves the use of operational forces during combat operations, This type of information is needed to make immediate tactical decisions, such as which particular ECM tactic should be employed so as to defeat the enemy's mission.

One of the most Important sources of both strategic and tactical intelligence concerning a potential enemy's operations is the interception and analysis of the signals radiated by his electronic systems. The most general purpose of the analysis of electronic reconnaissance data is to develop technical descriptions and to geographically locate the various emitters. An intercept receiver (either ELINT or ESM) is normally used for the collection and analysis of reconnaissance or surveillance data. An important advantage of ESM, when used as detector of enemy systems, is that it is completely passive. Also, it provides the potential of detecting enemy radiations from such sensors as radars, lasers and sonars at much greater ranges than the maximum range of those sensors.

3.2.5 ELINT SYSTEMS

The primary objective of an ELINT system is to compile operational data on enemy electronic systems and weapons. ELINT is usually carried out on a regular basis, both during times of peace and war, as well as just prior to and during specific missions. Peace-time operations have the objectives of gathering maximum possible data on the complete electromagnetic environment within specified areas of interest to any one nation. The latter ELINT effort is made in order to evaluate the enemy defensive weapons, early warning radars, ECM and ECCM, and to determine the manner in which to conduct the mission.In general, ELINT serves a strategic role of the enemy, as well as a tactical role in helping to develop or reprogram appropriate ECM and ECCM equipment to meet each threat. Specially equipped ships, aircraft, RPVs, satellites, as well as fixed and mobile land-based facilities are used for collection of ELINT .

The basic targets of ELINT are all types of radars, which are detected, located and identified by their signatures in their operating modes (e.g. search, tracking). The signature (i.e., characteristics) of each radar consists of measurable parameters, such as transmitter's frequency, power, mode, modulation, pulse width, pulse repetition frequency (PRF), etc., employed. Thus, the signature of every radar is collected, analysed and stored. Special ELINT systems have been developed which scan each frequency band continuously, perform a real-time analysis of each intercepted signal, determine its signature and compare this with others in a library in order to identify and locate the threat.

ELINT is also used to obtain data on enemy navigational systems, command, data and telemetry an links, the control and guidance techniques used for each weapon system (i.e., RF , IR. TV or laser) and the ECCM employed. In addition, ELINT information is also used for direction-finding or determining the exact location of enemy radars and defences, in order to guide countermeasures to these targets.

Thus, ELINT operations satisfy a variety of requirements. They can locate hostile electronic systems and weapons, update hostile force electronic order of battle (EOB) information, obtain information on specific transmitters and emissions, test hostile force ECM capabilities,. evaluate hostile force command and control procedures and a host of other intelligent functions which can help in tactical operations.

3.2.6 ESM SYSTEMS

The primary objective of an ESM system is to intercept the enemy electronic systems in a tactical, i.e., real-time environment. Interception of hostile electronic environment is generally attempted to achieve three basic functions-detection, frequency estimation and direction finding. These three elements of interception are usually integrated in a practical system.

Detection is achieved by using radiometer , channelised radiometer or the cross correlator

Frequency estimation is achieved by using ESM receivers.

Direction-finding is achieved by using special DF antennas, which provide measure of angle of arrival (AOA) of emitter pulses.

The principal job of an ESM receiver is to provide information on the existence and nature of various signals usually in the minimum possible time. An intercept system (i.e., ESM receiver) can answer one or more of the following questions:

- Are there any signals present?
- What are the electrical characteristics of and directional bearing to those signals present?
- Is there a particular signal present having certain prescribed characteristics?
- Is there a signal present which is tracking the location of the intercept receiver?
- Is there any new signal added in the general signal environment?
- Is there an unusual signal (not seen 'in catalogues) present?
- Is there a signal present that shows the characteristics of motion of a target?
- Are there CW signals, FM signals, single sideband (SSB) signals?

The list is almost endless. No single ESM receiver will answer all such questions. However, the aim of an ESM system remains the same, i.e., to provide a source of information for immediate reaction involving ECM, ECCM, avoidance, and targeting.

3.2.7 Radar Warning Receivers

An important example of an ESM system is a radar warning receiver (RWR) which intercepts radar signals and analyses their relative threat in real-time. To accomplish this analysis, the RWR must have a threat library representing the enemy's electronic order of battle (EOB, a document describing where and when specific enemy electronic systems are being or will be used in a given battle situation) stored in its microprocessor. The EOB is obtained through ELINT or electronic reconnaissance, which collects and records for subsequent analysis as much data as possible on enemy non-communication equipment.

Radar warning receivers are used in military aircraft and helicopters to warn of attack by surface-to-air and air-to-air missiles, air interceptors and anti-aircraft gun systems. They

are also used to warn tank crews and submarines of imminent threat. Once alerted to the type, direction and relative priority of the threats, the intended target may take some evasive manoeuvres or employ deceptive countermeasures, chaff or flares, as appropriate, to foil the attack.Ideally, an ESM receiving system should be able to

- Intercept a transmitted signal at any frequency
- Determine the types of modulation in the signal
- Identify the usable intelligence carried by the signal (i.e., frequency, PRF, pulse width, scan type and rate, polarisation, amplitude)
- Accurately measure the direction of arrival of the waveform so that the location of the transmitter can be calculatcd
- Process and preserve the signal characteristics for later in-depth analysis
- Provide significant information to the operator (and/or computer) to enable him to make intelligent and timely mission decisions.

In brief, an ESM receiving system must gather , process and display all signals of interest to meet its specific mission requirements.

The above requirements are hard to satisfy for the total range of signal parameters involved. For example, no single ESM receiver or antenna system can gather signals over the entire frequency spectrum of interest.

Radar warning receiver is generally the simplest form of ESM receiver consisting of an unsophisticated low-sensitivity equipment. The complexity of modern ESM receivers is increasing to cope with the continually expanding dense signal environment. Thus, ESM reconnaissance or surveillance receivers are generally considered more complex than RWRs, and they are used to map enemy radar and communications installations and to monitor radio messages. The more elaborate radar surveillance ESM receivers are similar in concept to RWRs, except that they generallv employ more sensitive receivers to intercept radar radiations at long ranges, have a higher direction-finding accuracy, and measure additional radar parameters, such as coherency , polarisation, traffic analysis, pulse rise and fall times, intra-pulse modulation, and statistical characterisation of features (like frequency, scan modulations, etc.).

3.2.8 Advanced DM Receivers

It is difficult for the simple radar warning receivers to cope , with dense signal environment. Their probability of intercept (i.e., performance) deteriorates, particularly when many emitters are present in the dense environment. It needs filtering or sorting of emissions in order to classify each signal to know the important parameters like the amplitude, pulse width, frequency, angle of arrival, coherency , polarisation, pulse train characteristics, etc. of the radar. Many advanced ESM receivers have been developed on the basis of various design approaches. These ESM receivers have excellent multiple signal handling capability in a dense emitter environment. Each receiving system has its own relative advantages and disadvantages for a specific application as discussed in the following.

3.2.9 Crystal video receivers.

They have the advantages of proven technology .They are low cost, small in size and are doing well in limited applications. However, the systems suffer from many limitations. Their capability is limited for fine frequency measurement; the analyser has to handle a wide open system and cannot readily handle complex and dense signals. They have poor sensitivity, are susceptible to ECCM, and are basically incapable of handling frequency agile systems.

3.2.10 Superheterodyne receivers.

They have the advantages of high selectivity, proven design and not being susceptible to jamming; but suffer from their limitations of coping with agile signals, slow search speed, low frequency resolution and needing multiple receivers for direction-finding operations.

3.2.11 Microscan receiven.

They have the advantages of high probability of detection and the ability to handle wide-band signals and frequency agile signals; but suffer from their limitations of requiring a channeliser , minimum pulse width that cannot go much below 0.1 microsecond, and again requiring multiple receivers for DF and a very wide IF bandwidth.

3.2.12 Channelized receivers.

They have the advantages of high selectivity, high probability of detection, and not being susceptible to jamming. However, they suffer from their limitations of limited frequency accuracy, limited resolution, and their requirement of a channeliser. In general, they cannot do monopulse DF in a size- and cost-effective manner .

3.2.13 Instanteneous frequency measurement (IFM) receivers.

They have the advantages of high probability of detection, very good frequency measurement accuracy , proven design and handling of frequency agile signals. On the other hand, they suffer from their limitations of poor sensitivity, easy jamming, inability to handle a very high data rate, simultaneous signals and CW signals.

3.2.14 Acousto-optic Bragg cell receivers.

They have the advantages of high probability of detection, high selectivity and high senstivity. However, they cannot handle frequency agile signals, measure pulse width, require channelisers, are slow in searching, and require two receivers to do monopulse DF and the hardware is still unproven.

3.2.15 Surface acoustic wave (SAW) receivers.

They have the advantages of high probability of detection, good sensitivity, minimum pulse width, handling frequency agile signals, having good high-dynamic range (i.e., an indicator of the signal variations that the system can accept, and reproduce, without objectionable distortion), handling multiple signals, doing monopulse DF with a single receiver and being hard to jam. The limitations of the receivers are that they take moderate time to resolve pulses that are close together, and basically the hardware is still unproven.

From the above discussion, it is evident that there is hardly any single ECM receiver which can be employed for all purposes. In practice, either a hybrid approach or a combination of two or three receivers is used to exploit their relative advantages to handle effectively the dense signal environment.

3.2.16 COUNTERMEASURES TO ESM SYSTEMS

To make ESM systems ineffective, a military force generally practices emission control (EMCON), which restricts emission of electromagnetic radiations until it knows that it has been detected. Active or radiating weapons are usually designed in such a way that the active sensor (i.e., radar, sonar, etc.) is only turned on for its terminal phase (of .he order of 10-30 seconds) so that minimum warning and reaction time is given to the target. Completely passive weapons such as anti-radiation missiles and heat-seeking missiles provide no warning for ESM systems. Friendly forces or systems, by tactfully managing their electromagnetic radiations, try to achieve maximum advantages in the area of intelligence data reception, detection, identification, navigation, guidance, etc. over hostile forces or systems in a given situation through emission control. So, friendly forces are to be always very careful and alert while using ESM systems for collection of strategical and tactical information about the enemy weapon systems and the forces.

4. Electronic Countermeasures

Electronic Countermeasures (ECM), as already defined, are actions that are taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum. ECM, are thus means of interfering with the enemy's electromagnetic activity. These means may be used to either deny him the information he seeks, or to give him false information or to overload his computing capacity with so much false data as to degrade the performance of his system and make it unable to perform its intended mission. ECM may also be used to enhance one's own weapon systems' effectiveness. This ECM mission may be achieved either by jamming, deception or disruption.

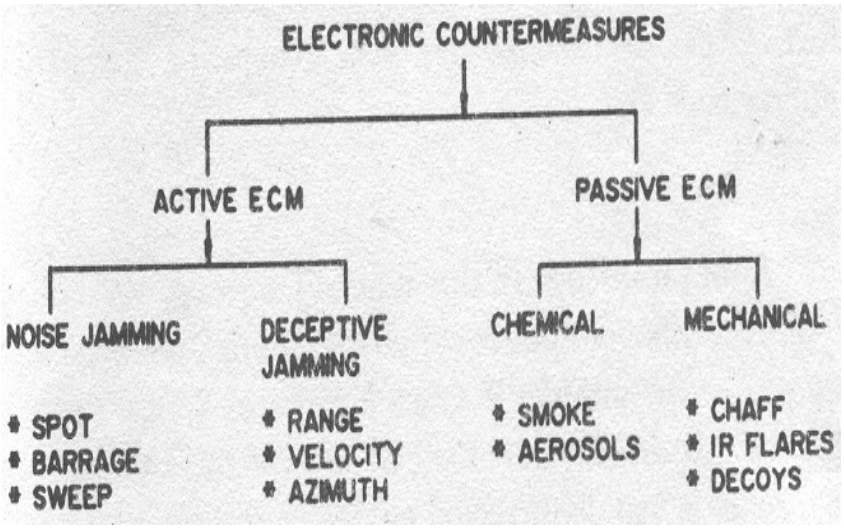
More comprehensively, there are four basic ECM operational objectives.

i. Prevent data acquisition and dissemination by hostile radars, ESM and communication systems, by denying them information regarding the presence, structure, composition or activities of friendly forces within the radar coverage, and prevent hostile ESM systems and communications from receiving information regarding the operation of friendly forces.
ii. Saturate threat systems' data processing and operator capability t.o accomplish timely and accurate detection; tracking of radar targets and to recognise, process and communicate essential elements of information.
iii. Introduce false, deceptive data into hostile electronic systems to generate ineffective responses by automated electronic systems, and to generate ineffective personnel or command and control actions.
iv. Destroy hostile electronic systems so as to deny s hostile forces the use of key elements of their radar sets and C^3 (command, control and communications) structure.

A number of ECM tactics, techniques or methods are used to prevent or reduce the enemy's effective use of the electromagnetic spectrum.

This wide range of techniques is illustrated in the form of a chart in Fig.8.

As can be seen from the figure, there are two major techniques or methods of ECM-Active (i.e., radiating) ECM and Passive (i.e., non-radiating) ECM. Further, ActiveJamming may be either Noise Jamming or Deceptive Jamming whereas Passive Jamming may be achieved by chemical or mechanical means. Within each class of jamming, there are different techniques used for denial or deceptive purposes.



4.1 ACTIVE ECM

This involves degradation of the effectiveness of the enemy system by generating an transmitting electromagnetic energy .This may be achieved either by noise jamming or by deceptive jamming.

4.2 Noise Jamming

The objective of noise jamming is to inject an interference signal into the enemy's electronic system such that the actual signal is completely submerged by interference. This type of jamming is also called 'denial jamming' or 'obscuration jamming'. The primary advantage of noise jamming is that only minimal details about the enemy equipment need be known.

Within the general class of noise jamming, there are three different techniques for generating noise-like If interference.

4.3 Spot jamming.

In this type of jamming, also called 'point jamming' or 'narrow-band jamming', all the power output of the jammer is concentrated in a very narrow bandwidth, ideally identical

to that of the radar. Spot jamming is usually directed against a specific radar and requires a panoramic receiver to match the jamming signal to the radar signal.

4.4 Barrage jamming.

In this type of jamming, all the power output of the jammer is spread over a bandwidth much wider than that of the radar signal. In other words, it involves the massive and simultaneous jamming of the whole of the frequency band.

4.5 Sweep jamming.

This is also similar to barrage jamming. In this case,.the power output of the jammer (i.e., jammer frequency) is swept back and forth over a very wide bandwidth, sometimes as much as an octave (a 2: 1 band). It is generally true that the bandwidth of sweep jamming is wider than that of the barrage jamming, but the relative bandwidth is often determined by the hardware used.

The actual difference between barrage and sweep jamming lies in the modulation techniques and size of the' frequency band covered. Barrage jamming often uses an amplitude-modulated signal covering a 10 percent frequency band (i.e., bandwidth equal to 10 percent of the central frequency). Sweep jamming often uses a frequency modulated signal and the frequency is swept back and forth over a wide frequency bandwidth.

Both barrage and sweep jamming are used when the exact frequency of the enemy system is not known. One major disadvantage of this form of jamming is that it requires much more output power than spot jamming.

4.6 Deception Jamming

The objective of deception jamming is to mask the real signal by injecting suitably modified replicas of the real signal into the victim system. In other words, this type of jamming is used to introduce false signals into the enemy's system in order to deceive or confuse, and hence, to degrade that system. This is in contrast to noise type of jamming, whose objective is to obscure the real signal by injecting a suitable level of noise-like interference into the victim system. For deception jamming, an exact knowledge of not only the enemy radar frequency, but all other transmission parameters is required. This technique, in away , is spot or point jamming of a more intelligent nature. Deception jamming is generally used for self-protection applications against terminal threat weapon types which employ tracking radars.

Deception jamming can either be manipulative, where friendly emissions are altered or simulated to mislead the enemy, or imitative, where false information is introduced into enemy receivers by imitating his signals.

Within the general class of deception jamming, three main electronic techniques to return false signals have been developed. These signals have characteristics similar to those of the radar, thereby deceiving the radar into erroneous conclusions about range, velocity or azimuth.

4.7 Range deception.

Range deception jamming is used to foil missile guiding radar systems where the tracking radar guides the missile (or other defensive measures) to the target in range by locking a range gate on to the target. This range gate delays the target echo and its position is relayed to the missile to be used for intercept information.

A range deception jammer, called a 'range gate stealer', attempts to break the tracking lock on itself by capturing the radar's range gate with a false echo and then moving it off to a false range (time) location.

4.8 Velocity range deception.

In velocity range deception, the Doppler shift is interfered with. In the deceptive velocity jammer operation, the CW (continuous to the wave) illuminator signal is detected by the jammer and a exact false, strong Doppler-shifted signal is sent back to the radar. The radar locks on to the incorrect Doppler signal and the jammer slowly sweeps the false signal's frequency more away from the actual Doppler frequency of the target. used When the radar has been led far enough away in frequency, the jammer is turned off and the radar is once more left without a target.

4.9 Azimuth (or angle) deception.

This is another deceptive ECM technique that degrades a tracking radar's ability to develop the correct azimuth and/or elevation data of a target. This technique repeats a replica of the received signal with an induced amplitude three modulation which is the inverse of the victim radar's have combined transmitter and receiver antenna scan patterns. An azimuth deception jammer, called 'inverse gain radar repeater' is normally used to deceive a conical tracking radar.The techniques of range deception, velocity deception and angle deception can also be applied against surveillance radars.

4.10 Smart noise Jamming.

A hybrid type of jamming which incorporates some of the features of both spot or barrage noise and deception jammers is called a 'smart noise jammer'. This is a repeater-type jammer used in a transponder (a device that sends a signal whenever It receives a certain command from a distant station) mode to generate responsive noise ten (the signal sent out by the transponder is called the 'response') over a short span of range, synchronised to the victim radar. This type of jammer generates a noise burst which is 'on' before and after the actual target return thereby covering the true return. This type of jammer allows a low powered repeater to respond to a number of threat radars by time sharing.

Deception jammers are generally more sophisticated and of higher complexity than noise jammers. The main reason for the higher complexity is that their performance characteristics must be more closely matched to those of each type of the system to be jammed than the performance characteristics of a noise jammer. There is also a need for more detailed knowledge of the victim system's performance parameters and modes of operation, both in advance and in the course of the actual jamming mission. This need can be met using ELINT equipment in order to provide real-time analysis of the system's transmissions.

Modern ECM systems employ a 'look-through' mode to provide periodic monitoring of the threat environment while simultaneously jamming multiple emitters. The objective of a jammer look-through mode is to allow the operating jammer to determine its own effectivness, such as correct tuning and sufficient power level, while it is simultaneously jamming the victim emitters.

4.11 PASSIVE ECM

This involves deception of enemy's system by employing confusion reflectors. This may be achieved either by chemical or mechanical means. This type of jamming is also sometimes called 'Expendable Countermeasures' (means an ECM device which is used up in its employment). Chaff and flares are the important examples. In its broadest sense, it not only uses the expendable passive ECM devices but also expendable active devices. These latter devices may be either jammers or deceivers, depending upon the particular effect desired.

4.12 Chemical Jamming

Smoke is the oldest countermeasure known to man. Long before radar had become the mainstay of battle operations, visual sighting was the only means of locating and aiming at enemy gunners. One way to confuse enemy gunners was to 'lay smoke', that is, to intentionally generate large clouds of billowing smoke, behind which friendly forces could then deploy, take aim unseen, and thereby avoid enemy fire until ready once again to come forth and battle. In the battle of Jutland in World War I, the German naval forces retreated under cover of smoke in order to protect their decimated flotilla from further losses.

The use of 'smoke', particularly against laser threats, has caused a resurgence of interest in recent times. Aerosols are the best chemical agents that are used as smoke, dust, mist or fog. They are used as obscurants (i.e., they decrease the level of energy available for the functions of seekers or vision enhancement devices).

Aerosols, in fact, are fine solid or liquid particles dispersed in the atmosphere. The entire family of aerosols are not used for countermeasure applications. Only some specifically selected chemical materials are fit for this purpose. The aerosol particle size and type are chosen in such a way that it allows both scattering and/or absorption of radiations from electro-optical system targets. Some forms of aerosols can partially absorb microwave signals also.

Thus aerosol particles both scatter and absorb light. However, the scattering effect usually is the dominant source of attenuation for a countermeasure application. The most common types of smoke (i.e., aersol material) in use are those using either white phosphorus having total obscuring power (TOP) of 6600 ft^2/lb, MBA aerosol having TOP of 5900 ft^2/lb, hexachloroethane (HC) having TOP 4450 ft^2/1b or fog oil having TOP 3200 ft^2/lb.

To be more effective, the suspended aerosol or resonant particle should have a small mass and a large scattering cross-section. This is usually obtained by using resonant size particles with a high index of refraction. In this sense aerosols are somewhat similar to chaff.

Aerosols are ideally suited for the defence of small, valuable, ground-based targets against visual and laser-directed air-to-ground weaponry .An automatic or remotely operated system can provide quick, temporary protection cloud in the immediate presence of threat.

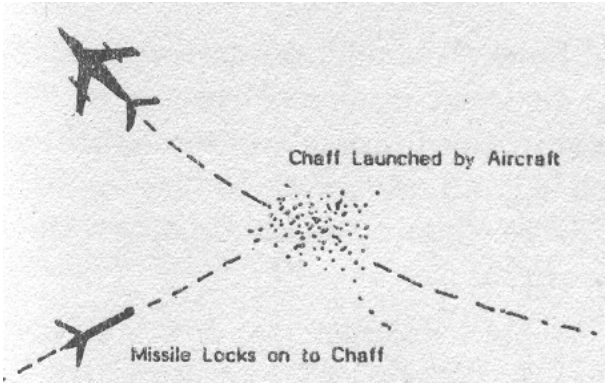
The use of aerosols or smoke, to diffuse the coherent light beam used in a laser is still being widely investigated by researchers for defence applications.

4.13 Mechanical Jamming

This involves deception of enemy's electronic system by use of specially designed mechanical objects. These (include such objects as chaff, flares, RPVs, drones, etc.

4.14 Chaff.

There exists today an electronic equivalent to 'smoke'; it is called 'chaff ' (during World War II, called 'window'). Instead of scattering or absorbing electromagnetic energy, as in the case of smoke, it reflects electromagnetic energy to confuse or deceive an enemy system.



Chaff consists of either thin metallised glass or plastic rods, or thin metal foil or wire, the dimensions of which correspond to half a wavelength of the frequency used by the enemy radar. Cartridges packed with large quantities of chaff of different sizes are dispensed from aircraft, ships or vehicles. The chaff forms a cloud of metallic dipoles, as shown in Fig.9 and appears on enemy radar screens either as a blot (i.e., clutter) masking the real target, or as hundreds of false targets around the real one. This effectively breaks the track of radar guided missiles. In 1973, Israeli boats used rapid blooming chaff to screen themselves from the radars of Syrian gunboats equipped with Styx missiles.

The dimensions and physical orientation of chaff is an important consideration in its design and use. An analysis of the action of chaff shows that for maximum signal return one should make its length a multiple of one-half wavelength of the radar signal. This length maximises the sympathetic electrical resonance effect, analogous to that which occurs with sympathetic vibration of a tuning fork or piano string. It is also observed that the thinner the chaff, the more pronounced and frequency-specific is the resonance effect. Also, the radiated energy is strongest broadside to the individual chaff element, similar to a tuning fork. In essence, each chaff element behaves like a single dipole with a doughnut-shaped pattern.

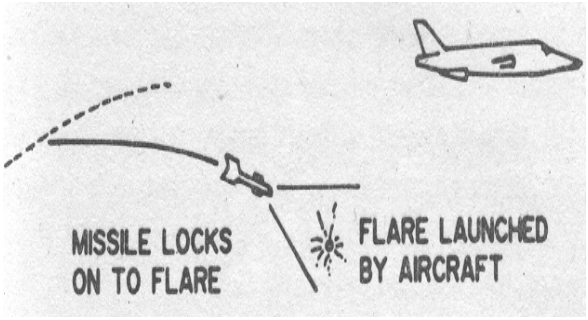
Thus chaff is both frequency-and orientationsensitive. Both these characteristics are compensated for by the typically small cross-section of chaff, which means that large quantities of chaff can be packaged in a small volume. Thus, one can use chaff of several different lengths in the same package to be effective against radars of widely different frequencies. Because of their small size, the chaff elements are randomly oriented upon dispensing. Thus their effectiveness becomes ominidirectional.

Chaff is usually packaged in units about twice the size of a cigarette pack. When this unit is dispensed in the atmosphere it creates a radar echo similar to that of a small aircraft. If a stronger echo is needed, then two or three units are dispensed simultaneously. Chaff is generally used to protect tactical aircraft, strategic aircraft and ships.

4.15 Flares.

A flare is a pyrotechnic (i.e., like fireworks) target launched from an aircraft or other vehicles causing infrared homing missiles or other optical devices to be decoyed away from the true target.

The flares are dispersed when the heat-seeking missile approaches its target to divert the missile from its target. This is illustrated in Fig.10.



Most dispensers used for chaff can also be used to drop infrared flares capable of confusing heat-seeking missiles. In addition to protecting tactical aircraft, flares also playa role in protecting strategic bombers. Early infrared (IR) weapons were very vulnerable to decoy flares, but most recent designs use flares or dual operating frequencies in order to estimate roughly where the peak level of IR output lies.

4.16 RPVs/drones/projectiles.

In recent times, other means of deception that have become increasingly popular are RPVs (remotely piloted vehicles) , drones and some special type of projectiles. An RPV is an aircraft platform that is under remote but direct control, while a drone functions with a pre-set sequence and has no remote control. RPVs normally utilise drones, controlled rockets, gliders, small boats, trucks or other unmanned remotely piloted vehicles as ECM support to assist strike vehicles in penetrating radar-missile-defended target areas by jamming, ejecting chaff, dropping expendables or decoys (low-cost vehicles; usually with some form of radar target size augmentation, that fool the hostile force into thinking that the decoy is a larger and higher-value vehicle) , acting as decoys themselves, or performing other ECM related tasks.

In other words, these decoys (RPVs, drones, projectiles and other aircraft-type vehicles) are usually smaller than a typical aircraft target; but are made to appear larger electronically.The intention is to trigger con' the enemy radar, thus forcing them to reveal their presence, location and operating characteristics (i.e., the radar's electromagnetic signature). All this information is quite vital to those forces which are trying to counter such a radar threat. For example, this tactic of using RPV s was employed by Israelis in the 1982 Lebanon War , to ascertain the microwave radio frequencies used by the Syrian SAM-6 surface~to-air missiles, which were later on sucessfully destroyed on their sites by the Israeli forces.

RPVs, drones and special projectiles containing chaff, flares or jamming equipment are also widely used to deceive the enemy. The jamming equipment may consist of simple jammers, radar signal repeaters, deception jammers or systems which simulate the target's electromagnetic signature. The main objective of these decoys is to draw enemy fire away from the real target. Consequently, they are made to follow the most deceptive path away from the real target. The active miniature jammer of low cost and limited power output is also an expendable like chaff, flares, etc. The placement of these active miniature multiple jammers in the vicinity of the threat emitter saturates its receiver and overloads its data processing system. The net result is delay or confusion in the detection of the real target. Delivery of such a small active expendable jammer could be accomplished using rockets, mortars, artillery, balloons, parachutes or the jammer could be contained in a remotely piloted mini-vehicle (mini-RPV). This ECM technique finds valuable applications in off-board jamming of anti-ship cruise missile, battlefield communications jamming and air defence radar jamming.

With either passive or active expendable ECM systems, the objective against radar threats is to provide a time window in which the target is shielded from radar detection

and tracking. Another advantage of expendable ECM systems is that they are operated from a distance , without involving much risk.

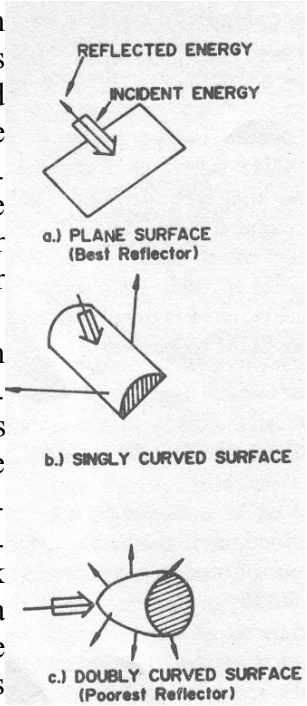
Active expendable ECM systems are generally more expensive than passive expendable ECM systems such as chaff or radio-directive decoy reflectors, and hence tend to be used where passive systems are not very effective. This generally occurs in the lower frequency range, usually below I GHz, where chaff dipoles are no longer practical because they require long (about 750 feet), non-resonant streamers, called 'rope'. Active expandable jammers can use either noise or deception jamming techniques, because of their simplicity. Of the passive expendable jammers, chaff is the oldest, and still the most widely used radar ECM technique.

4.17 RADAR CROSS-SECTION MODIFICATION

Another class of ECM includes such techniques which allow drastic reduction of the radar cross-section of a target. Reduction of radar cross-section of a target decreases the possibilly of its detection by the radar. This may be achieved by use of some specific mechanical and chemical means. A great deal of research has been done in this area, with the results conjured up in a single world 'stealth'. Following a..e the important means for the reduction of radar cross-section of a target.

4.18 Proper Design

Design of the target (say aircraft) and its orientation plays an important role in the reduction of its radar cross-section. Echoes from curved surfaces are smaller as compared to echoes produced from the flat surfaces because the resonant effect is less and the resultant re-radiation will be distributed in several directions. Keeping this in view, modern aircraft are designed to minimise the amount of flat surface area which might act as a good radar signal reflector. Where possible, all surfaces are made either cylindrical or conical, as shown in Fig. I 1 , thus reducing the possibility of reflections. The effect of surface curvature of an aircraft also depends on its orientation with respect to the radar. For example, if the aircraft is nose-on to the radar, then not only is the effective cross-sectional area minimum, but the surfaces are most doubly curved and the major re-radiation will be to the side. Thus, the radar echo will be small for a mono-static radar. However, when the aircraft is broadside to the radar it will look mostly like a flat surface; thus its radar echo will be largest for a mono-static radar. In practice, it is not unusual for the broadside radar cross-section of an aircraft to be as much as 500 times greater than the nose-on cross-section.



4.19 Radar Absorbing Material

To reduce the radar cross-section of an aircraft still further the aircraft skin is coated with an electromagnetic absorbent material, also called 'radar absorbent material' (RAM). Many non-metallic materials such as mono-filament carbon-reinforced material and new types of fibre glass have proved to be very effective as radar absorbent materials. Such special electromagnetic absorbing coatings are given to the outside of planes. Thus, much like a man wearing a black suit at night, the major portion of the electromagnetic energy is absorbed instead-of being reflected, making it difficult to locate the object.

4.20 MODERN ECM SYSTEMS

As discussed earlier, there are two basic types of radar ECM, jamming and deception. The general characteristics of each type are summarised in Table I.

Table I: General characteristics of the two basic types of radar ECM

(i)	General type	Jamming	Deception
(ii)	Equipment types	Spot jammer Barrage jammer Sweep jammer	False target Generator Repeater Gate-stealer Track breaker
(iii)	Primary effect	Deny position and velocity	Produce false position and velocity
(iv)	Signal type	Dissimilar to radar echo	Similar to radar echo
(v)	Data processing required by jammer	Frequency set on	False position False velocity Frequency set on
(vi)	Power required by jammer	Proportional to radar peak power	Proportional to number of false power targets and radar coverage power
(vii)	Primary problems	Minimum effective range Frequency Coverage Look-through Passive detection	Credible motion Credible target Echo-broadening Passive detection

From this Table it is evident that, in general, jammers have a simpler data processing requirement, a simple signal requirement, and conceal the aircraft at the expense of requiring more power. Deception, on the other hand, has a smaller power requirement per radar at the expense of more stringent signal waveform and data processing requirements. In addition, deception makes no attempt to conceal the aircraft; rather, it seeks to distract the attention of the defence system through false or misleading information.

Modern ECM systems are designed to detect, classify, and identify hostile radar threats, and to direct timely (within milliseconds) jamming responses automatically against these threats on a priority basis. The more advanced current ECM systems are designed specifically to cope with pulsed and CW radars. The high threat density of these types of emitters requires that the ECM system operate under computer control, which functions to distribute the jamming resources in an efficient manner.

A modern ECM system is intended to counter surface-to-air missiles, anti-aircraft guns, and air-to-air missile fire control radars, and to degrade, by noise jamming, early-warning and ground-controlled intercept radars.

A typical modem ECM system consists following functional parts.

i. An ESM system which intercepts and develops attributes (e.g. pulse descriptors) of the threat.
ii. A signal processor which filters the threat data to determine the characteristics of each threat.
iii. A digital computer which compares the threat data against a pre-stored threat library and establishes the prioritised response to each detected threat.
iv. A technique generator which translates the prioritised response into appropriate modulations suitable for applications to the jamming transmitter.
v. A jamming logic which acts. as a control switching matrix to select the proper jamming transmitter and point the steerable antennas (i.e., phased array) at the threat or select the proper fixed antenna sector .
vi. Jamming transmitters and antennas covering the concerned bands of interest.

The role of the digital computer is central to all modern ECM systems. It assimilates all the collected threat data and compares them against stored threat data to make a decision on the relative priority of each threat. It provides real-time solution to the complex problem of allocating the jamming resources of the ECM system in the spatial, time, power and spectral domains.

4.21 COMMUNICATIONS ECM

The discussion up to this point has emphasised ECM against radar targets. This is the most prevalent type of ECM which is employed in the airborne or ship-based systems. However, in land-based systems, a major part of EW activity is the interception and location of short range and low power HF, VHF and UHF radio transmissions used by the enemy in forward battle areas. Typical ECM systems include both interception and direction-finding (DF) capabilities.

The philosophy of ECM against communications emitters is somewhat different than that against radars. A major reason for this is that intercepted communications traffic becomes a major intelligence source for the commander. Also, the density and methods of operating tactical radios, particularly the netting, is different from radar. The essential

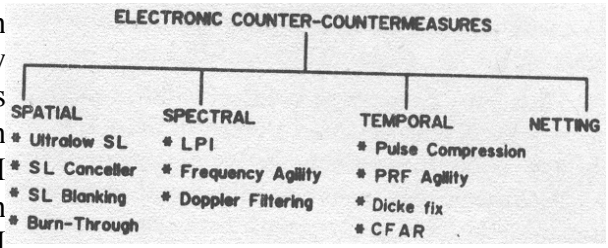
ingredient of communicaions jamming is radio direction-finding. Once a tactical communication emitter is located, there are three options open to battlefield commanders. These are: physical destruction, intelligence exploitation, or electronic jamming. An accepted military principle is that enormous tactical advantages can be gained b-y jamming or feeding confusing signals into the enemy forward communications net than by its actual destruction.

5. Electronic Counter-Countermeasures

Electronic counter-countermeasures (ECCM) is defined as actions taken to ensure friendly use of the electromagnetic spectrum against an EW threat. Thus ECCM is the art of reducing the effectiveness of an EW threat so that the cost of effective EW becomes prohibitive for the enemy.

There is one fundamental difference between ECCM and ECM. ECCM is mostly concerned with techniques which are embodied in the design of electronic equipment (e.g., radar and its constituent parts like receiver, transmitter, etc.) while ECM usually requires a separate item or unit of equipment which operates in its own right and not as an adjunct to another system.

5.1 ECCM TECHNIQUES



Many ECCM features are incorporated in the radar design. Thus ECCM is mostly concerned with the discussion of various radar design principles that have been developed on the basis of various ECM threats which a particular radar system can possibly encounter. Most of the ECCM techniques are based on the characteristics of transmitted radar pulse, which in turn, depends upon the radar parameters like power, frequency, PRF, pulse length, antenna gain, antenna polarisation, antenna scan, receiver's probability of intercept, etc.

Today, a wide range of ECCM techniques are employed. Some of the important techniques, shown in Fig.12, are discussed in terms of spatial, spectral, temporal and netting domains.

5.1.1 Spatial ECCM

This category of ECCM includes techniques which are space-based. Some of the spatial ECCM techniques are mentioned in the following.

5.1.2 Ultralow side lobes.

A radar antenna having very , side lobes in its spectrum is an important ECCM design technique. Ultralow side lobes prevent a jammer deceiver from affecting the radar at many azimuths. Low side lobe levels also make the job of anti-radiation missiles more difficult.

5.1.3 Side lobe banking (SLB).

This is also a radar ECCM and anti-interference technique that prevents some of the unwanted pulse energy entering the side lobes of a radar antenna from adversely affecting the radar's operation.

This device employs an auxiliary wide-angle antenna and receiver to sense whether a received pulse is from the side lobe region. If so, it is blanked from the output signal. This technique uses an omni-directional antenna and compares relative signal strength between the omni and the radar antenna. The omni- channel (plus receiver) has slightly higher gain than the side lobes of the normal channel, but less gain than the main beam. Therefore, any signal that is stronger in the omni-directional channel must have been received from a side lobe, and, therefore, is blanked. This technique is very effective in removing deceiving signals.

5.1.4 Side lobe canceller (SLC).

This is another radar ECCM technique, for use on a surveillance or tracking radar, that prevents some of the unwanted noise jamming energy that enters the side lobes of the radar antenna from adversely affecting the radar's operation.

This device employs one or more auxiliary antennas and receivers to allow linear subtraction of interfering signals from the desired output if they are sensed to originate in the side lobe of the main antenna. This technique also employs the same antenna and receiver configuration as the SLB, except that a gain matching and cancelling process takes place. Except the target signal, all false signals entering the side lobe of the main antenna get cancelled at the output. This technique is quite effective against a single noise jammer. With multiple jammers at various azimuths, however, the performance of this device is not very effective.

5.1.5 Monopulse technique.

This is a simultaneous lobing radar technique that measures both azimuth and elevation directions of a target on the basis of a single pulse, as distinguished from techniques such as lobe switching or conical scanning, in which angular location of a target is done on the basis of multiple pulses.

This technique of angle-tracking a target is inherently a strong ECCM feature, because amplitude modulations of noise or of repeated radar pulses from an ECM unit aboard the target, i.e., self-screening jamming, has little or no effect on the monopulse tracking operation. This is not the case with sequential lobing or conical scanning, which can be easily jammed.

5.1.6 Burn-through technique.

Burn-through means appearance of a true target on a radar indicator in a jamming environment. Thus, a burn-through mode is an ECCM technique, in which a radar increases its energy on the target in order to increase its ability to detect that target in a jamming environment. A burn-through radar is designed for a very high effective radiated power (ERP), by using high transmitter power or high antenna gain or both. The idea is to illuminate targets in a jamming environment with high amounts of average power to increase the detection range of these targets. Thus a radar can detect a target up to its burn-through range (i.e., radar-to-target slant distance); any target located at distances farther than the burn-through range cannot be easily detected by the radar.

5.1.7Spectral ECCM

This category of ECCM covers frequency-based techniques. Some of the spectral ECCM techniques are discussed in the following.

5.1.8 Low probability of intercept (LPI) technique.

The substantial transmitter powers radiated by most modern radars allow them to be detected by relatively modest intercept receivers in both their main lobes and side lobes. The interception of radar transmission ultimately leads to vulnerability through the use of either ARMs or ECM against a radar. The denial of signal interception would protect radars from most known threats. This is the main objective of LPI radar. It attempts to escape detection by an intercept receiver through a combination of actions. The two most significant features associated with an LPI radar are the spread spectrum transmissions and the low antenna side lobes.

In spread spectrum transmissions, the transmitted signal is spread over a large frequency band in such a manner that the the enemy ESM receiver finds it hard to detect the signal. The jamming will be less effective because it will have to be spread over a wide frequency band.

In low antenna side lobes, the design of an antenna is made in such a way that it produces low side lobe levels in its radiation pattern. Phased array radars are quite ECM resistant, so it is very difficult to jam such systems.

5.1.9 Frequency agility.

This technique refers to the radar's ability to quickly change its frequency within its operating band. Pulse-to-pulse frequency shift, or changing the transmitter frequency radically during every interpulse is the ultimate in frequency agility. Frequency agile radars are difficult to jam.

5.1.10 Doppler filtering.

This ECCM technique is for use on a tracking doppler radar to detect doppler targets and to aid in defeating velocity deception techniques. An MTI (moving target indicator) pulsed radar system uses a number of gates and corresponding narrow bandpass filters to discriminate moving targets from a background of clutter or slowly moving chaff particles. In essence, Doppler filtering is a radar ECCM and anti-clutter technique.

5.1.11 Temporal ECCM

This category of ECCM includes such techniques which are time-dependant or time-based. Following are some of the temporal ECCM techniques.

5.1.12 Pulse compression.

This is an ECCM technique in which a pulse radar transmits long pulses to increase the energy on a target, while still retaining the target range resolution of a short pulse transmission.

Pulse compression technique uses matched filter for discriminating against signals that do not correspond to the transmitted coded signal. Its implementation involves stretching the transmitted pulse and compressing the received pulse. It permits an increase in an average transmitted power (without increase in peak power) with no loss in range resolution.

5.1.13 Pulse repetition frequency (PRF) agility.

In this technique, PRF (i.e., the rate of transmission of radar pulse) is rapidly varied at a random rate so that the false targets appear jittery or fuzzy on the radar scope. An alternative to PRF agility is to change the PRF momentarily. This causes the false targets to change their position on the scope.

This is a pulse radar ECCM and/or anti-interference technique for use on a search or track pulse radar to degrade the effectiveness of false target repeaters, to eliminate blind speeds in MTI systems or to increase the radar's capability or compatibility in a dense signal environment.

5.1.14 Dicke fix.

This is an ECCM technique to counter continuous wave jamming, swept spot-noise jamming, and other related ECM techniques, which uses a wide-band IF amplifier and a limiter ahead of the normal bandwidth IF amplifier in a radar receiver, so that the recovery time from the effects of the swept jammer can be rapid. The Dicke fix or wide-band limiter device can provide some clear unjammed ranges where the radar can operate efficiently.

Dicke fix is, thus, a technique that is specifically designed to protect the receiver from fast sweep jamming. The basic configuration consists of a broad-band limiting IF amplifier, followed by an IF amplifier of an optimum bandwidth. The limit level is preset at approximately the peak amplitude of receiver noise. The bandwidth may vary from 10 to 20 MHz, depending on the jamming environment. This device provides excellent discrimination against fast sweep jamming (10-500 MHz) usually something of the order of 20 to 40 dB, without appreciable loss of sensitivity.

5.1.15 Constant false alarm rate (CF AR).

This is a radar receiver ECCM technique wherein the receiver adjusts its sensitivity as the intensity of the undesired signal varies. This makes the functioning of radars possible in an environment where interference due to signals from clutter, rain, jammers and other radiating sources are present. These undesired signals can obscure real targets on the radar display or overload a computer so as to degrade decisions on absolute detection threshold criteria. The CF AR technique keeps the detection of false alarm rate constant when the radar is receiving these undesired signals. CF AR docs not usually permit thc detection of a target if the target is weaker than the jamming, but it does attempt to remove the confusing effects of the jamming. Thus, CFAR does not give immunity from jamming; it merely makes the operation in the presence of jamming more convenient by making the receiver less sensitive.

5.1.16 Radar Netting

Up to this point the discussion was limited to ECCM techniques which are applied to a single, isolated radar . But a single isolated radar almost never exists. There are usually at least two or three radars that feed information to a central point from where the commander directs the conflicts in the battlefield. This combination of radars, often called a 'radar net', increases the potential ECCM capability of the system.

The radar netting has many advantages. For example, an air defence radar allows frequency diversity. This practice of operating radars in many different frequency bands immensely complicates the ECM problem, since the enemy must counter every frequency if he has to succeed in denying the defence accurate tracking information. Another advantage of radar netting is that it allows the defender to do triangulation (i.e., a process of locating an emitter by using crossing direction-finding signals from multiple receiving sites based on passive detection). The netted radars can function as an excellent ECCM device, provided the central node has some sort of automatic radar data control and data extraction facility. Ideally, the central control must have infinite data storing and processing capacity so as to avoid the saturation of the system at any stage.

A large number of ECCM tactics or methods have been developed over the years as a result of continuous improvements in radar design philosophy and signal processing techniques. Only a few were discussed in the above paragraphs. A comprehensive list of all radar ECCM techniques is given in Table 2.

Table 2: List of ECCM techniques

Angular Resolution	Matched Filtering
Automatic Gain Control (AGC)	Monopulse Tracker
Autocorrelation Signal Processing	Moving Target Indicator (MTI)
Automatic Cancellation of Extended Targets (ACET)	Multifrequency Radar
Automatic Threshold Variation (A TV)	Phased Array Radar
Automatic Tuner (SNIFFER)	Polarisation Diversity
Automatic Video Noise Levelling (AVNL	Polarisation Selector
Bistatic Radar	PRF Discrimination
Coded Waveform Modulation	Pulse Coding and Correlation
Compressive IF Amplifier	Pulse Compression, Stretching(CHIRP)
Constant False Alarm Rate (CFAR)	Pulse Edge Tracking
Cross Correlation Signal Processing	Pulse-to-pulse Frequency Shift (RAINBOW)
Cross-Polarisation	Random-Pulse Blanker
CW Jamming Canceller	Random Pulse Discrimination (RPD)
Dicke fix	Range Gating
Diplexing	Range Gate Memory
Frequency Agility	Side Lobe Blanker
Frequency Diversity	Side Lobe Canceller
Guard-Band Blanker	Side Lobe Suppression (SLS)
High PRF Tracking	Staggered PRF
Inatantaneous Frequency Correlator	Transmitter Power
Integration	Variable Bandwith Receiver
Inter-Pulse Coding	Variable PRF
Jamming Cancellation Receiver	Variable Scan Rate
Jittered PRF	Velocity Tracker
Logarithmic Receiver	Video Correlator
Main Lobe Cancellation	Wide-Bandwidth Radar
	Zero-Crossing Counter

5.2 COMMUNICATIONS ECCM

The second major military use of radiated electromagnetic energy is communications-sending of messages from one element of force to another. The radio communication bands that are most commonly used by the military are---HF band (3-30 MHz), VHF band (112-135 MHz) and UHF band (225-400 MHz).

The relationship. of electronic warfare to communications is more complex than to other uses of electromagnetic radiations, because both the presence of message and its contents are required to be protected during its transmission till it reaches its intended user. Determining the presence of enemy message is the goal of Communication Intelligence (COMINT), whereas providing protection to the contents of message during transmission is the goal of Communication Security (COMSEC).

Communication Security again has two parts. The first is Operating Methods, which deny the enemy access to the friendly messages and friendly communication channels, and the second is Cryptologic Methods, which deny- the understanding of the contents of friendly messages to the enemy even if he does get possession of them.

The Operating Methods are mainly concerned with common sense. For example, if the location of a particular aircraft in flight must be concealed then 'radio silence' is imposed. Normally, 'call signs'(to conceal the identity of the stations), frequency changes and operating time changes (to conceal the identity of operations) , pass words or authentication (to maintain the genuineness or identities of the sender and receiver), etc. are used for communication security .There are also a number of cryptologic methods or encryption techniques to conceal the contents of the message from the enemy, even if he does get hold of them.

To counter an ECM, on the order of priority or requirement, the communications ECCM equipment must adopt the following four doctrines or guidelines.

First priority. Prevent the transmissions from being observed by the enemy at all-imperceptibility (also referred to as low probability of intercept, LPI) .

Second priority. Minimise the possibility of extracting intelligence from such transmissions as may be detected- inscrutability.

Third priority. Maximise the chance of survival of the communications facility against the threat of physical attack-physical invulnerability.

Fourth priority. Maximise the chance of survival of communications facility against jamming--electromagnetic invulnerability.

There are a number of ECCM communication techniques to meet the above-mentioned priorities or requirements. Some of the important ones are mentioned here.

5.2.1 Encryption.

It reduces the intelligence value of an intercepted signal, because the enemy fails to understand fully- secured encrypted digital message.

5.2.2 Privacy.

This technique, though short of encryption, also plays an important role in the protection of a message to Some extent. The message is semi-secured and often it is of analog type. This technique has got much recognition due to the fact that even if it protects the message only for relatively short intervals, it is of great value in a tactical environment.

5.2.3 Frequency hoppers.

Slow and fast frequency hoppers are the current ECCM 'fashion goods'. They are relatively invulnerable to stand-off jamming, are less detectable and possess low probability of intercept, but they are vulnerable to modern direction finders.

5.2.4 Command frequency change.

They change frequency when under attack, and thus provide a limited means of evading a jamming attack.

5.2.5 Single sideband (SSB).

This technique provides low probability of intercept because no carrier is present.

5.2.6 Null steering.

This technique provides the survival of a communication facility against jamming. In this the outputs from two or more antennas are so combined that a 'null' may be steered towards jamming signals or other interference.

5.2.7 Null steering with smoke-screen jammer.

This is a very powerful technique for imperceptibility, inscrutability, electromagnetic attack, except in vulnerability to physical attack. This technique uses a 'clean jammer' on one's own working channel. The jammer, which is of an expendable type, is placed as far forward as possible towards the enemy and null steers are used to cancel the effect of the jammer on own-side communication.

5.2.8 Groundsat.

This is an unattended on-frequency VHF repeater that can be used to confuse the apparent point of origin of a transmission, which can hence deflect the physical attack. It is vulnerable to electromagnetic attack, which could take over the groundsat.

By adding a null steering device to both groundsat and receiver, great resistance to electromagnetic attack is achieved at the cost of complexity. Also, by using smokescreen jammer and the groundsat with the null steering, an unusual all round ECCM capability is achieved.

5.2.9 Spread spectrum.

Spread spectrum technique gives protection from interception and jamming, and thus provides a low probability of intercept. Spread spectrum produces very low energy density per channel in narrow-band receivers and per frequency band in wide-band receivers. It can, therefore, be entirely undetectable. Electromagnetic (EM) attack can be a disaster, but steerable notch filters can combat EM attack by line spectra.

5.2.10 Millimeter wave (MMW).

The millimeter wave region (30-300 GHz) consists of a number of bands. Without prior knowledge, the ECM system must be prepared to jam all the bands, which is a very difficult task. So, they provide increased immunity to unwanted detection.

5.2.11 Meteor scatter.

This technique uses the ionised gas trail produced by very small meteors entering the atmosphere to reflect VHF transmissions. Such longrange transmissions (say 1000 km and above) are difficult to jam or intercept.

5.2.12 Source coding.

Digital source coding, which involves irregular 'burst' data transmissions of short duration but relatively high data rate provides low probability of intercept.

The battle of electronic warfare--ECCM against ECM-thus continues and every day, new and more sophisticated technology is being called into use. The management and integration of large amount of data, increasingly of disparate origin and type, will be one of the major challenges for battlefield communications in the 1990s and beyond.

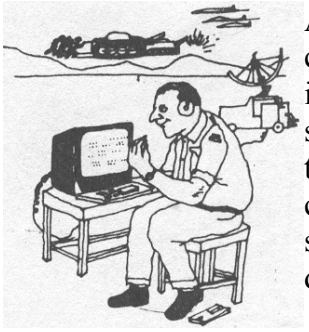
The battle of electronic warfare-ECCM against ECM-thus continues and every day, new and more sophisticated technology is being called into use. The management and integration of large amount of data, increasingly of disparate origin and type, will be one of the major challenges for battlefield communications in the 1990s and beyond.

6. Current and Future Trends in EW

The discussion of EW will remain incomplete if we don't discuss its current and future trends. Long experience and widely held expectations in the defence and other interested communities indicate that EW will dominate the battlefield of future, on land, sea and in the air. The reactive nature of the EW field as a response to the enemy's initiative is well known and serves to generate the requirements on which the present EW systems are based.

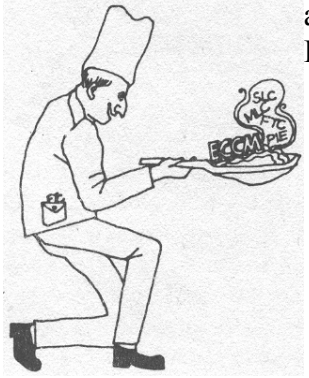
6.1 EW-A CONTINUING STRUGGLE WITH NEW DIMENSIONS

The history of EW development has been quite interesting and challenging. Radar was the first important development made by man after a long struggle with the application of radio waves in warfare. During the early days, radar when used in warfare, provided a remote, long distance, all-weather eye. Observation of warfare events on a radar scope was really a pleasure for the operator, as shown in Fig. 13. Man was not fully satisfied. He wanted to see events happening at still farther distances. He tried to increase the detection range by increasing the sensitivity of the radar but it resulted in many unwanted side- effects. These unwanted disturbances, called 'natural' ECMs-clouds, ground returns from trees, mountains, etc., and un-intentional man-made ECMs-returns from buildings, water tanks, ground vehicles, etc. began to make radar scope watching quite unpleasant. Later on, the advent of intentional ECMs like jammers and chaff made radar scope watching worse. There was nothing to see or hear of interest. Pity the radar operator in Fig. 14.



At this stage, the radar clearly required some medication to get cured from such a serious ECM disease. Man Went here and there in search of competent doctors and continued his struggle to find suitable medicines for the recovery of the radar. This resulted in the discovery and development of many kinds of medicines (now called anti-jamming or ECCM techniques). The learned specialists immediately came to the rescue of the radar with a full dish of 'alphabet soup' of Fig.15. This alphabet soup contained many ECCM techniques which were named after the abbreviations of many anti-jamming (AJ) techniques: ASB for Angle Sector Blanking, ACET for Automatic Cancellation of Extended Target, CFAR for Constant False Alarm Rate, FTC for Fast Time Constant, IFC for Instantaneous Frequency Correlator, LORO for Lobe-on-Receiver Only, MLC for Main Lobe Canceller, MTI for Moving Target Indicator, PIE for Pulse Interference Elimination, SLC for Side Lobe Suppression, ZCC for Zero Crossing Counter, etc. They poured this soup into the radar. As a result of this, the radar instantaneously became all right. The radar operator has also now

largely recovered and started watching warfare events with more renewed interest, as shown in Fig. 16. But the disturbances due to many intentional problems in warfare is not over for him once for all. The radar operator will still have unpleasantness of one form or the other. This interactive problem of ECM and ECCM is thus still going on. Man is continuing his struggle ceaselessly at many new fronts or dimensions of technology to get a more lasting or permanent solution to this EW problem.



6.1.1 CURRENT EW AREAS OF RESEARCH AND DEVELOPMENT

Due to the complex nature of the subject there are many and varied areas of research and development in the field of EW today. It is difficult to enumerate all the areas. However, there are some key areas which can be taken as most important and critical to a country's defence. Most of the world research efforts are focused around the following mission areas.

- Radiation detection and sorting in a dense signal environment
- Stand-off jamming for wide area penetration of enemy radar with minimum risk to the attacking force
- Extension of EW spectrum coverage to millimeter and optical wavelengths
- Decoys
- Airborne early warning and illumination warning
- Obscuration aids
- Radar and infra-red cross-section reduction
- High speed signal processing
- Microwave phased arrays
- Artificial Intelligence
- Simulation
- EW Integration

Each of these key or mission areas of research and development is correspondingly supported by a technical approach, as follows.

- Development of high speed, real-time Spectrum analysis by use of acousto-optic processing for100 to 1000 simultaneous spectral outputs

- Development of programmable high-power broad-band microwave amplifiers and high-gain radiators
- Development of tunable components suitable for power covering millimeter and optical wavelengths
- Development of expendable jammers, chaff and pyrotechnic flares
- Development of C^3, airborne early warning and laser-warning systems
- Development of aerosols and smokes that are effective over optical and infra-red spectra
- Development of low observables and stealth concepts, such as structure geometrics and absorptive coatings and paints that avoid high reflection
- Development of very-high-speed integrate circuits (VHSICs), submicrometer silicon technology, Use of gallium arsenide for even higher speed and strategic levels of radiation hardening in the digital area; surface-acoustic wave (SAW) devices, charge-coupled devices (CCDs) for correlators and filters, and acousto-optic Bragg-cell diffraction for spectrum analysers and correlators in the analog area; use of fibre optics in delay lines, signal processing and other EW applications
- Development of monolithic solid-state transmitter and receiver modules, including a digital phase shifter
- Development of expert systems for automatic EW data processing, threat analysis, resource allocation and decision-making
- Testing,. evaluation and development of new EW concepts and techniques, in addition to imparting training to EW systems operators
- Development of systems which integrate IE0/IR/RF sensors and jammers into a single hardware.

6.1.2 LEADING EDGE OF EW TECHNOLOGIES

The various key areas of research and development as mentioned earlier, are expected to generate a wide spectrum of technologies upon which the present and future EW systems will be built. In the following, the discussion is confined to a number of special topics that are related to the leading edge of today's EW technology.

These technologies mainly relate to functional parts of EW systems and other inter-related weapon systems, like antenna, transmitter, receiver, signal processing and other associated subsystems. These technologies show great promises and are expected to bring changes in future EW systems in terms complexity, sophistication and handling.

6.1.3 EW Antenna Technology

Almost all EW systems require some form of antenna. An EW antenna serves to couple transmitter signals into free space and receiver signals from free space into the EW system. EW antennas are different from other types of antennas used in radar or communications, by their broad-band, wide-angle coverage and diverse beam and a radiation pattern with appropriate polarisation characteristics which has the desired

spatial coverage. There are wide varieties of EW antennas, like spiral antennas, horn antennas, helical antennas, log-periodic antennas, dipole array antennas, etc.

Most of the EW systems in use today use fixed, wide-beam-width, broad-beam antennas for ESM applications and mechanically scanned or switched wide-bandwidth, narrow-beam antennas for stand-off ECM missions. But the mechanically scanned antennas are ineffective for simultaneous handling of multiple threats, which is quite common in a modern threat environment. To overcome this difficulty a new technique called 'electronic steering' has been devised. The electronic steering of an ECM transmitting beam is achieved through two approaches-the phased array and the lens-fed multiple beam array. This system provides wide-bandwidth, high efficiency, multiple threat handling capability, low side lobes and optimum signal-to-noise ratio in the presence of noise sources. Many more antenna developments are in progress.

6.1.4 EW Transmitter Technology

Three main components, travelling-wave tube (TWT), voltage controlled oscillator (VCO) and digital radio frequency memory (DRFM), are associated with a transmitter power source. TWT is a versatile source of RF power generation. VCOs allow a jammer to effectively function in a high signal density environment and respond to a variety of multiple threats. DRFMs are basically threat waveform storage devices which are capable of being used as exciters in a jamming transmitter. In this, first the threat information content of an RF signal is stored in the digital memory .The signal can then be reconstituted at some later time by sampling the digital memory. Emerging technology is playing a key role towards the improvement of size and performance of these components.

ECM jamming systems that evolved prior to 1970 generally employed cross-field type transmitting tubes (e.g., magnetrons and carcinotrons) which were used in noise jammers. As the threat. expanded, it became apparent that noise jammers needed to be supplemented with deception type jammers. In addition, power management concepts called for versatile RF transmission capabilities which could rapidly switch from one mode to another. This led to the extensive use of TWT amplifiers, which provided attractive characteristics like wide bandwidths, high gains, ease of modulation in the amplitude, frequency and temporal domains, etc., in ECM systems.

There are now two dominant types of TWTs-the helix TWTs and the coupled-cavity TWTs-which are found useful for ECM applications. The helix TWTs are used in broad-band operation for self-protection ECM applications. The heat dissipation properties of the helix structure generally limit the power handling capability of this type of TWTs, particularly at frequencies above 10 GHz. The coupled-cavity TWTs used in narrow-band operation are considerably heavier, but are capable of much higher power operation than the helix TWTs. They are extensively used for stand-off jamming applications, where maximum power is more critical than bandwidth. Atypical TWT operating at 2.5-8 GHz bandwidth can give 200 W power and at 7.5-18 GHz can give 100 W power. There is no currently available technology which has the potential to supplant the TWTs in the

foreseeable future. Thus, much efforts are being made towards the improvement of their performance in terms of broader bandwidth, higher power capabilities at higher frequencies, higher efficiency, greater packaging density, etc.

At present most ECM systems use TWT transmitters. However, recent development of solid-state gallium arsenide (GaAs) field-effect transistor (FET) amplifiers have made the use of these devices practical for ECM transmitters which operate in the mid-to high-microwave frequency range (e.g., 2-20 GHz). In addition to this, FET amplifiers offer a number of advantages over TWTs in the areas of reliability, linearity, low-voltage operation, small size and weight, less cooling required, broad frequency band operation, and lower noise figure. These potential advantages have resulted in considerable developmental effort aimed at increasing the power output of GaAs FET amplifiers. The main disadvantage of FETs With respect to TWTs for EW applications is that TWTs can ultimately supply far more power, particularly for wide-band use. Thus, the present state-of-art generally restricts their use to low or moderate power applications. However, the growing developments indicate that GaAs FET amplifiers may, in the near future, replace moderate power TWTs (e.g., 40 to 50W (CW)), and eventually challenge high power TWT amplifiers in the over 100 W class.

In some cases, high power FET amplifiers have been accomplished through power combining of multiple FET devices and using internal power matching techniques.

The most basic oscillators used in VCOs are transistor multiplier oscillator, Gunn oscillator and FET oscillator. An ideal VCO should have fast settling times, low post-tuning frequency drift and accurate frequency repeatability. Only fast settling time to the incoming frequency can allow the following of frequency agile radars. To be effective, the VCO should be able to tune in 50 to 100 ns and have a set on accuracy of the order of:t I MHz. These are critical areas on which the developmental efforts are concentrated.

DRFMs are key components of modern deception ECM systems. They have instantaneous digital bandwidths of the order of 400-600 MHz and threat storage capability for this bandwidth of the order of 50-75 μs. In this, increase of instantaneous bandwidth is the critical area of development. Advances in gigabit digital logic using GaAs technology is expected to increase the instantaneous bandwidth to the 1-2 GHz region or beyond.

6.1.5 EW Receiver Technology

The high threat density confronting the modern EW receiver is the driver of receiver technology .The EW threat scenario for a receiver is changing day by day. For example, during 1970s, the pulse density used to be about 40,000 pps (pulse per second), but, today it is touching the range of 1,000,000 to 10,000,000 pps. Also, the frequency range in 1970s used to be some selected portions of 2-12 GHz, but today the range is of the order of 40 GHz. Similarly, the pulse repetition interval (PRI) in 1970s used to be either stable or multiple pulse trains, but today it fluctuates in many modes--stable,jittered, staggered

or pseudorandom. Not only this, during 1970s the EW receiver used to confront such radar features as single frequency , inter-pulse processing, but today it is facing more complex radar features, like multiple frequencies, frequency hopping, spread spectrum, multiple agile antenna beams, intra-pulse phase shift, coded modulations, power management, digital processing, large time bandwidth product radar signals, increased duty cycles with lower peak power, bistatic operations, weapon systems using multi-mode seekers (IR, laser, RF), etc.

From the above description, it is evident that no single receiver can handle effectively such a dense electromagnetic environment. To meet the challenge of complex threat scenario, a wide variety of EW receiver architectures are employed as described in Chapter 2. They exhibit relative advantages and disadvantages in terms of sensitivity, selectivity, probability of detection, capability of handling frequency-agile signals, dynamic range, frequency accuracy, simultaneous signal resolution, susceptibility to ECCM, design reliability and cost, etc., to handle a specific threat situation.

An EW receiver covering frequency ranges 100 MHz-18 GHz, 26-42 GHz and 88-120 GHz consists of several components. Microwave multiplexing filters, microwave low noise amplifiers, doubly balanced mixers, pin diode switches, bandpass filter channelisers, local oscillators and fine channelisers using SAW filters are the most commonly used key components in the design of a microwave EW receiver. These components represent the key technology in EW receivers.

Many developments are taking place in low noise amplifiers and SA W delay lines. Most modern EW systems have replaced low-noise TWT amplifiers used in older equipment with wide-band low-noise RF solid-state pre-amplifiers which have high sensitivity. Surface acoustic wave (SAW) delay lines are the key components of channelised and compressive receivers. Their small physical size, high stability and excellent broad-band characteristics allow the construction of a large number of continuous bandpass filters and matched filters, which are most suited for real-time spectral analysis.

6.1.6 EW at Optical Wavelengths

The role of electro-optic/infra-red (EO/IR) techniques in modern EW has become increasingly important in recent years, particularly as a response to radio frequency (RF) and microwave (MW) countermeasures. The use of optically-guided anti-tank weapons, for example, proved an effective technique in the Mid-East wars. E0/IR (1200 Kilo GHz-20000 GHz) has thus earned an important place in EW. The modern EW designer or system planner who ignores the E0/IR portion of the spectrum does so at his own peril.

E0/IR techniques offer a number of advantages; for example, the wavelengths used are well separated from RF and MW portion of the spectrum, requiring the enemy to diversify his EW resources. Also, E0/IR signatures are typically multi-faceted; signal processing can be accomplished in the spectral, temporal and/or spatial domain. Small sizes of the devices due to extremely small wavelength or equivalently the high antenna gains of the small

apertures used provide additional advantages. The E0/IR systems thus find valuable applications in missile warning, over-the-horizon communications, night vision, surveillance, acquisition, fire control, laser designation and ranging. The heat-seeking sensor on missile systems is the most lethal utilisation of E0/IR technology. pyrotechnic flare which acts as a false target or as a decoy to the approaching heat-seeking missile is the most effective countermeasure used today.

However, these advantages are tempered by some drawbacks that can be of crucial importance in operating conditions. The E0/IR system primarily suffers from lack of all-weather capability; that is, clouds, precipitation and humidity can degrade or even negate an optical system. Also, optical systems are limited to line-of-sight applications. In addition, the optical surfaces are notoriously sensitive to dust, smoke and other particulates usually found in a battle area.

E0/IR is playing a key role in detection and signal processing techniques. Developments in sources (such as laser), detectors and signal processing are expected to give the system designer new flexibility in achieving high goals of exploitation of the total electromagnetic spectrum. The emergence of heat-seeking missiles has put more emphasis on the development of more pyrotechnic flares. Also, the recent emergence of laser threat has made the need for the development of laser-threat warning and response systems more urgent. Major problems lie in target background discrimination, optical channel obstacles m the atmosphere under water and dust. The E0/IR systems are expensive to design, engineer and build; however, with simplification of components and improvement in functions, their operation can be improved. Many development efforts in all these key areas are currently in progress.

6.1.7 EW at Millimeter Wavelengths (MMWs)

Millimeter waves (30-300 GHz) present new opportunities for a number of EW techniques. They find most promising applications in fire control, missile guidance and counter mortar/artillery location, due to their high angular precision and narrow antenna beams. This emerging set of applications of MMW systems is an adjunct or replacement for electro-optical or infra.:red (EO/IR) systems currently used in the battlefield, particularly for target acquisition and fire control. The MMW system is not blinded by smoke, fog or other atmospheric obscurants unlike the E0/IR systems.

In addition to this, MMW systems offer a number of other advantages over MW systems, like smaller antenna diameter required as compared ,to MW systems for same antenna gain/beam width, increased angular resolution, improved low-angle tracking, increased beam width, increased immunity from unwanted detection, increased Doppler sensitivity, reduced chaff illumination volume and smaller and lighter RF components. The high antenna gain and accompanying narrow beam width in MMW systems make them useful for efficient search of large volumes. Currently missile guidance is the most potential application of MMWs.

However, the MMW systems do have' some limitations. They are inferior to E0/IR systems in angular resolution. Also, MMW radars cannot be expected to provide the detection/tracking range of MW radars. They also show propagation attenuation at certain frequencies like 35 GHz, 94 GHz, 140 GHz and 220 GHz. The effects of propagation attenuation at these frequencies must be considered while designing, particularly the MMW ECM systems. Atmospheric attenuation can actually reduce the amount of jammer effective radiate;d power (ERP) required to jam a MMW radar in a self-protection ECM mission. However, the allocation of some absorption regions of MMW spectrum to raiders makes them quite attractive for LPI applications. Another limitation of MMW systems compared to MW systems is that several ECM techniques which are successfully employed in the MW region such as chaff and radar camouflage are apparently less effective at MMW frequencies. In particular, chaff dipoles made of aluminised glass fibres tend to become too small to be practicable above 35 GHz, and thus above 35 GHz spectral reflecting particles such as aerosols are required to be effective against MMW radars.

The propagation effects of MMWs are severe; however, at this stage of technology, ESM/ECM does not offer a significant problem to the MMW radar designer. A number of ESM systems which operate against MMW radars are currently under development. Also, parallelly, many investigations are going on in the development of suitable aerosols and smokes, which are most effective countermeasures against current MMW systems.

6.1.8 EW Low observability (or Stealth) Technology

The reduction of cross-section of a vehicle to escape detection falls into the class of techniques called 'low observables'. If low observable technology is carried to its ultimate limit, it is called very low observable or 'Stealth Technology'. Both low observables and stealth technology play key roles in ECM systems.

An aircraft is considered a low observable if its cross-section detectable by a radar can be reduced ten-folds. It produces many desirable effects that find use in ECM applications. The desirable effects of low observability are made clear in the following description.

It is well known that the effectiveness of a self- protection or stand-off ECM system in a radar jamming situation is a function of the ratio, σ/P_{eff} where σ is the shielded target's radar cross-section and P_{eff} is the ECM system's effective radiated power (ERP). Thus, for a selfscreening range or stand-off jamming range, the amount of required jammer ERP is therefore reduced in direct proportion to the reduction in cross-section. In other words, if the cross-section of a military aircraft is reduced by a factor of 100, the jamming ERP required to screen it from enemy radars is reduced by the same factor. This behaviour provides several desirable effects in favour of low observable technology. For example, an ECM system requiring large complex, high power jamming transmitters can be replaced with a system that is entirely solidstate. Low observable technology in this case provides the same level of ECM effectiveness while' reducing the complexity, cost and weight of the ECM components and increasing reliability .Low observable aircraft can penetrate through a dense threat environment to accomplish a mission, which is not

possible with a conventional aircraft. Thus low observable technology is expected to play an important role to improve the ECM effectiveness of current and future military aircraft.

Stealth technology is used to make an aircraft virtually impossible to be detected or intercepted. This is achieved by reducing drastically the radar cross-section of a target vehicle. There are apparently three methods for reducing the radar cross-section of an airborne vehicle. The first is to provide small radii, curved surfaces without any sharp discontinuities to the airborne vehicle. The second is through the use of anti-radar coverings. One form of anti-radar Covering absorbs the incident radiation such that reflections are suppressed. Another form uses interference coatings such that the incident and reflected waves mutually cancel. The third method is by controlling the reflected energy such that it is re-radiated away from its direction of arrival.

The air-launched cruise missile has significant stealth technology. Its radar cross-section is reduced to one-thousandths of a B-52 s~rategic bomber. It has been stated in the literature that stealth technology will be incorporated to some extent in all future US military aircraft and missile systems. Many details about stealth technology are, however, still highly classified.

6.1.9 EW Fibre Optics Technology

The emergence of fibre optics has opened a new window to the world of EW technology .As EW systems become more densely packaged and use high data rates at greater bandwidths, fibre optic components and subsystems offer the system designer new tools to address the complex issues required for physical and functional survival in the hostile operational environment that will be encountered ill the final decades of the century. Fibre optics has the ability to transmit great amounts of information over long distances with low power consumption and to provide immunity from electromagnetic interference, interception, ground loops and cross-talk. Fibre optics also promises lower cost, lighter weight systems with high reliability and survivability .

Fibre optics is currently finding use in fibre-guided missile system. The concept used in the fibre-guided missile can be. extended to a number of other fixed and mobile systems in which the fibre can be used to separate sophisticated signal processing from expendable portions of the weapon system. Their use in transmission lines and signal processing is under investigation for EW applications. In the next decade, the applications of fibre optics will grow beyond the role of being simply a noise-free, light-weight replacement for wire. By developing the necessary electronic interfaces and special purpose fibres, the great bandwidth potential of fibre optics will provide the EW systems designer with low loss, light-weight delay lines and antenna feed systems in which a single fibre transmission line will cover the complete electromagnetic spectrum from audio to microwave.

The only serious limitation of fibre optics is that if a fibre is damaged in the operation of a system, it is difficult to replace it immediately.

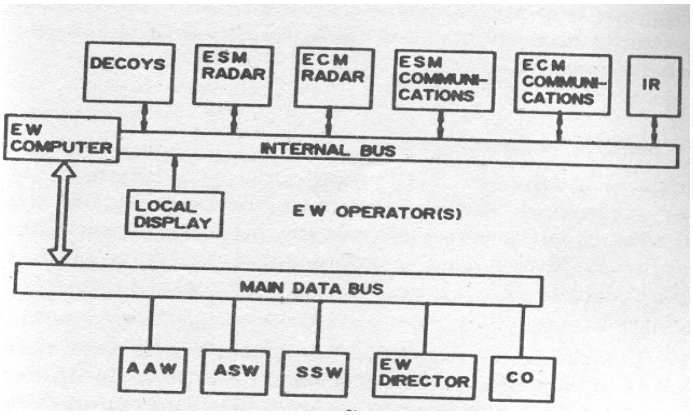
6.1.10 EW Signal Processing and VHSIC Technology

The present VHSIC technology thrust is aimed at meeting the high speed, low power consumption and military environment operation signal processing requirements in EW, communication, radar, precision guided missiles and microprocessors. Semiconductor technologies represented by VHSIC chips incl~e such classes of technologies as complementary metal oxide semi-conductor (CMOS), silicon on sapphire (SOS), N-type metal oxide semiconductor (NMOS) and oxide isolated bipolar (OIB).

A number of EW signal processors using VHSIC chips have been designed for intercepted signal analysis, like the CAM (content addressable memory), WAM (window addressable memory), etc. More advanced EW signal processors which can function effectively in a dense signal environment are under development.

6.1.11 EW Integration Technology

The integration of E0/IR systems and RF systems, as shown in Fig. 17, into a single hardware is another emerging design technology for the future EW systems. Such integration allows multi-sensor fusion and correlation which vastly improves total system performance and reliability. To be more cost-effective, integrated EW /EOW is used as a force multiplier. By integration, each sensor can make its unique contribution to the overall mission success.



Also, the integrated use of EO/IR and RF allows the optimum deployment of expendables and monitoring of their effectiveness against a threat. Integration can also provide defence against anti-radiation threats and optimum use of ECM.

For years, EW systems have been stand-alone systems in most of the applications. Further, various elements such as radar warning receivers (RWRs) and jammers in tactical aircraft have been separate and distinct systems with little or no interface. Now there is a trend and EW requirement to combine the RWR and ECM into a single system. Not only this; serious efforts are being made to integrate elements of EW and the weapon system or platform to gain overall control of the dense signal environment.

6.1.12 EW Artificial intelligence

Artificial Intelligence (AI) has added a new dimension to EW AI is an evolving computer technology which in the broadest sense attempts to capture in computer software the processes by which humans solve problems. It has been identified as one of the important military technologies of 1980s.

The reality of present AI applications is that they allow the implementation of a smart adaptive computer program, which can examine stored data and action on rules to draw inferences about the data. The inferences then allow the computer to interact with the knowledge source (e.g., user or input sensors), to request new data in an iterative manner until a conclusion is reached.

Several applications of AI have been identified in the field of EW. These include the fusion of multi-sensor data as a decision aid to threat analysis systems; to act as an expert adviser to decision makers in C^3I and C^3CM systems; reconnaissance, surveillance and intelligence data processing and threat assessment; sensor resource allocation and planning; and information retrieval and routing. Recently, AI has been used to compile and monitor the hostile air defence electronic order of battle (EOB) in support of a mission while penetrating enemy air space. AI, thus, has a lot of potential use in future EW systems.

6.1.13 EW Simulation Technology

Simulation generally means recreating a situation or environment for study and analysis of problems. EW simulation involves1he presentation of EW data as would be encountered in a realistic combat environment. Simulation technology serves many important functions in the field of EW.

The growing importance of EW in both strategic and tactical roles in modern combat philosophy, together with the advent of increasingly complex EW systems, have made it necessary to devise new and effective methods for the evaluation of equipment and the training of personnel. Traditional weapons can be tested and evaluated by firing against targets to prove their effectiveness. Similarly, their operators may be trained on the firing range. In contrast, since EW is primarily intended to thwart or deceive the enemy, rather than provide destructive effect, its effectiveness can only be demonstrated in the presence of a real or fully simulated combat environment.

EW simulators are important in many ways. For example, they are useful in the development of new concepts and techniques to counter enemy radars and weapons. Also, when accurate data is used to simulate the performance, it is possible to say with a high degree of confidence whether one's own new development will be effective or not. In other words, it provides a practical mechanism to assess the effectiveness of the developed EW systems or hardware. Further, in the case of EW, simulation is not an alternative method, but the only means short of war, of creating a realistic environment for evaluating a new receiver, signal processor designs, alternative jamming techniques,

optimisation of ELINT , checking ESM system performance and for training EW system operators.

A number of EW simulators have been developed in many advanced countries like USA for various purposes, such as dynamic electromagnetic environment simulator (DEES), air force EW evaluation simulator (AFEWES), and naval EW training simulator (NEWTS). The advent of minicomputer and the recognition by design engineers of its tremendous flexibility have both had a great impact on simulation technology. Formerly, both size and cost considerations had restricted the use of computers to huge simulator systems, but the relatively low-cost minicomputers have opened up a great many new field5 of application.

6.1.14 EW in C^3 Systems

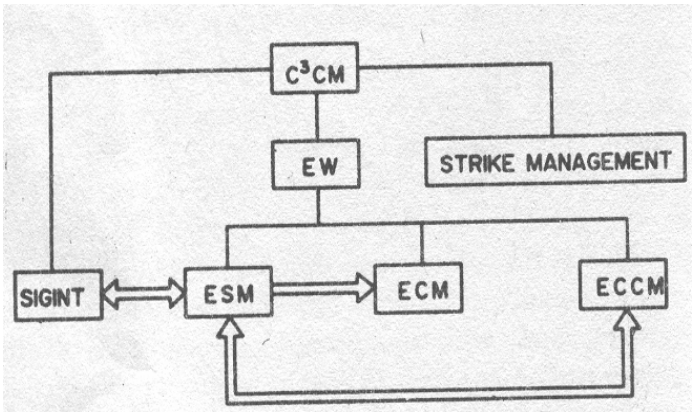
The ability of a military force to exercise command and control over its individual units, to communicate the basic data on minute-by-minute events to its control centres, and commands back again is considered to be one of the most vital factors in the success of modern warfare. This concept is commonly called Command, Control and Communications (C3) system or simply known as Command and Control system.

Any C3 system, whether strategic, tactical or theater, consists of the following basic elements.

- Sensor subsystems which gather information about location, movement, and activities of enemy and friendly military assets
- Navigation subsystems which inform friendly forces of their own location
- Command and confusion centres which assemble, integrate and display enemy and friendly force activities to decision-makers,. who then assess the threat and command appropriate response
- Communication links between the sensors and command centres and between the command centres and the forces to permit the transmission of information and commands.

An air defence system like Airborne Early Warning aircraft is the classic example of a command and control system. The latest development in this class is the AWACS (Airborne Warning and Control System). Due to the significant advances in modern technology .AWACS is the only system that can effectively provide vital command and control functions in a wide range of strategic and tactical missions through the entire spectrum of peace to war. AWACS, in short, provides full, long-range surveillance (detection, tracking and advance warning) of high-or low-flying aircraft (hostile as welt as friendly) , in a large volume of air space, as well as effective countermeasures to enemy ECM. Although AWACS are among the most effective air defence systems available today, they also happen to be the most expensive (30-90 million dollars).

Many command and control systems are also characterised as $C^3$1 systems,



where I stands for Intelligence. When C^3 systems are employed as force multipliers they become prime targets for enemy attack because, when neutralised, a force divider effect is accomplished. The neutralisation of C^3 systems is accomplished through the use of C^3 countermeasures (C^3CM). The basic methods employed with C^3CM are exploitation, deception, jamming and destruction. With this framework, as shown in Fig. 18, EW is a subset of C^3CM. The basic aim ofC^3CM is not only to neutralise the enemy $C^3$3 system, but also to protect its own friendly C^3 system from the enemy's destruction, jamming, exploitation and deception; an ECCM activity similar to that employed with radar and communication sensors.

EW plays an important role in the operation of modern C ^{3}systems. According to the modern concept of warfare, EW is considered as one of the basic elements of an overall military strategy , which when used in conjuction with other military assets, provides a means of neutralising a hostile force (force divider effect) while concurrently enhancing the power of a friendly force (force multiplier effect). EW thus, in modern warfare, aims at the neutralisation of an enemy's C^3 system while ensuring the capability of operating one's own C^3 system. To make the C^3 system ineffective, the overall system may employ any method like destruction, jamming, exploitation or deception. To protect the friendly C ^{3}system the overall system may employ a host of other methods. For example, destruction protection of a C^3 system may be achieved by employing such concepts as mobility, redundancy, hardening, distributed architecture and covertness; jamming protection may be achieved by employing such concepts as low probability of intercept, bistatic operation, decoys, netting, ECCM, mobility , and passive operation; exploitation protection may be achieved by employing such concepts as communications security (COMSEC), decoys, covertness, mobility and operation procedures; and deception protection may be achieved through such concepts as COMSEC, redundancy and operational procedures.

6.1.15EW in Space

The activities of EW have not been confined to battlefields on the Earth alone, but have extended their influence. to the space also. Man's conquest of space has brought a new dimension to arms technology , communication systems and method of surveillance with consequent innovations in the field of EW.

The use of satellites for military purpose began in 1958 when the United States launched the communications satellite SCORE which simply transmitted a pre-recorded message from space. Since 1958, more than 2000 military satellites, .initially experimental and later operational, have been launched by the USA and USSR alone, so as to have a secure world-wide satellite communications network free from all interferences including jamming and deception. Space EW now includes and will include for many years to come the military EW functions such as surveillance, reconnaissance, warning, survivable C3I, detection, targeting, weapon control, weapon delivery and target damage assessment. Till now about a hundred reconnaissance and early warning satellites like Ferrets of USA and COSMOS of USSR have been launched for electronic reconnaissance on ICBM launchings in general and 'to gather electronic intelligence on friendly and enemy radars. The ELINT operations through satellites are conducted to satisfy a variety of military requirements like location of hostile elements, updating of hostile force electronic order of battle information, obtaining information on specific transmitters and emissions, testing of hostile force ECM capabilities, evaluation of hostile force command and control procedures, and a host of other intelligence functions. To make the functions of ELINT satellites ineffective, there are a number of anti-satellite systems today.

Military space systems are making the transition from their two-decade old role of mission support, principally strategic intelligence gathering and long-haul point-to-point communications, to active missions requiring reliable operation during warfare. A wealth of self-protection techniques are being designed into spacecraft to defend them against various levels of jamming, attacks from anti-satellite weapons, and electromagnetic pulse (EMP) effects.1'he most promising survivability enhancements now being reviewed for possible integration to next generation space-based systems are-laser shields, optical manoeuvering/evasion, EMP hardening, orbital decoys, ECM, stealth or low observables, spacecraft proliferation and high-altitude orbits. There is a growing race between ECM and ECCM systems employed in space by the Superpowers. To defeat the Russian jammer system,the United States is building systems like the MILSTAR (Military Strategic- Tactical and Relay) EHF(Extremely High Frequency) satellite communications system which offers both extensive anti-jamming as well as laser and EMP hardening. The system has many ECCM features built into it like frequency hopping over a very wide bandwidth, narrow-beam, high-gain antennas providing excellent spatial discrimination, nulling, COMSEC/TRANSEC and sophisticated signal processing.

In March 1983, the US President, Ronald Reagan in his famous 'Star Wan' speech, officially announced a new defence doctrine based on space-age weaponry. He said that the United States would abandon the old strategy of detente achieved through the threat of massive nuclear retaliation and would pursue a new strategy based on the ability to prevent nuclear war. It would be a defensive strategy employing weapons designed to intercept and destroy incoming enemy missiles. These weapons would be 'directed energy' weapons, high energy lasers, in particular .

NASA is planning to set up a permanent space station and an Electronic Warfare Command and Control Centre by 1991. The Superpowers are already studying future

electronic combat in space and 1991 is not far away. The era of space fiction is over. I t has become a reality and a sort of electronic 'star wars' could be what the future holds in store--a space shuttle fleet fitted with high energy laser weapon systems patrolling the 'skies' ready to intercept and destroy enemy ICBMs still in their booster stage.

The Superpowers are exploring the possibility of employing two types. of countermeasures to nullify the effectiveness of 'space-umbrella'. Countermeasures against the platforms or space-stations (shuttles, Soyuz satellites, etc.) and countermeasures against directed energy weapons. Both require threat warning receivers for immediate detection of enemy radar, laser or IR source. ECM equipment similar to that used on Earth could be employed against the platforms onboard jammers and expendable jammers, chaff, IR flares, radar absorbing shields and so on. Against the laser beam, laser decoy mirrors and space mines of any other electro-optical countermeasures (EOCM) which may emerge from technology progress could be used. Of the $26 billion targeted for SDI (Strategic Defence Initiative) research for the next five years (1986-1991), USA has slated some S200 million for self-protection space-based systems studies.

It is likely that in future international crises, space will provide the perfect arena for a show of strength by the most technologically advanced superpowers in these new fields of military art and connected branches of applied science. A crisis could be resolved in favour of the superpower who could control the space more effectively through the use of EW-based spacecraft, satellites, ICBMs and radiation weapons.

From the increasing influence of EW in space, one can conclude that if one's way of life is worth defending in one's towns and villages, it is worth defending in space.

6.2 CURRENT EW DESIGN PHILOSOPHY

Design philosophy basically determines, first, which EW techniques are to be incorporated into or closely coupled to a hardware so as to make it effective against various threats, and secondly, how they are to be interfaced with the rest of the system.

Current EW systems are viewed from mission requirement point of view. How a particular threat {e.g. missile, tactical communications, anti-tank weapons) against air, naval or army platform is met effectively has remained. the crux of the EW problem since beginning. Many EW techniques have been evolved over the years to counter such threats. Design philosophy has primarily been the key basis for the development of all these EW tactics. From the discussion on the current EW scene, it is obvious that EW mission requirements are pursuing two distinct EW design philosophies-the stand-alone EW philosophy and the suppression of enemy air defence (SEAD) EW philosophy.

The stand-alone EW, also called 'self-protection EW' design philosophy meets one type of EW mission requirement. The primary aim of EW in this mission is to provide protection or survival of the system against a particular threat. The stand-alone EW design philosophy, in fact, is a carry-over from the electronic threat environment which existed from World War II through the mid 1960s. The threat in this time period

consisted of a few radar directed threats, well known in their principles of operation as well as frequency bands. EW was then a single countermeasure taken against a thinly deployed (both spectrally and geographically) array of hostile weapons. The basic EW encounter was a one-to-one situation, and each platform carried the EW equipment necessary for success in this environment. This philosophy still exists and that is why, most current platforms (aircraft, ships and troops) which operate against enemy actions have as a minimum requirement a radar warning receiver (RWR) with atleast quadrant threat direction-finding capability. The threat warning function is many times coupled with a defensive capability in the form of a self-protection jammer in combination with decoys, such as chaff or flares or which can divert weapons from the intended target. However it is difficult for anyone platform (particularly airborne platforms which have weight limitations) to carry enough EW to encounter today's sophisticated threats, even in a survival sense.

Suppression of enemy air defence (SEAD) design philosophy is another EW mission requirement. In this design approach EW techniques from many platforms are combined with other non-EW military assets. C^3CM plays an important role in SEAD mission. The primary aim of EW is to provide effective support to the C^3CM mission. The function of EW in this strategy, is to neutralise certain critical enemy radar and communication links, which helps to degrade the overall enemy air defence C^3 structure while preserving one's own C^3 capability, which is directing the suppression mission.

Thus, current EW design philosophy is playing a key role in the modern warfare a~ both fronts-self-protection of the system by itself, and degradation of enemy communication network in association with other systems.

6.2.1 CURRENT EW WORLD MARKET

The fear of war and potential of EW systems to handle such fears effectively has led to the establishment of many research and development organisations and production agencies in many countries of the world. There is a tremendous demand for EW systems. A number of EW companies with varied specialisations have come into existence to meet this growing demand. Today EW has become a highly competitive market. The various companies around the world earn millions of dollars through sale of EW equipment. Advanced countries like USA, USSR, France, UK, Italy, West Germany, Netherlands, Sweden and Israel are the leaders in the EW market. However, efforts in developing countries like India, China etc., are also going on in a limited scale to develop EW systems to meet the defence requirements of their own countries. Many under-developed and developing countries will have to depend on foreign sources of. supply till they establish their own design, development and production of state-of-the-art EW systems. A list of leading companies in the world and their I specialised EW products/services can be found in Appendix 2.