INFORMATION WARFARE THROUGH ELECTRONIC WARFARE

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd)

Abstract

Electromagnetic spectrum (EMS) pervades all operational domains, and it binds them together through networked connectivity. Freedom to operate in an electromagnetic spectrum is crucial to achieve information superiority by the armed forces. With advancements in computerisation, communication and sensor technology, the spread of electromagnetic spectrum employment has increased tremendously in all regimes. Battle of EMS superiority is fought through Electromagnetic Warfare (EW), which directly influences information superiority. IW has a much wider canvas of psychological warfare, command and control warfare and EW. This article exclusively covers the employment of EW as a tool of Information Warfare, as freedom of operation in EMS is crucial for all operational domains.

INTRODUCTION

Information is an important ingredient to plan and take decisions in all fields including civil enterprises, governance and military operations. The process involves collecting and collating relevant data, storing, interpreting, analysing taking decision and disseminating them. Technological advances in sensors, communications, computerisation and digitisation have transformed the information process tremendously. For military operations, the air and space based sensors generate massive multi-spectral data covering a very large swath of geographical area. This requires tremendous computational power, digitisation of data and Artificial Intelligence (AI) embedded algorithms to glean useful

information in a compressed timeframe. Manual analysis of electronic or photographic data would take months to collate. Accurate information derived from multiple sensors would ensure enriched information which is considered essential to plan and execute successful operations. Timely information is crucial to shorten the Observe, Orient, Decide and Act (OODA) loop and remain ahead of the adversary action plan, for successful execution of operations. Freedom to have access to the required information and denying the same to the adversary, has led to a concept of IW, which has been conceived for many decades. Information Warfare, as perceived by many practitioners, encompasses a very large canvas that includes cyber war, Command and Control (C2) war, psychological war and EW. The boundaries amongst these subsets are loosely defined. The IW, as defined in the Indian Air Force (IAF) Doctrine 2022, is, “Actions taken to preserve the integrity of one’s own information system, while at the same time exploiting, corrupting or destroying an adversary’s information system, and in the process, achieving an information advantage for the application of Information Operations (IO) - the offensive and the defensive”.[1] This definition excludes the scope of psychological warfare, which has been quite pervasive in recent conflicts, however, the IAF may have considered it to be beyond their operational domain. This is evident while dwelling on 'No War No Peace (NWNP)' scenario, the IAF Doctrine mentions cyber, electronic and psychological warfare, as inclusive to the IW, with a caveat that all instruments including the government and private media are to contribute towards achievement of information dominance.[2] The Doctrine of the United States Air Force (UASF) defines the IW more comprehensively as, "The military capabilities employed in and through the Information Environment (IE) to deliberately affect adversary human and system behaviour and pre serve friendly freedom of action during cooperation, competition, and conflict."[3] This definition amply covers employment of forces to influence military forces, political leadership and public. The USAF IW concept consists of six principal capabilities - cyberspace operations; electromagnetic spectrum operations (EMSO); information operations, public affairs (PA), intelligence; and weather (WX)[4]. What is amply clear is that electromagnetic spectrum is the glue that integrates all other domains of air, sea, land, cyber and space operations. As all the

military elements are networked to share information for better situational awareness (SA) and shorten OODA loop, it is crucial to maintain EMS superiority that will lead to information superiority. While the term EMSO is prevalent in the Western world as the scope includes electromagnetic spectrum management, the term EW is prevalent in the Indian military and it is defined as the 'Military action employed in the electromagnetic spectrum domain and directed energy to degrade, exploit, reduce or prevent hostile use of EMS and ensure own freedom of operation in the same'. The EW activity is divided into the elements of Electronic Support Measures (ESM), Electronic Protection (EP) and Electronic Attack (EA), this article will discuss the scope of IW execution exclusively through EW.

EMS, IW, AND EW RELATIONSHIP

All the ground based and airborne early warning, surveillance, tracking and synthetic aperture radars use some segment of EMS to provide information on hostile ground based and airborne targets. Passive sensors in the EMS regime of acoustic, electro-optical (EO), Infra-red (IR) and Ultraviolet (UV), microwave and radio frequency regimes provide digital photography, electronic order of battle (EOB), terrain layout, weather, communication network layout, communication content and military activity. Space based assets employ Radio Frequency (RF) spectrum copiously for recording information through sensors and downloading them to the ground stations for analysis and for sharing with airborne elements for SA. The satellite communication uplinks, downlinks and sensors can be degraded by EW means, which would result in significant degradation of the adversary information operations. For coordinating and controlling multi-domain operations, EM spectrum is the main 'electronic superhighway' which binds other domains together and ensures timely dissemination of information and facilitates command and control of the fighting force. Freedom of operation in employing EMS for information is ensured by the Electronic Protection (EP) element of EW, which provides resilience, and redundancy for IO. The IO of the adversary is exploited by monitoring the EM activity to map and monitor communication network and other potential targets. This activity is achieved by Electronic Support Measures (ESM) element of EW. The degradation, disruption, deception manipulation and destruction

of the hostile information sources is achieved through the Electronic Attack (EA). The IW and EW are, therefore, intricately linked to maintain information superiority over the adversary. The goal of EW is to achieve EMS superiority, contributing to gaining and maintaining information and decision advantages to achieve the military operational objectives. It is, therefore, important to examine the EMS operational environment and EW applications towards information superiority.

PRESENT EMS OPERATIONAL ENVIRONMENT

Technological developments have led to the EM spectrum being employed at much diverse and wider frequency bands as compared to the past. It is a physical entity characterised by frequency, waveform, power, and time. These EM characteristics are affected by atmospheric and other environmental attenuation considerations. The 'ideal spectrum windows' at different frequency ranges are, therefore, restricted. The EM operational environment has, therefore, become highly congested, especially so as the EM spectrum is being exceedingly employed for civil applications of mobile phone connectivity and internet of things (IoT). The EM spectrum transcends all geographical boundaries and, therefore, the environment is highly contested by the adversaries. The EM spectrum usage is also governed by the international and national policies, prevailing status of technology and each frequency band has unique physical properties, which constraints the employment of electromagnetic spectrum. Cross domain employment and network centric operations have increased the density of EM transmissions which results in electromagnetic interference (EMI) if the frequency distribution is not deconflicted at the planning stage. As the competition between the electronic protection and electronic attack remains dynamic, increased complexity and sophistication have been introduced in the waveform characteristics, employing technologically advanced spread spectrum frequency hopping (FH) techniques and encrypted transmissions, which are difficult to detect and counter. Spread spectrum technique modulates a signal across many carrier frequencies to make transmissions difficult to detect and jam.

EW APPLICATIONS FOR SUPPORTING IW

- **Information Mapping Services.** Information services of the adversaries are detected 'mapped' and geolocated by regularly

monitoring the electromagnetic transmissions of the adversary. Ground based and Airborne Electronic Intelligence (Elint) platforms like dedicated Elint aircraft, Unmanned Aerial Vehicles (UAV), and satellite based Elint sensors are employed to detect, identify and geolocate the adversary non-communication EOB and other active RF sensors. Technical parameters are recorded to create a data base of the 'RF signature' of the emitters, Advanced Elint systems have capability to 'fingerprint' each individual radar of the same type, which also provides deployment history of the radars. In peace, regular monitoring of the EOB provides deployment pattern for strategic planning and 'change detection' is analysed for conclusions. During the transition to war, such missions are launched more frequently and closer to the area of interest, for better assessment of hostile deployment. This facilitates better operational planning and offensive IW strategy. RF Communication Intelligence (Comint) assets are similarly employed to map the communications network and Command and Control (C2) Centres. The present fighters, transport aircraft and helicopters also have integrated Electronic Support Measure (ESM) receivers called Radar Warning Receivers (RWR), capable of recording and geolocating hostile radars, which supplements the data obtained from other Elint resources. The whole process of EOB generation involves compiling the data base of each sensor in terms of Signature, modes of operation, geolocation and operational characteristics. Similarly, communication networks are mapped for technical characteristics, modulations and geolocation. The communication activity and movement provide indication of the force movement or imminence of operation. Weather satellites and aerosonde balloons map the weather information of the target area, which is useful for planning operations with suitable weapons. The information obtained through Elint/Comint provides strategic and tactical awareness that supports present operations and future planning. The ESM receivers onboard fixed wing aircraft provide situational awareness and warn against immediate threat for tactical actions. The technical characteristics of the transmitters help in preparing threat identification data base and effective countermeasures.

- **EW for Offensive IW.** Offensive IW involves actions and activities taken to affect enemy decision-makers by attacking their information and information systems. In today's networked operational environment of all domains, any degradation or disruption in freedom to operate in EMS, adversely affect operational outcome. Electronic attack on C2 Nodes, communication networks, Integrated Air Defence System (IADS) are conducted to degrade situational awareness of the adversary and paralyse the C2 network. For overall EA planning, the entire AD network, including the C2 Nodes, networking topology, sensors overlap, crucial control systems of the weapons deployed, and weapons lethality zones are analysed to ascertain the optimum strategy. This would provide maximum pay off, in ensuring higher mission success rate of the follow-on attack forces. This EA could involve hard kill of C2 Centres with stand-off precision guided munitions, Anti-Radiation Missiles, or soft kill with offensive jamming of radars and communication networks. For each individual AD weapon system consisting of early warning radars, acquisition radars, fire control radars and communication network- the entire chain of control is analysed for planning the attack. Ideally, each link of AD network could be targeted, however, the EA assets would always be at a premium and therefore, the crucial link in the AD chain may be targeted to achieve maximum pay off. Time synchronisation with the attack force is conducted for maximum effect. For example, to degrade an Air Defence weapon system, the early warning, acquisition, and tracking radar vulnerabilities are analysed, additional inputs on, lethal ranges of the weapons, alternate routing profile of the attack force would be analysed to plan the attack strategy that would increase mission success rate by minimising attrition of the force. If attacking acquisition radar is the critical link to trigger missile launches, it would be targeted with higher priority whereas the early warning radar may be avoided by following appropriate flight profile or detection ignored. EA tactics involve degradation, denial, deception disruption and destruction of the hostile AD network. Consideration of selection of the operational tactic and technique would be governed by the most optimum operational plan that would ensure maximum success rate of the attacking forces. Various EA techniques are described in subsequent paragraphs:

- **Degrade/Deny.** Having analysed the adversary EOB and communication networks, EA is planned to degrade the adversary systems by electronically jamming the appropriate sensors. With effective jamming, the information on the position of the attack force, the strength and type of attack force would be degraded, however, there would still be some limited information available on imminence and direction of attack. With active jamming, the adversary would be forced to employ an alternate mode of operation which would degrade the weapon performance. For air operations, standoff jammers are employed to jam surveillance radars from further ranges, escort jammers are employed that accompany the attack force to degrade the acquisition radars. Tracking radars are targeted through airborne self-protection systems. Stand-in jamming is conducted by UAVs or other EW missiles fired ahead of the main package. Simultaneously, communication network is targeted to prevent or delay targeting and control inputs, while satellite communication network may also be targeted depending on the criticality of the mission. The plan is required to be well coordinated and synchronised to degrade the adversary information system for specific time and in a specific area. The main advantage of this soft kill EA is that the jammers could be re-used, re-tasked and reconfigured to meet the operational objectives. The main drawback being that the jamming effect is limited in time and space and the hostile systems would be fully functional when the jamming ceases. The ground and naval elements also employ similar tactics and techniques to degrade hostile military machinery. Recently, the Global Positioning System (GPS) receivers are being degraded by jamming the GPS receivers of UAVs, standoff weapons and time synchronisation of communication networks. Normal GPS receivers are easy to jam as their receiver sensitivity is very high to receive the GPS signals from satellites. This has also resulted in collateral GPS jamming of civil flights which could be hazardous for safe civil flight operations.

- **Deception.** Deception techniques are employed to deceive the adversary decision makers into believing the false targets or information created in the operational scenario, which would divert,

delay or dilute the enemy action. The information system of the hostile force is, therefore deceived into false assessment of the raid. For aerial attacks, the deception is achieved by launching airborne decoys that simulate profile of the attack force and generate similar radar cross section (RCS) ahead of the strike force. This technique was amply employed during the Beka Valley operation by the Israeli Defence Force (IDF) that deployed remotely piloted vehicles (RPV) and during the Gulf Wars the U.S. Forces deployed tactical air Launched Decoys (TALD). Another deception ploy that has been employee since 'Normandy Landing' campaign of World War II, is to conduct diversionary attack to lure away the enemy from the main axis of main attack from a different direction. This deception technique was employed by the IAF during Balakot Air strike in Pakistan, in February 2019. Active deception jamming deceives the tracking radars by generating false target position, which is achieved by capturing the tracking centroid of the radar and moving it away from the actual target, by generating stronger signal. The ground and maritime forces employ deception communication plans and multiple thrust axis to deceive the enemy into believing the false attack thrust. It is important to understand that the EW lessons learnt during past operations are as relevant today, as they were decades back. GPS spoofing has been copiously employed against UAVs and other platforms to falsify the systems of their actual locations. The Iranian Forces had successfully spoofed the GPS receiver of the RQ-170 Sentinel UAV on December 05, 2011, and brought it down in Iranian Territory.[5]

- **Destruction.** The EW action also includes physical destruction of the hostile sensors, weapon systems and C2 Centres either by directed energy or by other physical means. Hunter killer missions were developed during the Vietnam War by which the 'hunter' aircraft equipped with ESM sensor would lead the 'Killer' fighters equipped with bombs/rockets to the Surface to Air Missile (SAM) sites for their physical destruction. As the attrition to these missions increased with induction of infra-red shoulder fired missiles, Anti-Radiation Missiles were developed to destroy the SAM sites from standoff

ranges. The present Anti-Radiation Missiles (ARM) have much larger attack ranges and have sophisticated dual band terminal guidance receivers that ensure successful attack despite the victim radar going 'silent'. The radar operators were so intimidated by the ARMs during the first Gulf War that they used to abandon the site on detecting the ARM launch. The present air to ground precision guided missiles are also employed for DEAD (Destruction of Enemy Air Defence) missions as their terminal guidance systems may use target scene matching algorithms and similar systems to preclude tracking of radar electromagnetic radiations. Dedicated fighter aircraft like F-18G 'Growler' of the US Navy and, J-16 of the Chinese Air Force are equipped with high power jammers and ARMs for this type of mission. Major advantage of the hard kill option is that the sensor is put out of action for much longer period, and it impacts the hostile AD operations. The ARMs are quite expensive, and their employment would be selective.

- **EW for Defensive IW.** Freedom to use EMS for IO is crucial, especially in the networked multiple operational domains environment. Electronic Protective measures ensure robust, resilient EMS operation that should withstand and continue functioning despite hostile electronic attack. The process starts with preventing the adversary from exploiting our electromagnetic transmissions, corrupting, creating confusion, and ambiguity during the process of information analysis. The second aspect known as anti-ECCM ensures resilient and robust network and sensors that continue to operate under active jamming conditions and ensure graceful degradation. Most of the armed forces employ multi-spectral and multi-layered sensors which cannot be simultaneously jammed. Passive sensors remain electronically undetected and have jamming immunity. Networked sensors ensure composite picture despite jamming few of the radars as inputs from alternate sensors are available.

- **Anti-ESM Measures.** To prevent the adversary from detecting and recording our EMS transmissions and collating ELINT/COMINT, the armed forces promulgate Electronic Emission Policies (EEP) to avoid electronic transmission of sensitive systems closer to the border and

only designated training frequencies are specified to avoid exposing the entire operating frequency band of the radars. Similar emission policies are also promulgated for communication systems. Dummy transmitters or phased out airborne and ground based radars could be deployed closer to the border and operated at regular intervals to corrupt and confuse the electronic data being compiled by the adversary. Low Probability of Intercept (LPI) radars is employed to reduce the chances of detection by the adversary systems. Training of sensitive nature is carried out deeper inside our own territory to prevent information on operational tactics and operating scenarios. EW exercises are also conducted well in depth to prevent snooping by adversaries. The communication transmissions are encrypted and employ wider spread spectrum techniques to prevent monitoring of communication contents. The trials of new strategic weapons being developed are carried out deep inside our own territory and the area over the sea is sanitised of any 'snoopers' before clearing the trials.

- **Anti-ECM Measures.** Radars and other electronic sensors incorporate anti-ECM features known as Electronic Counter-Countermeasures (ECCM) during the manufacturing stage itself, to ensure continued operation during active jamming by hostile forces. These measures include frequency agility, wider band frequency operations, low side lobes, employment of IR and optical sensors as alternate sensor to circumvent jamming effect on RF sensors. Employment of passive aircraft detection sensors along with radars prevents total information denial of the airborne threats. The IAF has recently published a requirement to acquire Passive Surveillance System for this purpose. Active Electronically Scanned Array (AESA) transmitter technology is inherently jamming resistant due to electronic scan speeds, selectable radiation patterns and low side lobes. Most of the present radars employ AESA transmitters. V/UHF band radars are being digitised and upgraded to counter airborne stealth design advantage. Dummy transmitters that mimic actual radar transmissions are deployed around important radars sites to divert ARM attacks by generating stronger EMS. Corner reflectors that deflect the radar transmissions are deployed close to the high

power radars to confuse the ARM homing head about the exact source of transmission centroid. Most of the AD weapon stations have GPS spoofers/jammers to degrade precision weapons. Own GPS receivers can be incorporated with advanced receiver antennae that filter out the jamming due to adaptive antenna pattern generation. Communication networks are configured to ensure alternate lines of communication including optical fibre cables and satellite based communications to ensure enough redundancy. Netcentric centres generally have many servers located at different geographical locations to ensure uninterrupted takeover of operations in case one centre gets physically destroyed.

EW OPERATIONAL STATUS OF INDIAN ARMED FORCES

Armed forces all over the world including the Indian Armed Forces have shifted from the platform-centric operations to network-centric operations.[6] The IAF has operationalised Integrated Air Command and Control System, which has all C2 Centres, military and civil radars, SAMs and AWACS. The system provides common air situation picture and is networked with airborne elements. The IA has also deployed similar system called 'Akashteer', which provides filtered Air Situation picture and controls AD weapons. The IN has deployed maritime domain awareness that has networked all naval sea borne elements with C2 Centres. For mapping hostile ME spectrum, the IAF has airborne assets including fixed wing aircraft, UAVs ground based systems and Aerostats for ELINT and COMINT Operations. The Indian Army also employs UAVs and ground based systems for Sigint operations. The Indian Navy (IN) has a fleet of P-8I Poseidon Maritime surveillance aircraft that undertakes maritime surveillance and Intelligence Surveillance and Reconnaissance (ISR) missions. The IN has Sigint systems onboard most of the ships. However, the SIGINT Data analysis has not been fully centralised or automated. The IAF has airborne self-protection jammers, RWRs onboard all fighters and appropriate EW equipment onboard transport and helicopter fleets. The IA and IN airborne assets are also appropriately equipped with EW protection systems. All radars and sensors inducted in the armed forces have embedded ECCM circuits to defend against hostile offensive EW action.

TECHNOLOGICAL DEVELOPMENTS FOR EW

Artificial Intelligence (AI) is being embedded in EW systems for faster Sigint data analysis and dissemination. Netcentric operational capability has reduced the OODA cycle that can also update the jamming techniques of onboard EW systems while airborne. AESA technology has improved the jamming capability of Airborne Self Protection Jammers (ASPJ) and has improved the simultaneous multiple targets jamming capability. Digitisation and advances in computer technology have brought in much more advanced jammers and ARMs. There have been tremendous advances in the communications field that have made the communication systems more resilient and jam resistant. However, technological advances have also been employed to field in much more complex and advanced sensors with better resilience to jamming. This dynamic competition will continue to prevail in future.

PRESENT GAPS AND CHALLENGES IN EW

- Common network for sharing information near real-time, integrated and common network for all the three services is considered essential. This has not been achieved mainly due to the apprehension of secrecy and security.
- Airborne encrypted software defined radios are yet to be standardised for the three services due to which intelligence, airspace control, targeting and situational awareness cannot be fully exploited.
- SIGINT collation resources exist with all three services and other agencies. The data collated from fixed wing aircraft, UAVs and ground bases sensors are analysed in isolation which fails to enrich the quality of data. Data obtained from modern RWRs is quite accurate and substantial. However, it is not integrated with other SIGINT data to improve the data base.
- AI and ML applications are considered essential to analyse the SIGINT Data and to refine active jamming techniques against emerging new threats. The present EW systems lack the AI and ML tools.

- All the airborne self-protection jammers onboard the fighters have been imported from abroad and some of them came embedded in the fighters procured from abroad. DRDO has been attempting to develop the ASPJs for quite some time, without success, due to which the LCA-Mk-I fighter has been inducted without any ASPJ. The indigenous RWRs lack the directional accuracy required of a modern RWR. The Indian Defence industry has not yet achieved the capability to produce the contemporary EW systems. BEL has been manufacturing ground based Sigint systems which are difficult to maintain and operate.

- As the armed forces adapt to netcentric operations, complex communication waveforms with spread spectrum and FH techniques are generated to prevent communication monitoring and to ensure resilience against communication jamming. The armed forces require much more advanced COMINT and COMJAM systems to ensure effective interference against hostile networks. Much more R&D is required in this area.

RECOMMENDATIONS

- HQ IDS may prioritise standardisation of connectivity protocols for all the armed forces and integrate all the services C2 network to ensure faster dissemination of actionable intelligence, situational awareness and airspace management. This would also ensure seamless integration of Theatre Commands in future.

- Standard and interoperable airborne SDRs are essential amongst all the services to ensure connectivity across all airborne elements and C2 centers. This would drastically reduce OODA loop timeframes.

- Indian defence industry and DRDO must collaborate with reputed foreign EW manufacturers and coproduce EW systems, to accelerate technology absorption and work towards acquiring niche technology for EW systems.

- Developers of AMCA, LCA-Mk-II and other future fighters must embed EW systems and integrate them with onboard avionics at the

development stage itself, to ensure the most efficient approach to EW capability. These systems must be upgradable with AI and ML embedded in them.

- Collation and analysis of SIGINT data should be centralised from maximum sources to enrich data inputs. AI and ML applications must be employed for faster data analysis.
- Till now emphasis has been non-communication EW systems. With operationalisation of netcentric concept, the operators and defence industry must work towards development and employment more advanced COMINT and COMJAM systems.
- More research on Smart cognitive EW systems, which adapt to changing hostile EMS environment and counter new threats must be conducted to remain abreast of the current trends in EW research.
- HQ IDS may consider reorganising its structure to integrate cyber, EW and operational planning and ensure well synchronised operational plans for maximum effect.

CONCLUSION

EMS is the common e-way that pervades all other operational domains and binds them together. IW is highly dependent on EMS for operations. Therefore, freedom to operate in the EM spectrum is crucial to ensure operational superiority. EW ensures this freedom of operation in the EMS domain and prevents the hostile forces the same freedom. All elements of EW viz, EMS mapping, offensive and defensive EW contribute towards IW superiority. The armed forces have inducted EW systems, however, the defence industry and DRDO have not kept abreast of development in this field. There is deficiency of modern ASPJs and other EW which can only be plugged in with much more R&D in this field. For faster absorption of EW technology, collaboration with reputed foreign EW defence industry and coproduction will accelerate the process. At the national level all elements of the IW must be enmeshed and synchronised with military operations to achieve information superiority. Standardisation of the SIGINT data and communication network amongst the armed forces

would ensure much better SIGINT data for tactical decisions. Initiative by the present government to stimulate Indian defence industry would pay high dividends in EW operational capability of the Armed Forces in due course of time.

★★★

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd) was an Air Officer Commanding-in-Chief of an operational Command. He regularly writes article on defence strategy in various magazines and has been a keynote speaker in many International Seminars on Electronic Warfare and Air Defence.

NOTES

1 *'Doctrine of Indian AirForce, IAP 2000-22 (Indian Air Force Air Headquarters Vayu Bhawan Rafi Marg New Delhi 110106) p- 65*

2 *Ibid page 40*

3 *USAF DOCTRINE PUBLICATION 3-13,"Information in Air Force Operations, USAF February 01, 2023. P-4*

4 *CSAF signed USAF IW Strategy, July 2022.*

5 *Iranians claiming to down US Drone, 04 Dec 2011, BBC News https://www.bbc.com/news/world-middle-east-48700965accessed on Oct 06 2024*

6 *Air Power and Emerging Technologies. KW Publishers Pvt Ltd New Delhi), 2022, Chapter 4, p 67.*