IMPORTANCE OF THE ELECTRO-MAGNETIC DOMAIN

The Israeli surprise air attack on 07 June 1981 on the under construction Osiraqnuclear reactor in Iraq 17 km South East of Baghdad is the fine example of offensive use of Electro Magnetic Spectrum (EMS) to gain undetected entry in Baghdad air space for destruction of its nuclear reactor (code named Operation OPERA.).Israel showed its EMS prowess once again when in a coordinated air strike supported extensively by Electronic counter measures successfully destroyed Syrian nuclear reactor (Al- Kibar facility) 300 miles inside Syria on 06 Sep 2007.(code named Operation Outside the Box).[1]

More recently, in 2012 South Korea reported GPS failure. This was blamed on the North Korean Jamming of the GPS signals. Starting on March 31st it continued for week and affected signal reception of more than 1,000 aircraft and 700 ships, originating from five locations along the border. The Aircraft traffic however, was not affected because the GPS system is normally used as a backup, not a primary navigation tool.[2]

Above instances depict the quality of mission success with domination of the electromagnetic environment by the attacker. The majority of military systems contain cyberspace- and EMS-dependent components. This calls for close coordination in application of cyber and ESM inwarfighting.Similarly,in the space domain, the command and control andinformation distributionare ESM dependent. ESM overlaps several air, land and maritime operations as well. Hence, as we move towards a highly digitised society, our systems across all domains in civil and militaryare becoming spectrum dependent.

EMS Application

The Electronic magnetic Warfare (EW) measures can be applied from air, sea, land, and/or space by manned and unmanned systems.It has application in wide range of equipment that transmit and receive radiated data and thus one finds that there is a significant proliferation of

[1]https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/
[2]https://www.reuters.com/article/us-shipping-southkorea-navigation/south-korea-revives-gps-backup-project-after-blaming-north-for-jamming-idUSKCN0XT01T

Electromagnetic (EM) spectrum-dependent systems in all military domains—air, land, sea, space, and cyberspace.Nearly every modern weapons system—airplanes, unmanned vehicles, satellites, tanks, ships use the EM spectrum. Similarly, all communications, sensors, ISR systems, most weapons, situationawareness in all domains, command and control systems etc. use EM spectrum. Even the emerging concepts, such as net-centric warfare and multidomain warfare too are spectrum dependent.

While EM spectrum has facilitated a shortened Observe, Orient, Decide and Act (OODA) loop by providing real-time air situation picture and an efficient command and control of the battle, it has also in the inverse increased the vulnerability since the adversary can attempt to disrupt it. Therefore, today in a battle, gaining supremacy in the electromagnetic domain is vital to have edge in the war.In pursuit of this, the military must work for an unimpeded access to own electronic equipment while denying their use to the adversary. The supremacy is achieved by considering own vulnerabilities particularly in the legacy systems and working out the alternatives while exploiting opportunities in Electronic Warfare (EW).

Similarly,all critical infrastructure across various domainscontrolled by public or private entitiesin civil,academia, industry, Services with EM signature can be disrupted or denied.A humanmade Electro Magnetic Pulse(EMP) can disable the electric grid and all electronic systems unless these have robust protection against it. A high-altitude detonation of an appropriately designed nuclear weapon can create this effect, even though it would also be possible to create similar effect by a Cyber attack. One can only imagine the catastrophic effect it will create and lower the nations resolve to fight. The mobile network once again is highly suspectable to EM interferences and would impact both the civil and military assets. With high dependence this will have impairing effect on the operations unless we revert to point to point impregnable fibre optics communications. The problem will increase manifold when we move to 5G networks particularly, when these are out sourced. Similar consideration should be given to GPS which is also jam prone and navigational services are likely to get affected both in civil and military. With the advent of nano technology, smaller gadgets are available which can easily be carried by same platform used on the land, air and sea along with other offensive and defensive weapon

systems or by independent platform with exhaustive EW capabilities to support the offensive operations.

Adoptive Threats and Cognitive Electronic Warfare (EW)

The EW threat in present time has become more challenging as the radars/ communications can easily change signal structure and quickly adopt frequencies. But the jammers too arenow dynamic and can adopt with the type of equipment these encounters and even choose the time to interfere.The advances in artificial intelligence (AI) and machine learning technologywill allow the use of massive amounts of datawhich will make it easy with automatic choice of EW against the electronic equipment be it radar, weapons system, command and control center or space satellite etc.While on the attack side the focus is to collect the signal, carry self analysis, learn and self apply with out human intervention. The requirement on the defence side too isthe same. The defence is developing the new AESA radars and radars with wide spread of the frequency of operation which creates arequirement for a wide instantaneous bandwidth capability for theactive jammer thus making it difficult to jam.

Use of Unmanned Systems

Besides the ISR and attack roles,the unmanned systems are also being used by the attacker against the defences.These can be used for active and passive jamming. For example, the Raytheon has developed a Miniature Air Launched Decoy Jammer (MALD-J) released by attacking aerial platform, is a relatively simple air-launched unmanned aerial vehicle (UAV) designed to jam and spoof enemy radar. The jammer will entice the ground radars on wrong targets clearing the arena for the actual manned aircraft who will carry out their mission.Several such unmanned jammers could be released by the manned air craft.[3]Even if the defence uses the alternate means of operation, still the ultimate aim of the attacker to spread the OODA loopis achieved. Thus, EMS will not only fight its own independent battle but, it will enable the other domains too tosucceed by impairing the adversary's capabilities in these domains. The advent of new

[3]https://www.militaryaerospace.com/communications/article/16709112/todays-battle-for-the-electromagnetic-spectrum

materials, small power systems, and faster, smallerand more capable processors are making it possible.

Chinese Strategy

The central themeof the modern warfareis to win the spectrum warfare. If you do not win this, you cannot win the real war as well.In this ongoing standoff on the Eastern Ladakh we may face Chinese machinations in this area and we have to be prepared to deal with this.China has established a Special Strategic Force (SSF) specially for this purpose in its reorganisation, which combines, cyber, electromagnetic and space capabilities to conduct independent operation across these domains.[4]Rand corporations'findings too note the significance of the Strategic Support Force which is responsible for integrating the cyber data with the electronic and space warfare information.[5]

PLA does not consider electronic warfare and cyber warfare mutually exclusive. Together these dominate information operations during wartime. Although China has not established a formal information warfare doctrine, it sees complementariness between Cyber and electromagnetic spectrum.
From a Chinese standpoint, warfare across the electromagnetic spectrum requires initiative and offensive action. In the offensive action, PLA will effectively deny the enemy the use of its electronic equipment. Offensive operations across the electronic medium would employ electronic jamming, electronic deception, directed energy weapons and electromagnetic pulse radiation. The defence on the contrary would require hardened facilities, dispersion, countermeasures, and physical retaliation.

The dominance of EM spectrum would surely be aChinese strategy against any future skirmish with India. An article in the India today, quotesa Chinese General Wang Hongguang , a former deputy commander of the China's Nanjing Military Region who in his four prong strategy to deal with India in the current standoff in the eastern Ladakh has air supremacy and

[4]https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%20Section%202-%20China%27s%20Military%20Reorganization%20and%20Modernization%2C%20Implications%20for%20the%20United%20States_0.pdf
[5]https://www.rand.org/pubs/ research reports /PRA394-1.html

simultaneous capture of electromagnetic control of the spectrum to destroy India's command net work as the first step . This is followed by the other steps viztargeting of the India's key infrastructures, axillarypositions, armoured clusters, logistic warehouses, oil depots etc., occupation of key strategic heights, dividing and trapping the Indian deployments by cutting off the Depsang plains and Siachen glacier and finally occupying the National highway-1 from Srinagar to Lehto cut off the connection between Ladakh and the rest of the country.[6]

Own position

Not that we are unaware of the Chinese strategy on exploitation EM spectrum and steps must be in place to deal with it as well as wrest spectrum dominance from the Chinese but, unlike the Chinese,we still consider EMSas a service specific domain. We have a cyber agency but, it appears disconnected from our Electro Magnetic realm. There is a need for unifiedstrategy against the adversarybecause of complementariness between Cyber and EM Warfare.Synergising cyber and EM Warfare can force multiply the effects of their operations. These apparently are two sides of the same coin; one focuses on the data corruption while the other to disable the electronic equipment. For example, to incapacitate the adversary's command and control, the attacker could use cyber and spoof the computer network and at the same time jam the carrier frequencies with offensive use of Electromagnetic warfare.Cyber/spectrum conundrum does not apply to military alone but it has application in civil infrastructure too for example satellite services are spread across all sectors similarly,provision of most servicesare data dependentwhere automation and computers are extensively used.

Independent service approach to EMS goes to prove that organisationally we still do not consider EM Spectrum as an independent domain. Like cyber, EMS apart from active war may be applied much before war in the grey zone (activities below the threshold of the war)[7] The best example of

[6]https://theprint.in/opinion/indian-armys-approach-to-electronic-cyber-warfare-is-nowhere-as-evolved-as-chinas-pla/266292/

[7]https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0004_ELECTROMAGNETIC_DEFENSE_TASK_FORCE_2_2019.PDF

this one finds the incidents in 2018 where in several US diplomats suffered traumatic brain injuries at Cuba and China. The analysis and the investigation revealed that victims' brains had been raised byan external electromagnetic source.

Though the ultimateuse of EMSis likely to be servicespecific andmore precisely mission specific in any operation in which time and manner of application would finally rest as per the judgement of the field commander but, joint doctrine must dictate its use which would be in the nature of advisory in character with general dos and don'ts.[8]

There is a need is to enhance the awareness at all level of their hierarchy of the adversarial use of ESM in civil operationstoo,particularly of those who are connected with critical civil infrastructure such as power,banking and finance,transportation (railways, airways), telecommunication etc. At the same time,we need to be aware of the measures necessary to increase the robustness/hardening of the legacy equipment to avoid the debilitating effect of the EM warfare during their use.In armed forces, the coordination /integration between cyber warfare and EM warfare must percolate down to the theatres and even lower fighting formations for successful operations.

Conclusion

EM domain is generally less understood than other visible domains.Even if unseen, the nefarious operationby the adversary in this domain below the threshold of war will most certainly be used because of reliance on contactless wars in the modern times. When used, it can impact the operation of civil infrastructure on ground or in space and military warfighting ability. Its affinity with cyber warfare must be understood and planned accordingly.

[8] https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347