EXPLOITATION OF EMS IN RECENT CONFLICTS: LESSONS FOR INDIA

Gp Capt GD Sharma, VSM (Retd)*

Abstract

Electro Magnetic Spectrum (EMS) in recent years has evolved into a formidable combat support enabler which boosts the capabilities of the supported domain. An appraisal of previous operations, provide an important and cost-effective way to avoid documented mistakes committed earlier in EMS domain. Their study at the same time also provides suggestions for protection and use of own EMS domain with advantage. Beginning more than a century ago with the Russo-Japanese war of 1905, EMS has emerged as a viable option with experiences gained in subsequent wars. A focussed study of the two world wars, Vietnam war, Falkland war of 1982, Arab Israeli wars of 1973 and 1982, Russian operations in Chechnya, Georgia and Ukraine and finally war between Azerbaijan and Armenia in Nagorno-Karabakh region in the year 2020 demonstrate that EMS is a viable tool to gain advantage both in non kinetic and kinetic phases of wars. It is an essential instrument to dent the adversary's ability to function in the electronic domain while maintaining own operations by hardening of our own electronic equipment and pursuing methodology for operations despite jamming by the adversary including use of the alternate means. Today, we positively face a serious challenge in this dimension from our adversaries; hence, it needs greater attention from our military strategists.

EMS in recent years has evolved into a formidable combat support asset, and forms a key part of conventional Armed Forces. At the tactical level, electromagnetic spectrum operations translate into creating advantages in battles and engagements which at the operational level, focus on employing military forces in a theatre of war to obtain an advantage over the enemy for attaining strategic goals. At the national level however, the aim is to prevent electromagnetic spectrum attacks against critical information infrastructures in all situations.[1]

Development of credible Electronic Warfare (EW) capability can give an asymmetric advantage against the adversary with a lot more technical dependence. Besides enabling the offensive heft, the EMS-enabled capabilities may eventually reduce risk by limiting exposure of combatants as well as present a commander with an array of non-kinetic options that can achieve effects at lower cost.[2]

Electronic Magnetic spectrum is an enabler of different domains. Thus, instituting a war in EMS domain boosts the capabilities of the supported domain. The R&D in advanced materials could further enhance the capabilities of EMS equipment due to their lower power demand, smaller size and weight, higher sensitivity, and covering wider frequency range for sensing and transmitting which will eventually revolutionize commander's operational capabilities.[3]

The militarization of the electro-magnetic spectrum began with the arrival of radio in the 20th century. Since its first use, it has become one of the defining characteristics of modern combat and continues to advance at a staggering pace. This foretells that the future battle spaces will include directed energy weapons, UAV fleets and even more complex forms of Electronic Counter Measures (ECM) and Electronic Counter Counter Measures (ECCM). An appraisal of previous operations, provide an important and cost-effective way to avoid documented mistakes committed earlier while at the same time guides in use of the offensive aspect of the

1 https ://www.researchgate.net/publication/339943524_Non-kinetic_Warfare
2 ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
3 ibid

EMS to own advantage. A scan of the past wars therefore, reveals some useful lessons to the military strategists and practitioners alike.

EMS Evolves as a War Fighting Tool

The earliest use of EW was attempted during the Russo-Japanese War in 1905. In this war, the Russian naval commanders while being trailed by the Japanese ships, in an effort to shake them off attempted to jam radio transmissions of Japanese ships but, failed as Japanese could still transmit information about their movements to their high command for higher directions, without getting jammed.[4]

In World War-I, the belligerents experimented with electronic deception of the simplest forms, such as false transmissions, electronic espionage, dummy traffic and other similar ruses for misleading the enemy.[5]

Specialized EW equipment began to be developed during World War II. It is emphatically illustrated in the battle of Britain wherein, the use of radar for detection of air threats turned the tide in favour of the British since it invariably succeeded in intercepting the attacking German Bombers with their Spitfires and Hurricanes. The Germans answered it by introducing a “Blind Radio Guidance Technique” for their bombers to carry night raids on British military installations. The British however, countered these by “Bromide”, a deception technique to mislead the bombers from their targets.[6]

EW technology became progressively more specialized and sophisticated after World War II. In the initial stages of Vietnam war of 1965, United States due to lack of ECM capability suffered aircraft losses to Soviet SA-2 ‘Guideline’ radar-guided Surface-to-Air Missiles (SAMs) and 57mm. radar-controlled Anti-Aircraft Artillery (AAA). From 1971, it employed the first fully integrated tactical airborne jamming system “Northrop Grumman developed EA-68 Prowler aircraft”, to jam radars

4 https://www.army-technology.com/features/evolution-electronic-warfare-timeline
5 ibid
6 https://www.drdo.gov.in/sites/default/files/publcations-document/Electronic%20Warfare.pdf

and reduce its losses. This was the first demonstrated use of ECM[7].

EMS Transforms to a Potent War-fighting Domain

Both Yom Kippur War (Arab-Israeli war of 1973) and Bekka valley conflict of 1982 stand out in an imaginative use of the EMS to gain advantage in the war. This operation also established the necessity of possessing a complete range of EW equipment,

The surprise, complacency, inadequate preparedness, poor Electronic Intelligence (ELINT) and lack of understanding of the potential of the EMS were the main reasons for setbacks in both wars first to Israelis in 1973 and then to the Arabs in 1982.

In the initial stages of 1973 War, the Arabs with surprise and formidable SAM defences caused heavy losses to the Israelis. However, Israeli forces soon overcame their inertness and managed to adapt Electronic Counter Measures (ECMs) to suppress the radar-controlled SAMs and radar-controlled Air Aircraft Artillery (AAA) to reduce their losses and finally succeeded to turn the tide in their favour.[8]

In Bekka Valley conflict of 1982, it was the turn of the Arabs to get surprised. After the previous successes of the SAMs against the Israelis in the 1973 war, the Syrians never expected that Israelis will take risk in the presence of extensive SAM systems deployment. But they committed two major mistakes. First, the mobile SAM-6 missile batteries were immobilized and deployed in dug-in position for over a year in the Bekka valley. This allowed the Israelis to pinpoint the precise location of each target. The second Syrian mistake was the lack of emission control by its SAM operators as they often turned their radars on more frequently even while practicing engagements. This aided in identification of the exact Syrian radar frequencies needed by the Israelis to jam them. After this, Israel used mastif and scouts Remotely Piloted Vehicles (RPVs)in highly successful jamming operations and also in targeting the Syrian

7 Ibid
8 https://www.army-technology.com/features/evolution-electronic-warfare-timeline

radars with anti-radiation missiles. Both RPVs were also capable of relaying their information to ground and airborne command posts for immediate analysis in real time.

The Israelis also employed Boeing 707 and E-2C Hawkeye aircraft for suppression of Enemy Air Defence (SEAD), The Boeing 707 was used primarily in Electronic Support Measure (ESM) role and as an Electronic Counter Measure (ECM) platform whereas, the E-2C Hawkeye served as an airborne command post. With real-time display of the tactical situation, the commanders were able to monitor and control attacks and also coordinate the jamming and deception to effectively disrupt the Syrian defences.[9]

The Yom Kippur war and Bekka Valley conflict clearly established the need for outstanding Command, Control, Communications, and Intelligence (C3I) network, control of the electronic spectrum, and superior technology. These wars also showcased synergy of air and land action in destroying the Syrian SAMs, as land-based jammers, artillery, rockets, and missiles not only contributed, but participated in the destruction of the Syrian SAMs.

The wars underlined a valuable lesson that control of the electronic magnetic spectrum is vital for own access of C4ISR as well as for denial of its use to the adversary. Along with this, a need for an integrated plan was also established which included jamming, RPVs, decoys, chaff, and anti-radiation missiles to defeat SAM sites and enemy aircraft without incurring unacceptable losses of the friendly aircraft. Finally, the wars brought out that comprehensive training in EW and competent leadership play a huge role in determining the outcome of an engagement.[10] These lessons have been reaffirmed once again in recent conflicts.

The Falkland war of 1982 between Argentina and United Kingdom once again established the importance of EW capability. In particular, the absence of an early warning resource with UK maritime task force

9 https://apps.dtic.mil/sti/pdfs/ADA192545.pdf
10 ibid

proved costly for the British since it could neither detect a low flying Argentinian aircraft which fired a sea skimming Exocet missile that sank its destroyer HMS Sheffield nor initiate any action to deceive the missile. To meet the need for an AEW aircraft, the Royal Navy later successfully deployed several Sea King helicopters equipped with Search Water Early Warning Radar. Thus, the need for capable detection radar, an accurate fire control system, an effective close-in missile and an electronic countermeasure suite was clearly established in this war.

Despite these drawbacks, the British with professional, highly trained manpower supported with an excellent command and control organization, achieved stupendous success in the Falklands War. This is partly also attributed to lack of credible EW systems with Argentina to disrupt the British operations.

The war also underscored the need for an optical designation and guidance mode for engagement by their close in SAM systems in coastal areas and in high sea conditions, since terrain masking and land/ sea clutter degraded the radar controlled operating modes.[11]

Iran-Iraq War 1980-1988. The release of the archived files by the U.S Defence Intelligence Agency has given a good account of use of EMS during the Iran Iraq War which lasted for almost eight years. In this war, as Iranian Air Force was practically grounded due to the lack of spares, Iraqi Air Force had air superiority. Hence, there were few occasions for use of ECM. Iraq mainly employed ground based electronic warfare assets to collect the tactical information of Iranian forces which positively influenced the outcome since it helped Iraq to identify and track Iranian units' movements. There were some drawbacks in Iraq's EMS operations. First, it was incapable of intercepting frequencies in the upper ultra-high (UHF) and super high frequency (SHF) ranges in which Iranian tropo-scatter and microwave systems operated. Second, the dissemination of the information suffered due to the rigid command and control structure as battlefield commanders at the lower echelons did not always receive needed information of Iranian forces. Third, Iraq also

11 https://www.ukessays.com/essays/history/electronic-warfare-in-falkland-war-history-essay.php

avoided use of jammers since it disrupted its own information gathering. Hence, Electromagnetic Interference (EMI) and Electro Magnetic Compatibility (EMC) of own equipment are of vital importance.[12,13]

United States pioneered in exploitation of EMS in Operation Desert Storm (Gulf War of 1991). In this war, apart from attacks on radars, use of ARMs and use of drone decoys to degrade the defences, ECCMs to counter these were used. The Global Positioning System (GPS) which was declared operational after another four years was also used along with the Joint Surveillance and Target Attack Radar System (JSTARS) and Electronic Intelligence (ELINT) aircraft to provide improved targeting data and programming information for attack.[14] For the first time, F-117A stealth aircraft was employed against critical strategic Iraqi command and control installations.[15] In Desert Storm, just like the Israelis in the Bekka valley, U.S. used BMQ 74 drone decoys for defence suppression.[16] The Gulf war also exposed the vulnerability of the GPS to jamming and spoofing.[17] The armed forces therefore, must rely only on own satellite navigational platforms. In any case, GPS service accessed from a universal source, is firstly never reliable secondly, it may not be available, when needed. Moreover, as this service is always vulnerable to interference, back up is desirable.

Russian Use of EW in Operations

Russia has consistently invested in EW modernization and fielded a variety of new EW systems to augment the capabilities of all service branches. Some of them have been tested on the battlefield in Eastern Ukraine and Syria. Russians perceive that EMS could provide an inexpensive, asymmetric response to the military technological development of the West. While its key objective is to suppress enemy

12 https://www.archives.gov/files/declassification/iscap/pdf/2014-033-doc01.pdf
13 https://csis-website-prod.s3.amazonaws.com/s3fs- public/legacy_files/files/media/csis/pubs/941015lessonsgulfiv-chap06.pdf
14 ibid
15 https://www.pbs.org/wgbh/pages/frontline/gulf/weapons/stealth.html
16 https://www.gps.gov/policy/legislation/loran-c/
17 https://www.cnet.com/news/gps-at-risk-those-signals-are-more-vulnerable-than-you-realize/

command and control systems its equally important goal is to protect the country's own military personnel, equipment, and infrastructure.

Russia's development and reliance on EMS, integrated with its combat operations can be seen in the recent history of its military conflicts.

In the first Chechnya War (1994–96), the Russian Armed Forces used EW to disrupt communications of the Chechen fighters But, it faced a crunch due to the lack of the trained personnel in its specialist units. In Chechnya II Russia's use of EW was better organised and it was able to achieve greater success in disrupting enemy communications. EW forces also made improved use of jamming and direction-finding equipment, for monitoring of enemy communications.[18]

In 2008, during its five days war at Georgia, the terrain masking caused by mountainous terrain impacted Russian EW effort, as it limited the coverage of Russian fixed-wing aircraft and helicopter-mounted jammers. Russia however, following the Russo–Georgian War has launched an ambitious defence modernisation programme which is likely to continue till 2025. The programme also comprises procurement of a range of EW equipment which is mainly aimed at suppressing radio communications and navigation systems of the adversary and for protection of own command and control systems from high-precision weapons. The modernisation is a closely guarded secret and seems to have drawn from the learning from the US and NATO engagements during past two decades. It has heavily invested in EW as an asymmetrical response to NATO's technological edge across the spectrum of conflict and as an integral part of its anti-access/area denial strategy.[19]

Russia's military operations in Syria, September 2015

In Syria, Moscow's EMS effort was limited. It sought to strengthen its air defence and EW support at key locations in Syria to enhance its A2/ AD strategy only after its SU 24 M was shot down by Turkish Air Force in Nov 2015. [20]

18 ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
19 ibid
20 https://www.militarytimes.com/flashpoints/2019/10/30/us-forces-could-learn-from-intense-electron-

Russian Invasion of Ukraine/ Crimea in 2014

In stark contrast to Russia's operations in Chechnya, Georgia and Syria, the seizure of Crimea and the war in the Donbas relied heavily on extensive use of EW. Every Russian armour or infantry brigade has an EW company, a unit usually more than three times the size of a platoon. These units are capable of jamming, deceiving and geo-locating enemy signals at different bandwidths, and disrupting or hijacking drones.[21] Russia used highly mobile tactical EW groups throughout the conflict which constantly changed locations to avoid detection. Russia's forces employed a variety of EW systems to jam and intercept communications signals and jam and spoof GPS receivers.[22] Since its GPS was also being shared by Ukraine, Jamming and spoofing of own GLONASS by Russia was also reported. As a result of GPS interference, Ukraine lost over 100 RPVs in the years 2015 to 2017. Thus, these operations once again highlighted the vulnerability of both GPS and the drones and established a requirement of an alternate system for navigation and targeting. It used its own unmanned aircraft with electro-optical cameras and electronic direction finders to specifically locate and then jam counter-battery radars ahead of mortar and other artillery strikes. In Ukraine, Russia also hacked the mobile phones and passed fake messages to lower the morale of the Ukraine forces which highlighted its use of synergetic relationship between cyber and the EW.[23]

The Western studies following the Russian conflicts have concluded that Russia's Armed Forces' have developed a formidable capability in electronic warfare (EW) and in the event of a Russian assault, it could pose a serious challenge to NATO's planned defence of the Baltic states, and even to its entire Eastern Flank. This capability is an integral part of Russia's A2/ AD approach and is intended to target NATO's C4ISR. Russia's advances will enable its EW forces to jam,

ic-war-battle-in-ukraine/

21 https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101

22 https://www.militarytimes.com/flashpoints/2019/10/30/us-forces-could-learn-from-intense-electronic-war-battle-in-ukraine/

23 https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare

disrupt and interfere with NATO communications, radar and other sensor systems, Unmanned Aerial Vehicles (UAVs) and other assets, thereby negating the Western technological edge.[24] The Russian advances also draw attention to the fact that the military strength alone must not be judged based merely on simplified comparison of the weapons systems and technological advances, but it should also take into account the EW capability of the opponent. It is also assessed that just like China, Russia also follows a system where Cyber and EW maintain symbiotic relationship, which was seen in use in its 2014 war with Ukraine. To facilitate its EMS exploitation, Russia has carried out structural changes in the military organisation and included dedicated EW battalions as part of the Tank and Infantry brigades. These battalions provide EW support to the brigades far ahead of their area of operation. In fact, Russian Ground Forces do not move or conduct operations without EW support. Russia has also reorganised its disparate EW units into EW brigades. Each of this brigade consists of four EW battalions and one EW company. Such changes in Russian EW organisation brings out the stark difference of the Russian forces from the Western ones.[25]

24 ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
25 Ibid

Russian Federation EW brigades

Independent studies show that Russia has made spectacular advances in developing the jamming equipment. In the field of jamming, the mobile EW systems like “Krasuha-2” and “Krasuha-4” are capable of jamming vital radar frequencies and other radio-emitting sources at far ranges. Krasukha-2 for example, can jam Airborne Warning and Control System (AWACS), airborne radars and guided missiles up to ranges of 250 kilometres, whereas; Krasuha-4 can suppress these as well as spy satellites in lower earth orbit. The jamming system could even disable adversary’s radar EW and communications systems.[26] These systems have been operationally deployed opposite Ukraine and in the Middle East conflict, where Russia deployed its Krasukha systems at Syria in an effort to form a sort of electronic shield over Russian and allied forces.[27]

Russian army also has counter drone specialised units in the ground forces to defeat enemy drones. In the past, Iran is known to have used one such jammer (Avtobaza) to force down a U.S. Air Force RQ-170 stealth drone on the Iran-Afghanistan border in December 2011.[28]

Russia also has satellite jamming EW systems (Tirada-2) which can jam uplinks and downlinks of the satellite in its counterspace operations which obviously has advantages over the anti- satellite hard kill option. Russia deployed the systems to jam satellite links as well as the field radio relay links during the Ukraine war.[29] All these developments confirm the belief that Russian current EW capability may give it an asymmetric advantage against the perceived superior Western military technology.

Military lessons from Nagorno-Karabakh war: 2020

The conflict between Armenia and Azerbaijan over the disputed Nagorno-Karabakh region included the heavy use of missiles, drones, and rocket

26 https://web.archive.org/web/20150714165635/http://kret.com/en/product/12/
27 https://www.vice.com/en/article/ywbwaj/russian-army-specialized-drone-hunters-krasukha-jammer
28 ibid
29 https://www.thespacereview.com/article/4056/1

artillery. In this war, Azerbaijan was the clear military victor. The 44-day war featured a diverse array of legacy and advanced air and missile strike and defence platforms and UAVs. The use of these provides insight into how future wars will employ the growing spectrum of missiles, drones, and artillery.[30] Azerbaijan also used loitering munition attacks to destroy heavy ground units, including T-72 tanks and highly rated S-300 air defences. The military strategists have taken note of serious drawbacks in Armenian's EM domain. These are briefly explained below: -

(a) The sensors of Armenia's most 'modern' air-defence systems, the S-300PT and PS series and the 9K37M Buk-M1, are designed to detect and track fast-moving fighters. Their Moving Target Indicators (MTIs) disregarded small, slow-moving drones. Besides, systems were incapable of multi-sensor tracking and fusion of plots from different radars. Thus, Armenians were unable to detect the threats and react against these.

(b) Armenia lacked jammers to interrupt guidance links of drones which moved freely with impunity.

(c) Azeris used the Israeli Harrop loitering munition, which has two guidance modes: it can either home in on radio emissions by itself with its anti-radar homing system, or the operator can select static or moving targets detected by the aircraft's electro-optical sensor.31 Jamming of guidance link and discipline in transmission could have saved the Armenian assets.

(d) Azerbaijan also reportedly modified its Soviet-era An-2 Colt biplanes with remote-control systems, to activate Armenian air defences. This enabled Azerbaijani forces to find, fix, track, and kill targets with precise strikes far beyond the front lines.

(e) While drones played a large role in this conflict, their capabilities ought not be exaggerated. These platforms are very

30 https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense

31 https://www.iai.co.il/p/harop

vulnerable to air defences that are designed to counter them which Armenia did not have in adequate numbers.

(f) The bulk of Armenia's air defences consisted of obsolete Soviet-era systems, like the 2K11 Krug, 9K33 Osa, 2K12 Kub, and 9K35 Strela-10. The Turkish TB2s flew too high for these systems to intercept even if they were able to detect these relatively small aircraft.

(g) Both Armenia and Azerbaijan lacked Short-Range Air Defence (SHORAD) arsenals in size and quality. Azerbaijan was able to exploit this gap with its large fleet of sophisticated drones.[32]

Armenian Air defence was not prepared up to the level of Azerbaijan's air threat both in terms of sensors and in weapons systems. Inability to detect the drone threats, the lack of ECM and anti-drone countermeasures, deficient SHORAD arsenals required to tackle the drone threats and EW training of the personnel significantly affected the Armenian war. Russian EW support came in the end but, it was too late and did not change the result of the war. Nagorno- Karabakh conflict thus, has valuable lesson in preparation of air defences.

Conclusion

In the modern times, an adversary aims to win the war without fighting in the battlefield. Along with cyber and Information domains, EMS provides a feasible tool to subdue the adversary both in kinetic and non-kinetic war situations. The radars and sensors, communications, navigation, weapon guidance and targeting systems, space systems, C4ISR systems etc. in military are all electronic magnetic spectrum dependent. Hence, these are primary targets for EW forces. EW suppresses or protects depending on whether it is used for attack or defence. The results of several wars have affirmed repeatedly that availability and proficient use EMS can have significant effect both in war and no-war situations and

32 https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense

has emerged as a critical domain similar to any traditional domains of war like land, air, sea and space.

Some important lessons which need cognisance by the military strategists/ practitioners are as follows: -

(a) The disruptive role played by EW in network-centric operations is likely to grow, with cyber-warfare playing a secondary supporting role. Our Northern neighbour, China, too has made rapid strides in EW and has even displayed its EW vehicles in a military parade in Beijing which shows the importance it places in EW capabilities.[33] Alternate means of operations must form part of our plans.

(b) EW could interfere with friendly systems. Hence, EMI and EMC of own equipment is vital.

(c) EW capability could become an integral part of India's A2/ AD in response to any adversary's challenge to our sovereign areas.

(d) **EW Training.** Proficiency to operate in EW environment is of vital importance. Thus, incorporate EW training in professional military education at all levels.

(e) Over Reliance on Electronic Communication. Over reliance on electronic communications and GPS navigation can be disastrous to an operation. There is a need to find alternate means. Map reading skill is of vital importance.

(f) **Camouflage.** The need to camouflage applies to the electromagnetic spectrum as it does in the physical realm. There is a need to look for ways to minimize the EMS signature. Terrain could be effectively used in some cases to mask the signal from the enemy.

(g) **Deception.** It is difficult to completely mask electrometric signals with current technology. Flooding the area with false signals could make it impossible to distinguish the real ones from the fake.

33 https://www.nbcnews.com/think/opinion/russia-winning-electronic-warfare-fight-against-ukraine-united-states-ncna1091101

(h) Rigid command and control structure is an anathema in EMS supported battle. Innovation and flexible approaches are keys to success.

(j) To exploit EW, forces must possess intelligence and EW equipment to cover the entire range of EMS of the adversary.

(k) Symbiotic relationship between Cyber and EW will accrue advantage to the side which is able to exploit it in a war.

(l) Military strength based on a mere comparison of the weapons systems and technological advances is not the true measure. It should also include EW as an essential element.

(m) Integration of the EW battalions with the mobile fighting formations (armoured and infantry brigades) will provide combat support for own protection and in an offensive.

(n) Uplink and Downlinks of satellites are vulnerable to cyber takeover and jamming actions. Create backup civil satellites.

(p) Develop asymmetrical edge in EMS to nullify adversary's technical edge and use it as an integral to our A2/ AD strategy.

(q) Maintain EMS discipline to deny its Information to the adversary.

***Gp Capt GD Sharma, VSM (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi