RESEARCHERID
THOMSON REUTERS
[IDSTM-18]
IC™ Value: 3.00
ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ELECTRONIC WARFARE

Sandeep Choudhary[1], Rajnish Mitter[2], Sonu Manderna3
[1]M.Tech Scholar, LIET Alwar (Rajasthan)
[2,3]Assistant Professor EE Deptt., LIET Alwar (Rajasthan)

ABSTRACT
Electronic warfare or EW is the use or control of electromagnetic energy either in defense, or for the purpose of a military attack, on an enemy. Electronic Attack, 'Electronic Protection' and 'Electronic warfare support' are the three principle components of EW. The purpose of EW is to deny the opponent the advantage of, and ensure friendly unimpeded access to the EM spectrum. Stealth technology is being used to reduce the Radar cross section of a target such as aircraft to avoid detection. Other techniques include new passive jamming systems namely multi-wave dipole reflectors (chaff) and the use of Radar absorbent materials for reducing combat equipment visibility. In EW, Jammers are being used to jam analog communication, digital communication as well as cell phone communication. In fact, in today's high-tech environment, the electronic warfare is something that cannot be ignored since in the final analysis electronic warfare will decide the outcome of future military conflicts.

Keywords: Electronic support, Electronic Attack, Signals Intelligence, electronic harassment, Stealth technology, anechoic chamber, frequency modulated noise, broadband transmitter, jamming- to-signal ratio, lock – on, Electro-optics sensor, seeker detector

I. INTRODUCTION
Electronic warfare (EW) refers to any action involving the use of the electromagnetic spectrum to control the spectrum, attack an enemy or impede enemy assaults via the spectrum. EW can be applied from air, land, sea and space by manned and unmanned systems and can target communication, radar or other services. Electronic warfare is the constant gathering of information on the enemy's capabilities and his plans for using these capabilities. It is the development of technology and planning for actions to do when and for how long to achieve maximum enemy confusion and to gain time.

II. EW – THREE MAJOR SUBDIVISIONS

2.1 EW
'EW is something that cannot be ignored, and any country which does, does so at its peril Admiral Gorshkov

- Electronic support
- Electronic attack
- Electronic protection

2.2 Electronic support
Electronic support attempts to ascertain information about an adversary by intercepting radiated energy. This radiated energy could be from radars, communication networks or telemetry transmitters. An overlapping discipline, signals intelligence (SIGINT) is the related process of analyzing and identifying the intercepted frequencies (as a mobile phone or radar). When signal is analyzed over an extended period of time, then intelligence is generated. If the information is put to immediate use, it is called combat information, not intelligence. Electronic support generates combat information, whereas SIGINT generates intelligence. Reaction to combat information is immediate, whereas intelligence is used to formulate long range picture.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

2.3 Electronic Attack

When radiated energy from a friendly source is used to deny an adversary access to his or her information, it is referred to as electronic attack. In electronic attack, receiver is the target of attack. Examples of electronic attack include radio Jamming and radar deception.

2.3.1 Jamming

Jamming is used to deny information in three fundamental ways –

- denying an adversary, the ability to talk to another element
- jamming a SIGINT system.
- deceiving an adversary's electronic support system.
- Jamming commercial TV and radio broadcast station may be included in electronic attack campaign.

2.3.2 Look- through

Look-through is incorporated in jammers to maximize the utility of the available power from them. It is to enable to monitor that jammer is still trying to communicate at the first frequency. A receiver collocated with the jammer cannot monitor at the frequency that is being jammed simultaneously. If it did, it may be damaged or desensitized enough so that it could not hear the target. Therefore, for a short period of a few tens of milliseconds the jammer is turned off so that the monitor receiver can measure the target energy at the frequency. In the absence of look – through, the jammer could waste a good deal of time jamming a target that was no longer trying to transmit at that frequency.

III. A TYPICAL EW SYSTEM CONFIGURATION

A block diagram of a typical EW system is shown in Figure 1. Some of these components may not exist in every system and some may contain others. The components shown in the figure are described below.

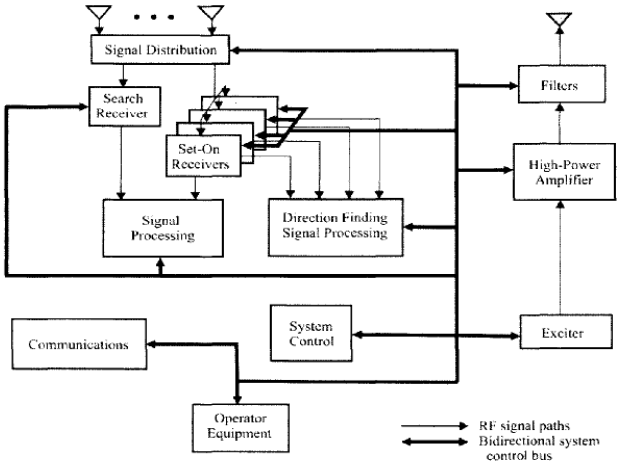

Fig 1: Typical EW System

3.1 Signal distortion

Signal distortion is accomplished normally at the output of the antennas and before the receivers.

3.2 Search receivers

The search receiver searches the frequency spectrum looking for signals of interest, and then measurements are made of the detected signal to characterize it.

3.3 Set on receivers

These are used for relatively long term analysis of signals. Search receiver acts as the RF portion. The outputs of these receivers are used to measure parameters of signals.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

3.4 Signal processing

This includes the determination of the modulation on a signal measuring the baud rate of a digital communication signal and so on.

3.5 Exciter

It is essentially an RF signal generator with the capability to modulate the signals generated. The most frequently used technique for modulating the communication signals is simply random noise frequency modulated on the carrier. This signal raises the noise level at the target receiver, thereby reducing signal to noise ratio and thus degrading the performance of target receiver.

IV. ELECTRONIC HARASSMENT

It is a term referring the use of electronic devices to harass/torture and/or physically harm a person. The electronic device or weapon could be one emitting an electric current, impulse, beam or wave with disabling effects on a human being.

V. STEALTH TECHNOLOGY

The purpose of stealth technology is to make an object or weapon system more difficult to detect. Stealth is used to reduce the risk of detection by many sensors including the following.

5.1 Radar

By reducing amount of energy reflected back by radar. Stealth technology is used to reduce the radar cross section (RCS) of a target such as aircraft to as low as $0.01m^2$. Such a small RCS is roughly equivalent to a medium sized bird. Of course, a true stealth design does not just refer to RCS but should encompass every aspect of stealth, including visual, audio, IR etc. The normal RCS of a military aircraft varies between $10m^2$ to 1000 m^2. For an aircraft to be called a stealth aircraft, the RCS must be below 0.5 m^2 .Reducing the RCS from 5 m^2 to 0.5 m^2 will give a range reduction to 35%.However, if RCS is reduced to 0.1 m^2, the detection range can be reduced by 90%.

5.2 Infrared

By reducing IR emission from heat sources such as the exhaust and engines.

5.3 Magnetic anomaly detector

By reducing the magnetic disturbance around a body by use of non-magnetic materials.

5.4 Practical stealth

- To reduce the RCS, the flat surface presented to a radar beam must be eliminated from basic design as any flat surface presented at 90 degrees to a radar beam is an excellent reflector.
- Cavities such as engine inlets and exhaust make a large contribution to RCS as they tend to be short and straight to improve engine efficiency, reduce weight and avoid complexity to reduce the RCS from engine intakes, curved, baffled or flush inlets are used in stealth aircraft, even though they have an adverse effect on weight, complexity and performance.

5.5 Use of Radar Absorbent Materials (RAM) to reduce RCS

Sharp edges, small radius curves, cavities, physical breaks in the skin and changes in the skin material can all add to the RCS. RAM are special materials that "soak up" the illuminating radar energy. The atomic structure of these materials is made up so that radar energy causes their molecules to vibrate, which absorb the energy and turns it into heat. RAM could be dielectric or conductive. RAM is made up of either carbon, an energy absorber, or magnetic iron compound (conductors) of the ferrite family, that absorb the radar energy as they conduct it. Most types of RAM have poor structural strength and are normally bonded to fiber glass or Kevlar to withstand the high loads and aerodynamic pressure of flight. Bonded RAM have been developed which can now be used as structural parts of the airframe, while others provide excellent absorption for relatively light weight and density. The perfect RAM would absorb all wavelengths and give total protection from all aspect angles. However, practically such materials absorb some wavelengths better than others and therefore only provide a degree of protection. Their absorption of radar energy is gradual and their degree of absorption (normally measured in decibels is proportional to their thickness).

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

5.6 Types of RAM

Two types of RAM are in use. The first of these is a plastic honeycomb used on the leading and trailing edges of the wing. The principal of this honeycomb is that of an anechoic chamber with its ranks of pyramidal absorbers lining the wall.

The second type of RAM consists in using paint materials which weaken the electromagnetic currents in the aircrafts skin and this helps to suppress reflections. This paint material contains microscopic particles of a ferrite compound.

VI. ELECTRONIC PROTECTION (EP)

Previously known as electronic counter measures (ECCM), involves actions taken to protect personnel, facilities and equipment from any effects of the friendly or enemy use of the electromagnetic spectrum that degrade, neutralize or destroy friendly combat capability. Jamming is not a part of EP, it is an 'Electronic Attack measure. The use of flare rejection on an IR missile to counter an adversary's use of flares is EP.

VII. INFRARED SEARCH AND TRACK (IRST)

It is an electronic warfare support system measure (ESM) equipment that detects radiation in the IR band. Such systems have been used in the naval environment since early 1980's like any ESM. IRST is a passive equipment that cannot measure range. Its primary role is to detect and track multiple targets at ranges in excess of missile launch and to detect approaching missiles. A typical IRST system may simultaneously detect and track up to 50 targets. Field of view is usually 25 degrees. The sensor detects the IR radiation from the target skin or exhaust, and then builds and maintains a track file on the target with data being updated on successive scans. When the system reaches a sufficiently high confidence level that it has acquired a valid target, the bearing and deviation are passed to the central weapon computer. Some IRST systems use a pulsed laser to measure target range.

VIII. JAMMING - ANALOG COMMUNICATIONS

The amount of jammer power required to prevent communication depends upon the type of modulation used. Some types are more easily jammed than others. Analog voice (AM or FM) requires significantly more jamming power than digital comm. It is generally necessary to jam with 100% duty cycle in Analog comm. The most effective technique is to modulate a high- power carrier signal with a FM noise signal.

IX. JAMMING DIGITAL COMMUNICATIONS

One of the design criteria for digital communication system is the bit error rate (BER) environment in which they are to operate. If BER is above this level, then communication degradation will occur. Initially this will be in the form of information transport slow down and, if the BER gets high enough complete denial of information exchange will occur. A digital signal need not be jammed continuously in order to generate a high BER. A BER of 0.5 can be achieved against a continuously broadcast digital signal by only jamming 33% of the time. In fact, denying information on digital communication signal is considerably easier than on analog signals.

X. GPS JAMMERS

GPS jammers cause GPS receivers to malfunction and to display the last coordinates calculated prior to jamming. This Russian invention exhibited during MAKS International aerospace show in Zhukovsky, Russia, caused quite a stir all over world and terrified military users. US forces cruise missiles were staying off course due to the use of GPS jammers by Iraq during us invasion of Iraq in 2003 .US forces destroyed these GPS jammers by carpet bombing and as a result, the problem was completely solved.

XI. NARROW BAND /PARTIAL BAND JAMMING

This is used to jam targets at individual frequencies. The jammer at the frequency used by the targeted communication net transmits a powerful noise signal. Such a technique is frequently used for standoff jammers to minimize frequently fratricide associated with barrage jammers. It is possible to utilize the same broadband transmitter and antenna to jam more than one target signal at a time. One exciter is required for each such signal since the exciter determines the frequency to be jammed. Further, it is also possible to time share a jammer to jam more than one signal simultaneously.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

XII. DATA OVERLOAD

It is also possible to load the transport channel with information to the point where it becomes completely saturated One would conceivably want to insert bogus data over the channel, thus disallowing the intended information to get through, or at least slow the transport of valid information. Most computers are vulnerable to such data overload, since valid information can be difficult to separate from bogus data. Unless and until computers can reason with data, as opposed to just processing it, they will be vulnerable.

XIII. BARRAGE JAMMING

In this technique, the jammer must be much closer to the target ES/SIGINT system than the friendly communications; otherwise the jammer will interfere with those friendly communications. One of the ways to implement such a jammer is to generate a relatively narrow (1 MHz, say) signal comprised of a carrier frequency modulated with noise. This signal is then stepped from 1MHZ portion of the spectrum to the next, usually in succession, dwelling at each step for some period of time, for example 1 msec. One can cover, say, the lower portion of the VHF frequency band of 30 to 90 MHz in 60 msec.

XIV. FOLLOWER JAMMER

For targets using frequency hopping (FH), either a barrage jammer or a narrow band jammer can be used. In the latter case the ES equipment must be able to follow the transmitter as it changes frequency. In FH, the frequency of transmitter as well as the tuned frequency of the receiver, is changed rapidly to avoid effect of jamming fixed on a frequency. Tactical jammers have been used to track such changes in frequency. Modulation is usually added to such jammers so that the whole communication channel is jammed, not just one of the frequencies The speed at which a frequency- hopped communication network hops is also a consideration for effective Electronic Attack (EA) against it. If hopping rate is high, a point is reached where transmitter and receiver hop to the next frequency just as the jamming signal arrives at the receiver at the old frequency rendering EA ineffective. The closer the jammer is to the receiver and/ or transmitter, the faster this rate must be to render the jamming ineffective.

XV. THIN JAMMERS

A thin jammer system consists of a set of small, relatively low power jammers spread around a region. They are typically deployed on ground with minimum antenna height and are battery operated so that their duration and radiation power is limited. In most cases, they are expendable and so they must be inexpensive and therefore unsophisticated. Thin jammers are often placed on ground or best in trees close to the ground or even they can be located on vehicles. The jammers in vehicles can implement higher radiated power than those are battery powered. Further, they can be more sophisticated, since generally, they are not expendable. Another significant advantage is that they can be deployed closer to the target networks than equivalent standoff jammer configurations.

XVI. SMART JAMMING

This technique uses pulsed signals. Some sort of electronic support receiver makes the measurements in the spectrum to determine the correct time to jam. Using such pulsed techniques has the advantage of using less energy to achieve the same jamming- to-signal ratio but only at the appropriate moment and increasing the peak jamming power for same energy use.

XVII. JAMMING SPREAD SPECTRUM SIGNALS

Spread spectrum signal spread their energy across a wider bandwidth. The transmitter bandwidth is the frequency over which the signal is spread or rapidly tuned. A hostile receiver does not have the synchronized dispreading capability whereas the desired receiver for a spread spectrum signal has dispreading capability. Therefore, the signal intercept jamming and emitter location are generally complicated. Since the noise power required for jamming is proportional to bandwidth, it will need to be high enough to hide the signal.

XVIII. JAMMING CELL PHONES

18.1 TDMA and CDMA

Digital cell phones systems are using either Time division multiple access (TDMA) or Code division multiple access (CDMA) to allow multiple conversations on each RF channel. This means that the jammer can jam the whole RF channel using normal communication jamming techniques. However, if specific conversations are to

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

be jammed, it will be necessary to use modulation equipment like that used by the cell phone system to jam in the appropriate time slot or with the appropriate code.

18.2 Jamming the uplink

The jamming link is from jammer to tower. To jam a single RF channel of a GSM system operating at 1800 MHZ with cell phones operating at 1watt of effective radiated power (ERP), it has been seen that a jamming to signal ratio of 0 dB will be sufficient. A jammer of 100 W serves the purpose.

18.3 Jamming the down link

In this case the desired signal link is from tower to the cell phone and the jamming link is from the jammer to the cell phone. The desired signal ERP is now 50 W. A high jammer power of 550W has to be used to achieve the required 0 dB jamming to signal ratio.

XIX. SEARCH FOR LOW PROBABILITY OF INTERCEPT (LPI) SIGNALS IN EW

LPI signals are harder to detect The simplest LPI feature is emission control i.e. reducing the transmitting power to the minimum level that will allow the threat signal (radar or communication) to provide adequate signal- to-noise ratio in the related receiver. The lower transmission power reduces the range at which any particular hostile receiver can detect the transmitted signal. Using a narrow beam antenna with suppressed side lobes can serve the same purpose since the antenna will emit less off-axis power and thus will be more difficult for a hostile receiver to detect. Further, the modulation used in LPI signals spread the signal's energy in frequency, so that the frequency spectrum of the transmitted signal is order of magnitude wider than required to carry the signal's information (the information bandwidth). Spreading the signal energy reduces the signal strength per information bandwidth. Noise in a receiver is proportional to its bandwidth. Therefore, the signal- to- noise ratio (SNR) in any receiver attempting to receive and process the signal in its full (spread) bandwidth will be greatly reduced by the signal spreading as shown in figure 2 below.

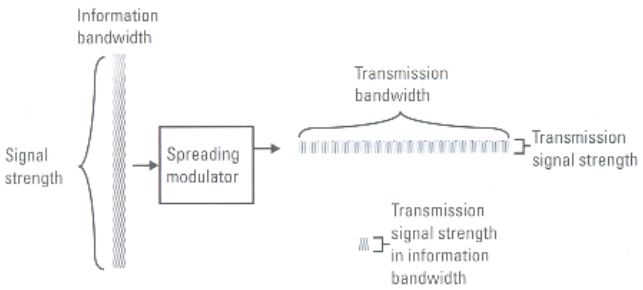

Fig 2: Signal Spreading

XX. WARNING RECEIVER SYSTEMS

Such receivers came into widespread use on United States tactical and transport aircraft during Vietnamese war. The warning receiver is programmed to alert a pilot when the aircraft is being illuminated by a specific radar signal above predetermined power thresholds anticipated by Eliot systems. When the pilot has been alerted, the aircraft can be maneuvered to evade the threat or initiate counteraction with onboard electronic warfare capability.

XXI. PASSIVE ECM – USE OF CHAFF

Chaffs are metallic strips cut to length resonant at defense radar frequency so that they return spurious radar echoes to enemy radar. Chaff can confuse the enemy as well as can screen or mask aircraft or higher – speed ships so that enemy is unable to determine their presence. Chaff can also help an aircraft break track once it is alerted by its warning receiver that it is being tracked by radar.

XXII. USE OF ELECTRO –OPTICS (EO) IN EW

22.1 Electro – Optics

It is the interaction between optics and electronics leading to the transformation of electrical energy into light, or vice-versa using suitable devices. EO equipment convert either the infrared (IR, visible or ultraviolet (UV)

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

portion of the electromagnetic spectrum into a form that may either be displayed to a user or interpreted automatically by a computer. The 1991 Gulf war brought EO sensors into limelight as TV screens across the world showed the Coalition Forces carrying out attacks in the day as well as night. The sub systems considered in EO are

22.2 Infrared (IR)
These systems operate in the non-visible portion of EO spectrum

22.3 Lasers
Lasers operate at a single wavelength which may be selected from a broad section of the EO spectrum.

22.4 Imaging systems
These are used to convert EM radiation from any part of the EO spectrum and display it at visible wavelength. An imaging IR system will outperform TV system has additional capability to operate in any light condition

22.5 EO sensors
EO sensors detect either reflected or emitted radiation just as in optical sighting wherein the light reflected off an object or body is detected by the human eye.

XXIII. IR GUIDED MISSILE SYSTEMS

In the nose of every heat seeking missile is a tracking system with a Field of view (FOV) of about 1.5^0 This tracking system is mounted on gimbals that allow the seeker to be steered through an angle of $40\text{-}50^0$. The IR seeker has two distinct roles, tracking the target and then be able to discern the target direction relative to the center of FOV. Error signals will need to be generated, which will result in the tracker being steered towards the target. The second role of the seeker is to provide guidance signals for the missile control surfaces.

XXIV. IR JAMMERS

IR jammers reduce the lethality of homing missiles. Active IR jammers add spurious, modulated IR energy to the targets IR signal in the missile seeker to lose the lock-on. Other approaches could involve saturating the seeker detector with very strong IR signal or damage the detector or IR dome with a power laser.

XXV. CONCLUSION

Electronic Warfare has emerged as an extremely important discipline for any nation in defending itself or countering any enemy assault by a hostile nation. The EW encompasses 'Electronic Support', 'Electronics Protection' and 'Electronic Attack' measures. Jamming is being effectively used to deceive an enemy's electronics support system and to disrupt hostile communication including cellular communication. Stealth Technology makes use of radar absorbent materials to suppress the reflections from aircraft in order to avoid detection by ground based radars. Use of Electro-Optics has become indispensable for effective EW. No wonder, that in present high-tech scenario, it is a generally accepted military principle, that victory in any future war will go to the side that can best control and manage the electromagnetic spectrum and thus the thrust on Electronics Warfare.

XXVI. REFERENCES

[1] Introduction to Communication Electronic Warfare Systems by Richard A. Poisel. (ARTECH HOUSE, BOSTON, LONDON) Page 13-17, Page 38-47, Page 559-560.
[2] Electronic Counter Counter measures– Wikipedia-(Date last modified- 7 Jul (2010).
[3] Tactical Battlefield Communication Electronic Warfare by David L Adamy (ARTECH HOUSE, BOSTON, LONDON) Page 251- 263, Page 271- 272.
[4] "Electronic Warfare Sensors" – Technical News letter Oct.(2008).
[5] India Strategic –Military Aviation 2008-10 Published Jun (2009).
[6] Electronic Countermeasures – Wikipedia-(Date last modified- 9 Oct (2010).
[7] Electronic Warfare Support Measures – Wikipedia (Page last modified- 30 Jul (2010).
[8] Target Acquisition in Communication Electronic Warfare Systems by Richard A. Poisel. (ARTECH HOUSE, BOSTON, LONDON) Page 2- 10 .
[9] US GAO-01-28-EW Study Report on use of Suppression Aircraft - Nov (2000).
[10] Anti-radiation missiles – Wikipedia – (Date last modified 28 Sep (2010).

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[11]Mobile phone Jammer – Wikipedia –(Date last modified- 11 Oct (2010)
[12]Radar Jamming and Deception – Wikipedia –(Date last modified -1 May (2010)