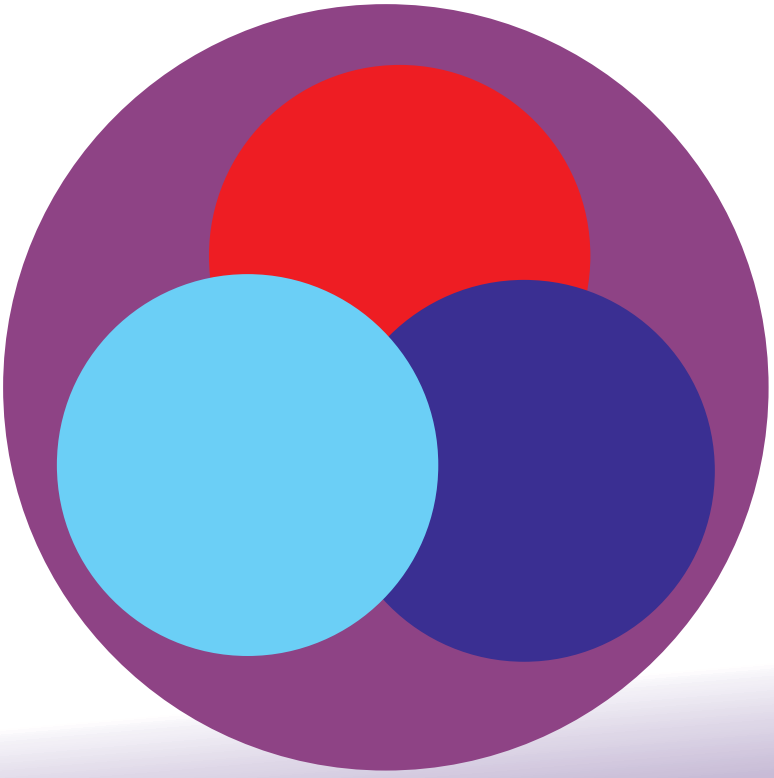
February 2022

SYNERGY

Journal of the Centre for Joint Warfare Studies



ELECTROMAGNETIC SPECTRUM KEY TO MILITARY DOMINANCE

SYNERGY

JOURNAL OF THE
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS
(Established : 2007)
Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road,
New Delhi - 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

Synergy is a bi-annual Journal that is published in Feb & Aug every year. It is supplied to the members of CENJOWS. Articles, abridged version of Research Papers and Dissertations may be sent to the Secretary CENJOWS as per the guidelines contained in the Journal. Advertisement enquiries concerning space and charges may also be sent to the Secretary CENJOWS.

The Centre for Joint Warfare Studies (CENJOWS) is an independent, professional research institute established in 2007, in pursuit of strengthening the concept of 'jointness' within the defence force, as well as with other agencies that jointly contribute towards a nation's war fighting capability. SYNERGY is the CENJOWS Journal that strives to expand and deepen the understanding of issues concerning defence, national security and civil-military interface which are so very essential for joint war fighting.

Price : **Rs. 200/- INR or US 10$**

ELECTROMAGNETIC SPECTRUM
KEY TO MILITARY DOMINANCE

INDEX

ELECTROMAGNETIC SPECTRUM: KEY TO MILITARY DOMINANCE

FOREWORD

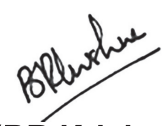
The Electromagnetic Spectrum (EMS) provides means for transfer of energy and information. Exploitation of various bands of the EMS for civil as well as military use has become so critical that disruption of its assured use can adversely impact economies and militaries. The demand of EMS to meet commercial and life-style requirements to accelerate National growth and well-being is increasing phenomenally. Militarily, EMS is the connective tissue which drives cross-domain synergy and integration of operations in land, sea, air, space and cyberspace. Consequently, the dependence of militaries on EMS to gain situational awareness, information dominance and decision superiority, as also to employ kinetic and non-kinetic vectors, has increased manifold. This dependence on EMS, thus, is vulnerability too, which is through counter operations. The EMS has, therefore, become a contested environment.

Militaries, the world over, are evolving doctrines, organisations and strategies, leveraging niche technologies like AI/ML, to exploit new capabilities in the EMS, in conjunction with cyber and psychological operations, deception, operations in the space domain and kinetic operations to gain information superiority. Prowess in EMS has been demonstrated in the recent conflicts in Ukraine and Syria. China advocates “Information Confrontation” and “Systems Warfare”, and has integrated hitherto dis-aggregated capabilities in Space, Cyber, EMS and Psychological domains under a “Strategic Support Force” created in 2015, and also advocates EMP attacks on critical information infrastructure. Challenged by near peer adversaries, US promulgated a reviewed “Electromagnetic Spectrum Superiority Strategy” to retain its traditional superiority in the EMS, its Army has integrated EMS and Cyberspace operations in the CEMA framework, and is deploying new EW across various echelons.

A comprehensive understanding and exploitation of EMS has been inhibited by a narrow platform-centric approach, and a narrow focus on the EW subset of EMS. There is a need to garner EMS superiority for information dominance, across multiple domains, especially in Grey Zone conflicts. Technological developments today promise cognitive and adaptive software defined radios and radars, have revolutionised the sensors (imagery and surveillance) and AI driven SIGINT and EW. Besides, convergence of 5G/6G and IoT technologies has ushered new possibilities, as well as vulnerabilities. Hitherto unexplored Directed energy weapons like High Energy Lasers and High Powered Microwave, and scalable EMP weapons are a reality. Emerging research in Terahertz spectrum and Quantum technologies is breaking new ground.

The EMS threat envelope is assuming unprecedented dimensions and in the future conflicts, this constrained resource will be heavily contested in time, space and direction. C4ISR capabilities in space and cyberspace can be severely crippled in an EMS denied and degraded environment. Superiority in the invisible battle-ground of EMS, and its assured and secure availability across domains, therefore, is a sine-qua-non for military superiority. The need for AI driven dynamic EMS management, together with agile and adaptive doctrines, organisations and systems, bolstered by leap-frogging R&D, and a clear roadmap, was never more urgent.

This issue of the Synergy Journal has compiled the challenges, possibilities and pragmatic strategies to achieve EMS superiority, comprehensively, in one volume. I am sanguine that it will find wide readership, which will cement a better understanding of the varied Military dimensions of EMS capabilities on the future battlefield.



(BR Krishna)
Air Marshal
CISC & chairman CENJOWS

FROM THE DIRECTOR'S DESK

Militaries endeavour to seek **information and decision superiority** to create overwhelming effects in the physical and virtual domains, so as to gain psychological and cognitive dominance, sapping the will of the adversary. **Networked system of systems, wired and wireless**, form the backbone of the transformed C4ISR, strike and sustainment functions. The **Electromagnetic Spectrum (EMS)** provides the **critical connective glue** which **delivers cross-domain synergy by seamlessly binding** the air, land, sea, space and cyber-space domains. However, excessive dependence on space, cyber and electromagnetic systems **has also created critical vulnerabilities** for the joint forces which the adversaries aim to exploit. Concurrently, critical services and information infrastructure, as well as competitive commercial exploitation of technologies like 5G/6G and IoT for citizens, need assured EMS availability, constraining availability for military use. The EMS, thus, is **increasingly getting constrained, congested and fiercely contested.**

Ironically, the Armed Forces have **traditionally viewed the EMS through the lens of Electronic Warfare, mostly restricted to tactical and platform centric capabilities**. Sophisticated exploitation of **EMS capabilities in recent conflicts and grey zone operations is instructive** and has already triggered wider debates and discourse in leading militaries on all facets of EMS, including management, dynamic

exploitation, cyber-electromagnetic convergence, organisations, doctrines, technologies for adaptive and multi-function systems and strategies, as well as R&D pathways, to build the desired capabilities.

This edition of Synergy **aims to ignite an informed debate on EMS capability**, a true **measure of cross-domain synergy**, which calls for collaboration and convergence not just between the three Services, but across ministries. **Innovative ideas, creative research and suggestions are invited**, for only then can we leapfrog to achieve a competitive advantage in cutting edge EMS capabilities.

(Sunil Srivastava)
Lt Gen (Retd)
Director

ELECTROMAGNETIC SPECTRUM- CRITICAL FOR MILITARY SUPERIORITY

Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)*

Abstract

Warfighting concepts exploit the physical (Land, Sea, Air, Space), information (Cyber & Electromagnetic Spectrum (EMS)) and cognitive (understanding, decision-making) domains to ***gain military superiority*** *in time and space. Traditionally, the attrition based approach to warfare has prioritised hard kill capabilities in land, sea and air domains. However, since late 20th century, warfighting concepts have evolved to achieve favourable conflict outcomes with* ***minimal attrition, placing greater emphasis on information and cognitive domains.*** *Military capabilities in the physical domains are heavily* ***dependent on the EMS,*** *which transcends and integrates them. A degree of* ***superiority*** *in time and space* ***in EMS,*** *is sine-qua-non to gain* ***information and cognitive dominance,*** *which* ***delivers military superiority, even in grey zone conflicts.*** *Cross-domain EMS capabilities, bolstered by disruptive technologies like AI, are critical for* ***outcome delivery in multi-domain operations (MDO).*** *EMS, however, is congested due to commercial use, constrained due to limited allocations, contested due to enemy actions and its* ***optimal exploitation is constrained*** *by doctrinal, technological, spectrum management and organisational shortcomings. The challenge is to* ***develop pragmatic and realisable strategies*** *for*

*organisational reforms, technology development, doctrines and policies for **EMS capability development** to achieve military superiority. This paper discusses the **salience of EMS in the information domain** in the competition-conflict continuum, the threat envelope, associated challenges and suggests **strategies to gain military superiority through EMS superiority,** in the Indian context.*

Grey Zone Conflicts and Information Dominance

A **binary** conceptualisation of States being **either at peace or at war is now irrelevant.** Traditional **wars,** where **violence** is the predominant means of **political coercion, are losing currency** since they carry **unacceptable costs**. However, **enduring peace** remains elusive and political **coercion** by States manifests as persuasion, coercion or compellence, in an **enduring competition-conflict continuum,** which entails competition short of conflict, conflict itself and return to competition[1]**.** This continuum is characterised by diplomatic **engagement** and military **deterrence; crises** below armed conflicts; and **few high-end, yet limited armed conflicts.** In a **conflict** between States, unlike a war, **violence** is not the primary, **but one of the means** of political coercion. Pure **competition** between States **rarely entails** military **violence,** but the **threat of violence (deterrence)** and other non-violent means are used to coerce and persuade[2]**. Deterrence and escalation dominance are critical** even during conflicts, to **preclude** undesired **escalation.** Instruments like **information warfare (IW)** hold greater salience in this **grey zone,** an **operational space between competition and conflict.**

The grey zone involves **coercive actions** to change the status quo, **below a threshold** that would prompt a conventional **military**

1 Kelly McCoy, "Competition, Conflict, and Mental Models of War: What You Need to Know about Multi-Domain Battle", Modern War Institute, 26 Jan 2018; https://mwi.usma.edu/competition-conflict-mental-models-war-need-know-multi-domain-battle/; Accessed 25 Dec 2021

2 Nick Bosio, "What Is War? Defining War, Conflict and Competition", Australian Army Research Centre, 5 March 2020; https://researchcentre.army.gov.au/library/land-power-forum/what-war-defining-war-conflict-and-competition; Accessed 26 Dec 2021

response, by blurring the line between military and non-military actions and attribution[3]. Operating **below the threshold** for military escalation is critical, especially between **nuclear armed adversaries** in the Indian context. **State-sponsored terror by Pakistan** against India tests **India's threshold** for escalation to a limited conflict. This **threshold was breached** by Pakistan's **grey intrusions** in **Kargil** (1999), but the Indian response remained **limited.** The Pakistan sponsored **terror-attack on the Indian Parliament** (2001) led to a prolonged face-off between both militaries, but India eschewed military operations in this **failed "military coercion".** Post the terror attack on **Mumbai (2008),** India chose to impose only **diplomatic costs.** Emboldened by India's strategic restraint, our **revisionist adversaries,** driven by escalation avoidance, risk aversion and economic costs, are **relentlessly attempting** political coercion at minimal costs, with **sophisticated grey zone** operations below the threshold of an armed conflict, which are **incremental and prolonged.** Their **provocative grey zone actions include** economic coercion, subversion, terrorism, cyber attacks, information campaigns, intrusions, infiltration, cease-fire violations, opportunistic land-grabs, stand-offs, military manoeuvres and clashes. I**ndia needs to operationalise** the **Kautilyan advocacy** of varied responses like Prakashayuddha (open war), Mantrayuddha (diplomacy), "Kutayuddha" **(concealed or psychological war)** and "Gudayuddha" **(clandestine war, without being at war)[4],** especially when the **tolerance threshold is crossed,** while ensuring escalation dominance.

India's **tolerance threshold was crossed** by Pakistan sponsored terror attacks at **Uri (2016) and Pulwama (2019) and coercive** posturing by China at **Doklam (2017) and Eastern Ladakh (2020).** This forced a **paradigm shift** in the restrained Indian responses, which now manifested in **surgical strikes** at the terror infrastructure in Pakistan

3 Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe, 'Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War". RAND Corporation, 2019'; https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf, accessed 27 Dec 2021

4 Kajari Kamal, "Kautilya's Arthashastra: Indian Strategic Culture and Grand Strategic Preferences", Journal of Defence Studies, Vol 12, No 3 July-Sep 2018, pp 27-54

(2016 and 2019), and **reciprocal military posturing** opposite PLA **in Doklam and Eastern Ladakh.** India clearly signalled a **capability and preparedness to climb** the **next rung** in the grey zone conflict, even **a limited conflict,** to **defend** her national security interests. **Deterrence and escalation control** are rooted in perceptions, and **information dominance** is the key. **Evidence of Balakote strikes and PLA casualties at Galwan assumed unprecedented salience.** Therefore, besides **hard and kinetic options,** India's military should have credible **non-kinetic** capabilities in the **information** (psychological, cyber and EMS) **domain,** to **deter the adversaries,** right from the inception of a crisis. Our response strategy must exploit **information warfare (IW) and EMS capabilities,** which are already being leveraged by most militaries.

EMS Superiority- A Key Enabler of Military Superiority

Evolutionary Background. Electromagnetic Warfare **(EW)** was heralded by radio interceptions in the Russo-Japanese War (1904). The **1920s** saw research on **"death rays",** eventually deployed as laser weapons in the 21st century. **Radars** were instrumental in downing the German aircrafts in the **1940 Battle of Britain. 1948-52** saw **jamming** of BBC and VOA by USSR. The **1962 Cuban missile crisis** could have witnessed **electronic deception** by drones creating radar signatures of U-2 Spy planes. The **1973 Yom Kippur war** saw Israeli missile boats **jamming Styx missiles.** The **1989 invasion of Panama** saw the **stealthy F-117s** defeating radar detection. The **1991 Gulf War** saw use of **GPS** for navigation and missile guidance, but also its vulnerability to jamming. **In the Indian context, EW arrived post the 1971 war.** Over time, our EMS capabilities have evolved. These are largely platform centric and include counter-IED measures.

Network-Centric Warfare (NCW) & EMS. Electronic traditionally refers to radios and radars, **whereas EMS** also includes IR, lasers, microwave, PNT signals and natural radiations. The EM Operational Environment (**EMOE)** is the space which includes **military as well as non-military usage.** EMS enables a joint force to **achieve asymmetric advantages**

against any adversary.[5] Militaries exploit information and networking technologies to integrate **dispersed decision-makers, sensors and shooters** to generate decisive combat power for achieving the mission outcomes. Essentially, shared situational awareness, **better and quicker decisions,** increased survivability, high tempo of operations, greater lethality and a degree of self-synchronisation help achieve this **NCW** capability[6]**. NCW translates information superiority into combat power,** which is substantially underwritten by exploitation of the EMS. **EMS has been exploited with telling effect** in conflicts like Yom Kippur, Falkland, Lebanon and more recently in Ukraine, Syria, Libya and Nagorno-Karabakh. Concerned by the growing EMS footprints of China[7] in the South China Sea[8], the US has ramped up its Electronic Warfare **(EW)** assets[9], to counter China's anti-access area denial **(A2AD)** capabilities. The US has also recently promulgated an **Electromagnetic Spectrum Superiority Strategy[10],** which emphasises that EMS provides the **critical connective tissue** that enables all-domain operations, and **represents a natural seam and critical vulnerability** across joint force operations. **Without EMS superiority,** a nation's economic and national security is exposed to **significant risk[11].** EMS threats have multiplied through the **proliferation[12]** of affordable **EW** and cyber tools to **Non-State actors.**

5 WR Alan Dayton, Winning the Invisible Fight: The Need for Spectrum Superiority; Center For Strategic & International Studies, Washington DC; Dec 2016; http://defense360.csis.org/wp-content/uploads/2016/12/Transition45-Dayton-Spectrum-Superiority-1.pdf; accessed 25 Dec 2021. p.1

6 For a graphical illustration of NCW, see "Network Centric Warfare: Creating a Decisive Warfighting Advantage", Director, Force Transformation, Office of the Secretary of Defense, Washington, 2003; https://www.hsdl.org/?view&did=446193; Accessed 26 Dec 2021

7 J Michael Dahm, "Electronic Warfare and Signal Intelligence: A Survey of Technologies and Capabilities On China's Military Outposts in the South China Sea", The John Hopkins Applied Physics Laboratory, LLC, 2020; https://www.jhuapl.edu/Content/documents/EWandSIGINT.pdf; accessed 25 Dec 2021

8 Matthew P. Funaiole, Joseph S. Bermudez Jr and Brian Hart, "China Is Ramping Up Its Electronic Warfare and Communications Capabilities near the South China Sea", Center for Strategic and International Studies; 17 Dec 2021, https://www.csis.org/analysis/china-ramping-its-electronic-warfare-and-communications-capabilities-near-south-china-sea; accessed 25 Dec 2021

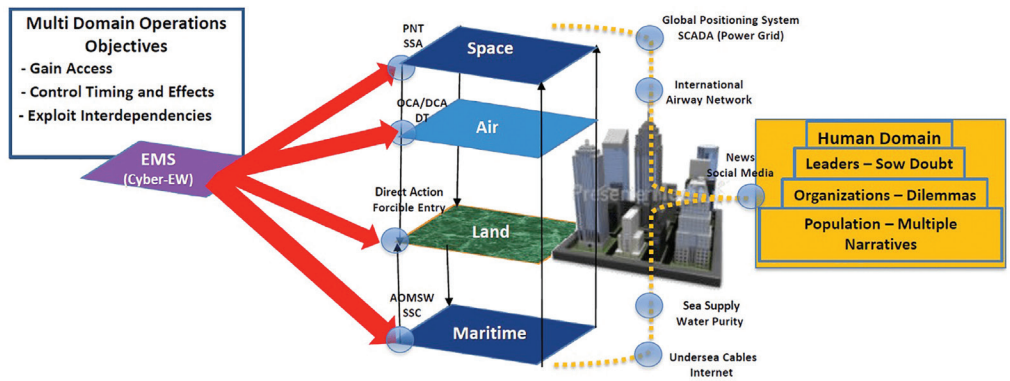
9 Ryo Nakamura and Tsukasa Hadano, "US to strengthen electronic-warfare abilities in South China Sea", Nikkei Asia, 17 July 2020; https://asia.nikkei.com/Politics/International-relations/South-China-Sea/US-to-strengthen-electronic-warfare-abilities-in-South-China-Sea; accessed 26 Dec 2021

10 DoD Electromagnetic Spectrum Superiority Strategy 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF, Accessed 16 Dec 2021

11 ibid

12 China Electronics Technology Group Corporation, a Government-affiliated company that produces much of the nation's spectrum-warfare hardware, is a fixture at major arms trade shows.

Military Superiority and EMS. IW impacts the **cognitive domain** and destabilises the adversary by **influencing the will of decision makers.** IW includes Psychological Operations (PsyOps), Deception, Cyber Operations (CO), EMS operations, operational security and Signal intelligence (SIGINT). **Cyber and EMS** capabilities **integrate the interdependent physical warfighting domains,** enabling **system vs system,** multi-domain operations. The **EMS empowers Space,** which **enables** operations in air, land, and sea domains, **in turn facilitating the ability to influence the human (cognitive) domain[13].** The interdependence of domains and actions to create multiple **dilemmas in the Human/ Cognitive Domain,** are depicted below[14].



Create multiple dilemmas at the time and place of our choosing with interdependent domain authorities

In essence, the **information domain (Cyber and EMS)** is where data and information are created, processed, stored and shared through robust, secure, resilient and reliable **networking- wired and wireless.** This is also the domain where information is denied, disrupted or degraded. The **cognitive/ human domain** is where information is evaluated by knowledge entities and **decision makers,** to arrive at

13 Jeffrey M. Reilly, "Multidomain Operations A Subtle but Significant Transition in Military Thought", Air and Space Power Journal, Spring 2016; https://apps.dtic.mil/sti/pdfs/AD1003670.pdf; accessed 26 Dec 2021

14 Ernest Nisperos, "Joint All Domain Effects Convergence: Evolving C2 Teams", Over the Horizon Journal, 10 March 2020, https://othjournal.com/2020/03/10/joint-all-domain-effects-convergence-evolving-c2-teams/; accessed 26 Dec 2021

timely and better decisions. The **physical domains (land, sea, air, space)** are where these decisions deliver **mission effects**- strikes and manoeuvres. **Military superiority, thus, entails** compressed planning and execution cycles, as each side aims to create **decision paralysis** for the other. **EMS** operations are at the speed of light, whereas **capabilities in other domains require time** for movement of forces. However, establishing **superiority** in any domain is **temporary** and **local superiority in different domains offers the freedom of action** to attain mission success[15]**. EMS can enable or cripple C4ISR and is, thus, critical for enabling** understanding and decision-making in the **cognitive domain,** which ultimately affects **the will to fight.** EMS, thus, is a critical arena for **military superiority.**

EMS Superiority and Fundamentals

- **EMS Superiority.** EMS environment includes all EM energy propagating through free space, as well as EM signals transmitted through wiring. **EMS is impacted** by enemy action, natural phenomenon, or interference by own systems. **Atmospheric and solar disturbances** degrade and distort **IR and optical** frequencies, **radar** accuracy, microwave transmissions, satellite links, HF radio and GPS accuracy. Natural **EMP** is hazardous for ordnance and volatile materials. Therefore, **EMS usage** demands deconfliction, mitigation, harmonisation, besides countermeasures. **EMS superiority entails gaining** access to a **mission critical segment** of EMS, **at a chosen time and place,** ensuring that harmful EMI will be mitigated and **access denied** to the adversary. **EMS superiority provides** greater **control of the escalation ladder,** giving additional options to handle real-time crises.

- **Military Uses of EMS.** Besides **growing commercial** devices, sensors, drones, mobiles and vehicles, the **EMOE** includes

15 Jeffrey M. Reilly, "Multidomain Operations A Subtle but Significant Transition in Military Thought", Air & Space Power Journal, Spring 2016; https://apps.dtic.mil/sti/pdfs/AD1003670.pdf, accessed 26 Dec 2021; pp 62-63

communication, C2 systems (data and signals-PNT, IFF), active and passive sensors (radars, IR) and attack systems (jammers, dazzlers). **EW applications broadly** use **RF** for communications; **Microwaves** for data-links, radars and SATCOM; **IR and UV** (greater bandwidth) for IR detection, intelligence collection, communications and sharing large volumes of data; and **lasers** for satellite communications, transmitting data, targeting, dazzling satellite sensors and destroying drones. Aircraft use IR to track stealthy aircraft and satellites use it to detect missile launches. **EMS** technologies deliver a **picture of the battle space** through like IR, radar and LIDAR. **Passive radars** leveraging GSM frequencies can detect stealth aircraft with head on or side flight profile. **5G technologies** in three bands- **high band** (MMW 24 to 300 GHz); **mid band** (1 GHz and 6 GHz); and **low band** (below 1 GHz), will have distinct features in each band. **5G military applications** include autonomous vehicles, C2, logistics, maintenance, AR/VR, IoMT and distributed ISR systems with improved data rates and lower latency. **EW** capabilities are terrestrial or airborne. **Thus,** the **C4ISR and counter-C4ISR** framework, which makes up the entire system of systems that enables sensing, decision-making and targeting, **depends heavily on EMS.** EMS systems need to be **interoperable, agile, trusted** and with **low signatures** to ensure **LDI/ LPD** (low probability of interception/low probability of detection).

- **EW Essentials.** Dependence on EMS is a vulnerability and **EW encompasses** the use of **EMS and Directed Energy (DE)** to ensure own assured use of the EMS or to attack the enemy. EW activities include detection, denial, deception, disruption, degradation, exploitation, protection and destruction. These are undertaken through EM Attack (**EA**-to degrade/deny enemy use of EMS), EM protection (**EP**-protecting own access to EMS) and EM support (**ES**-identify and catalogue all emissions to enable EP or EA). ES helps recognise threats, collect targeting and SIGINT data, and facilitate operational planning. **SIGINT**

comprises communications intelligence (COMINT), electronic intelligence (ELINT), and instrumentation signals intelligence. However, **ES and SIGINT** differ in purpose, scope and context. **ES largely relates to immediate operations (EA or EP),** but also feeds SIGINT, which is ongoing and intelligence driven. **EA** is a **silent Killer** since it is unnoticed until systems fail. EW also includes **navigation warfare,** which targets Position-Navigation-Timing (PNT) services. GPS spoofing of precision guided munitions (PGMs) has also been done successfully in Ukraine.

- **Directed Energy Weapons (DEW) and Massed Effects.** Massed effects can **destroy electronic devices** through high-powered microwave **(HPM)**, directed-energy **(DE)** and EM Pulse **(EMP)** weapons. A 2005 report on Chinese use of low-yield, low-altitude nuclear warhead is instructive[16]. **Microwaves heat the skin without injury** and high-power weapons can destroy ballistic missiles. Advanced microwave weapons and **non-nuclear EMP** weapons are flexible, reliable and scalable; and their **shrinking size** makes them **weapons of choice for terrorists[17].** High-power EM weapons can destroy the electronics of communications systems, AWACS, ISTAR, re-fueler aircrafts and LEOs[18]. The Counter-electronics High Powered Microwave Advanced Missile Project **(CHAMP)[19]** of US uses **high-power microwaves** lasting less than half the time it takes to blink, too brief to harm human beings, but more than enough to destroy electronic circuitry in a critical C2 node. **Vehicle mounted** 50-150kW High Energy Lasers **(HEL)**/ HPM can destroy UAVs, helicopters and rockets, artillery and mortar and **150-300 kW** systems on ships can counter cruise missiles. **Counter-UAV** systems employ a combination of radio, EO, IR, or acoustic sensors. Once detected, a UAV can be jammed,

16 ibid, p.64
17 JR Wilson, "The new era of high-power electromagnetic weapons", 20 Nov 2019, https://www.militaryaerospace.com/power/article/14072339/emp-high-power-electromagnetic-weapons-rail-guns-microwaves; accessed 25 Dec 2021
18 ibid
19 ibid

spoofed or destroyed using guns, nets, **lasers** or traditional air defence systems.

- **EM Radiations- Biochemical Effects.** Bursts of EM energy raise the skin and body temperature and **microwave or terahertz waves** can be used for crowd and perimeter control. **These are considered safe and effective,** since only the **very thin top layer of the skin is heated temporarily,** but it is intolerable. However, high powered microwaves can also damage the heart, create leaks in blood vessels in the brain, produce hallucinations and stun a victim. VLF EM radiations **can induce the brain to release chemicals that induce slumber** or flu-like symptoms, which dissipate when the radiation stops. A device called the **Pulse Wave Myotron** is commercially available, which **incapacitates movement or speech,** without affecting involuntary muscles like heart.

- **Multi-function Systems.** To reduce the signatures, multifunction EM devices are advantageous. A radar warning receiver **(RWR)** can locate, classify and possibly **identify** an emitting source.[20] Vehicle mounted systems can locate and suppress enemy networks, as well as provide near real time digital information.[21] **Advanced passive/ active EW systems** on fighters provide a 360 deg EW picture, while simultaneously jamming, **without interfering** with RWR and AESA radars. UAVs perform multiple **EW tasks.** Automated C2 systems, like the Russian **Baikal-1ME** also feed EW systems.

- **EMS Manoeuvre and Adaptive Systems.** Akin to land, sea and air, **forces must "manoeuver"** within the EMS. Besides **'time'** and **'space', EMS** manoeuver also includes **spectrum parameters** (frequency, power, modulation) to exploit the spectrum

20 Jonas Kjellén, "Russian electronic warfare: The role of electronic warfare in the Russian armed forces", Swedish Defence Research Agency, FOI-R-4625-SE, September 2018; https://www.foi.se/rest-api/report/FOI-R-4625-SE; accessed 30 Dec 2021

21 Lee, J., Jung, K. H., Jung, K. H., Choi, Y., Chung, Y-S., & Chung, H-K. (2020). Improved active interference canceling algorithms for real-time protection of 2nd/3rd level facilities in electronic warfare environment. Appl. Sci. 10(7). https://doi.org/10.3390/app10072405

dynamically. This is a paradigm shift from fixed usage. This freedom of manoeuver[22] helps **gain local superiority in the spectrum** to accomplish the mission. EMS manoeuvre is also achieved through **Adaptive and Cognitive Systems,** like Manet, programmable radars and AI-enabled EW systems. This agility **renders hostile EA ineffective.** Specialised EMS C2 structures are needed to enable EMS manoeuvre.

- **Spectrum Management and Sharing.** The **Government manages** the use of the radio spectrum (3Hz-300GHz) to balance government, private and public interests. Due to the **dual use nature** of EMS and miniaturisation, the global economy has an enormous dependence on EMS-based services. The wireless broadband industry is seeking additional spectrum to meet the demand for greater mobility and data connectivity. Efficient Spectrum Management Operations **(SMO)** are needed to facilitate frequency deconfliction and interference mitigation. During operations, EMS-enabled Cyber Attack **(CA), EA,** and **offensive space control** (OSC) must be **de-conflicted** to **preclude unintended effects.** The existing fixed frequency allocation is inefficient and **dynamic spectrum sharing must be adopted.** AI technologies need to be leveraged to enable **dynamic sharing** of the spectrum between commercial and military uses. Shedding of defence frequencies for commercial use impacts exploitation **of legacy equipment.**

- **EMS and Target Saturation (Swarming).** Drone swarms and simultaneous launch of a large number of missiles **swamp** defence systems. In recent conflicts, low-cost, small weaponised drones have evaded, saturated and defeated advanced AD systems, accomplishing EA and ES tasks. In Nagorno-Karabakh (2020) they were used for EA. However, **radar saturation has been overcome** with combination of kinetic AD systems and

22 JP 3-85, US Department of Defence, "Joint Electromagnetic Spectrum Operations", 22 May 2020;

EW systems, by the Russian **Pantsir AD and EW systems** to neutralise majority of drone attacks on Khmeimim air base (Syria).

- **Interoperability.** The capability to **interoperate securely with other Services remains a challenge,** since their Decision Support Systems and networks are yet to be integrated and the need for a **Joint Multi-Domain C2 System is yet to be met.** Notably, frequencies used for Defence in India are different from NATO, which also impacts multi-nation interoperability. Common system protocols, topologies and technologies can address the problem. However, a common system **can not meet the diverse, nuanced and future requirements of different Services.** Therefore, **the present systems,** evolved over time, **can not be easily shed.** However, advanced technologies that leverage **middleware**[23] that integrates **dissimilar systems** into SoS (System of Systems) provide a solution.

- **Net-enabled Weapons.** The **kill-chain comprises of five elements-** sensors, communications, processing, decision nodes and weapons. Network-enabled weapons, with two-way communications **are continually updated** after launch, to **guide, divert or abort** the attack. Combat **UAVs** require a **large amount of bandwidth** for command and data links. However, net-enabled and GPS aided weapons are vulnerable to EA.

- **Software Defined Radio (SDR) and Systems.** High capacity software-based mobile/ man-pack tactical radios (operating between 2MHz and 4GHz) **can bring together separate Service radio nets,** while ensuring **interoperability** with **existing systems.** These **systems** provide the capability to access maps/ visual data and satellite communications. These networks also integrate manned and unmanned systems. Software-defined systems can, thus, **change the threat spectrum** dynamically.

23 Todd Harrison, "Battle Networks and the Future Force Part 2: Operational Challenges and Acquisition Opportunities", Center For Strategic and International Studies, CSIS Brief, November 2021; https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211103_Harrison_Battle_Networks_Part2_0.pdf?vsuBpGNyDDOwNE_hMzckmGEfb8fq13dx; accessed 27 Dec 2021; p.9

EMS Operations (EMSO) and Cross-Domain Synergy

Modern militaries operate in an increasingly complex, congested and contested EM environment, which creates vulnerabilities and opportunities for spectrum dominance. Countries are developing integrated EW planning and management tools to provide enhanced synchronisation of EW capabilities[24] and creating Cyber-EW Coordination teams for **integration of CO, EW, SIGINT** and **SMO** with conventional fires and manoeuver, across multiple domains[25]. China and Russia see EMSO as central to gaining an **advantage in the techno-cognitive confrontation,** because this **domain links space, cyberspace and EW.** This synergy is becoming **essential at tactical levels, for exploiting fleeting opportunities** to unbalance the adversary. Russians opine that EW is the most effective and cost-effective means to neutralise technical advantages[26]**.**

- **MDO.** Since EMS pervades the physical domains, EMSO must be coordinated and de-conflicted in time and space. Militaries are creating new **Multi-Domain Task Forces** which can deliver long-range precision joint strikes, **integrate air and missile defence, EW, space, cyber, and IO** to provide integrated capabilities to defeat of A2AD and systems warfare strategies.

- **EMS and Cyberspace Symbiosis.** Most information, and certain weapon systems, have both **cyber and EMS-dependent components.** They increasingly use **cyber devices** like Digital Signal Processors, Graphic Processing Units and FPGA (Field Programmable Gate Array), besides memory devices, interfaces and operating systems to deliver functionalities. These **embedded computing (cyber) devices** in **radios and radars** create a **vulnerability in networks/ systems,** which

24 Michael Senft, Convergence of Cyberspace Operations and Electronic Warfare Effects, January 2016; https://www.researchgate.net/publication/338680628; accessed 25 Dec 2021

25 FM 3-12 Cyberspace Operations and Electromagnetic Warfare, Headquarters, Department of the Army, August 2021; https://irp.fas.org/doddir/army/fm3-12.pdf; accessed 25 Dec 2021

26 Chris Dougherty, "More than Half the Battle Information and Command in a New American Way of War"; The Center for a New American Security, May 2021; https://s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-2021.pdf; accessed 30 Dec 2021, p.19

can be exploited since **EMS provides an entry point for cyber actors, and vice-versa.** Thus, there is a **convergence between EMS and cyber capabilities. EW and CO**, both form part of **IO**, have **similar missions-** collecting information to disrupt and deceive the enemy systems; are used in conjunction and **complement** each other. Thus, most militaries are **removing the organisational and doctrinal divide between the two disciplines**, ensuring close integration between these capabilities. **Chinese** writings advocate Integrated Network EW **(INEW),** which combines EW, CO and kinetic strikes, and name **EMS a vital fourth dimension**[27]. Both China and Russia emphasise **CO early in** a conflict to cripple networks, and then **execute EW,** after adversaries switch to radio[28]. Russian forces in Ukraine have used a mix of EW and cyberattacks before artillery strikes[29]. CO and EW technologies converge in the **physical and protocol layers.**[30] CO can potentially penetrate AESA (Active Electronic Scanned Array) radars and SDR, since both **rely on software codes.** Cyberspace uses portions of the EMS, like Bluetooth, Wi-Fi and satellite links. Cyberspace and EW effects impact multiple domains simultaneously, necessitating early **integration at higher levels** into the overall scheme of manoeuver.[31] Notably, **some EM devices are not networked,** like stand-alone unattended sensors and expendable jammers, which need to be addressed by commanders in the field. Therefore, convergence of CO and EW would call for review of doctrines and procedures, **given that higher level approvals are required to conduct offensive CO.**

- **EMS in Space.** Military space capabilities like C2, communications, navigation, ISR, precision strikes, missile

27 Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2013 (Washington, DC: Office of the Secretary of Defense, 2013); p. 37.
28 ibid, p.18
29 ibid
30 Michael Senft, op.cit.
31 FM 3-12, op.cit, p.1-5

launch detection & tracking, and Space Situational Awareness (SSA) **entirely depend on EMS** that links **satellites, ground stations and users.** Significant **vulnerabilities** in the EMS can be exploited through jamming or spoofing and directed energy weapons. Additionally, **malicious code** inserted through EMS can allow remote control and prevent access to sensors or communications. While use of commercial satellites **facilitates dis-aggregation and redundancy,** but at slower functional speeds and no military hardening. EMS activities for space operations include **exploit capabilities** to identify the location of jammers; **attack capabilities** to deceive and disrupt enemy satellite uplink, downlink, or crosslink signals; **protect capabilities** to harden these links and sensors; **management capabilities** to deconflict EMS activities to mitigate EMI risks. These EMS capabilities **assure friendly use and degrade enemy use of space.** Importantly, EMS operations in the **space domain can** have unintended outcomes, that is why Ukrainian forces experienced very little jamming of their satellite communications, **because Russian satellites also use the same Ka-band** for satellite communications.

EMS and 'Grey Zone' Conflicts

- **Grey zone strategies** leverage both coercion and the risk of escalation. **An effective response strategy** for grey zone aggression must balance the risk of escalation with the need to be effective. Responses to **grey zone threats** are also shaped by **the political will** to use military power[32]. Any **inaction** is a sign of **weakness,** which **emboldens** the enemy's 'grey zone' attrition strategy[33]. Threat of an EM weapon can convince the responder to not only to de-escalate, but also **not to intervene at all[34].** For example, disruption of the Global Navigation Satellite System

32 Ignacio Nieto, "Electromagnetic Operations in 'Grey Zone' Conflicts-The Tool of Revisionist Countries to Confront the International Order", Joint Air Power Competence Centre, https://www.japcc.org/electromagnetic-operations-in-grey-zone-conflicts/; accessed 25 Dec 2021

33 ibid

34 ibid

could affect the economy, besides military targets and the target country is **unlikely to respond** given the **lack of attribution** and other **significant EMS vulnerabilities.** This establishes the viability of EM weapons in 'grey zone' strategies.[35] Analysts have argued[36] that EM weapons ensure escalation control and offer an **effective response strategy** by degrading sensor and weapon networks with small, less-escalatory attacks and denying adversaries the option of conducting scalable precision strikes. During **crises,** disruption of C2 will lower the morale and effectiveness of **isolated** units.

- **Escalation Control.** Creating decision and escalation dilemma in the minds of the adversaries may **prevent shooting wars.** The desired effects can be achieved with repeatable, scalable and affordable methods. **Ambiguous red lines,** backed by **credible resolve and capability,** are also **useful,** since clear redlines can be cleverly **circumvented** by a number of small-scale actions. Ambiguity, will deter the adversary. **Non-attributable and scalable punishments** through the EMS domain present a good option. A combination of non-kinetic EMS options and calibrated deterrent force posture strategies can be leveraged. New operational strategies are needed to **protect forces** postured in range of enemy long range sensors and weapon networks, **and degrade such networks, if necessary, without significant escalation,** by employing non-attributable EW. Thus, EMS concepts and capabilities can provide **escalation dominance** by adding another rung to the escalation ladder, while removing one for the adversary. EMS operations also deter grey zone small-scale strikes, leaving the adversary with **only the non-preferred option of large-scale** attacks. Should the confrontation escalate into a larger conflict, EMS would bolster force resilience. However, the **dilemma** in exploiting **EMS systems for EA** is that technical

35 ibid

36 Bryan Clark, Mark Gunslinger, Jesse Soloman, "Winning in the Gray Zone Using Electromagnetic Warfare to Regain Escalation Dominance", Center for Strategic and Budgetary Assessment (CSBA), 2017; https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final2-web.pdf; accessed 29 Dec 2021

parameters will be compromised, and the adversary will develop counter-measures.

- **Russia's Grey Zone EW Strategies.** The Russian Grey Zone doctrine is based on **reflexive control,** to covertly shape adversary behaviour to a more favourable pattern. As practiced in Ukraine, the Russian new-generation warfare **(NGW)** takes **five forms-** political **subversion**, proxy **sanctuary; intervention;** coercive **deterrence** and negotiated **manipulation**[37]. The Russian military accords primacy to the cognitive and psychological impact of information and considers **information confrontation** as a framework that includes cyber, space, EW, PsyOps and denial and deception **(maskirovka)**, which combines the information-technical and information-psychological aspects. Russia finds EW an **asymmetrical response** to NATO's technological edge[38]. In Ukraine, Russia has used EW to bring down drones, disable or prematurely detonate electronic fuses on shells/missiles and target forces whenever they used radios[39]. Small Russian **UAVs with EW pods** located and jammed counter-battery radars before Russian artillery strikes. Russia's EW shut down or manipulated Ukrainian cellular networks. Fake EW messages and manoeuvres triggered erroneous Ukrainian force deployment. Russian EW Brigades model the adversary C2, identify weak links, and execute **disorganisation plans.** The Russian **deception and disorganisation concepts** integrate information, cyber and EW[40]. Notably, the Russians did not enjoy an asymmetric technology advantage, but **exploited the Ukrainian doctrinal and strategic stasis.**

37 Phillip Karber & Joshua Thibeault, "Russia's New Generation Warfare", Association of the United States Army, https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare; accessed 25 Dec 2021

38 Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Centre for Defence and Security, Estonia; Sep 2017; p. ii; https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf accessed 25 Dec 2021

39 Todd Harrison, op. Cit. p.5

40 Brian David Johnson, Alida Draudt, Jason C. Brown, Lieutenant Colonel Robert J. Ross, "Information Warfare and age Future of Conflict", From 2019 Threatcasting Workshop hosted at Arizona State University, https://threatcasting.asu.edu/sites/default/files/2020-07/threatcasting-2020-The%20Future%20of%20Information%20Warfare-WEB_0.pdf; Accessed 25 Dec 2021

The EMS Threat Envelope- PLA Capabilities

In 2015 the PLA integrated its previously **disaggregated space, network and EW elements** by creating the Strategic Support Force **(SSF)** and **operationalised** the **INEW concept** of the early 2000s. The SSF is placed directly under the CMC, since **safeguarding China's security interests in space, EMS and cyberspace are China's National Defence aims[41].** The PLA advocates **information dominance early in a conflict,** and is pursuing **intelligentised warfare capabilities[42].** The PLA's concept of IO includes cyber, EW, space, technical reconnaissance (ie SIGINT) and psychological warfare[43] and combines these with propaganda, denial and deception[44]. The **311 Base,** tasked with the **"three warfares[45]"** now falls under the SSF. In the **space domain,** PLA has developed co-orbital, **EW and directed energy capabilities[46]** and is actively developing hypersonic weapons and EM rail-guns[47]. The PLA also intends to leverage **AI-assisted network vulnerability analysis and EMS management[48].** The Combined Arms Brigades have organic **information, EW** and UAV assets[49]. PLA conducts **cyber-simulation** and **annual training exercises** under realistic degraded EM environment[50]. EMS capabilities aim to degrade adversary's systems to **influence decision-making,** in conjunction with other non-military tools[51]**. Hard EW measures** like **non-nuclear EMP weapons or HELs**

41 Military and Security Developments Involving the People's Republic of China 2020 Annual Report to Congress, Office of the Secretary of Defence; https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-China-Military-Power-Report-Final.PDF, accessed 25 Dec 2021. p. 26

42 Military and Security Developments Involving the People's Republic of China 2021, A Report to Congress, Fiscal Year 2020, Office of the Secretary of Defense; https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF; accessed 25 Dec 2021; p. 86

43 ibid, p. 78

44 ibid

45 The Three Warfare Concept includes psychological warfare, public opinion warfare, and legal warfare.

46 N 42, p. 79

47 ibid, p.147

48 ibid, p.162

49 ibid, p.42

50 ibid

51 Marcus Clay, "To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power", War on the Rocks, 22 January 2021, https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/, accessed 25 Dec 2021

are advocated as tools for **strategic deterrence.**[52] PLA advocates the integration of **controllable and high-impact network (cyber) and EW** with rapid **high-intensity precision** strikes[53]. EW and network attacks are advocated on **satellite datalinks.**[54] Besides SSF, CMC level joint structures like the **Network and Electronic Bureau** and the **ECM Group** at the Joint Operations C2 Center likely coordinate and conduct INEW and EMS operations[55]. The **Winning Mechanisms of Electronic Countermeasures**[56]**,** an authoritative text[57], claims that **destruction of 10% of critical nodes** will collapse the **enemy's information network,** whereas the network would still remain intact even after **40% of ordinary nodes** are destroyed[58]. It divides enemy **targets into five categories-** reconnaissance; wireless communications; guidance and fire control; navigation and positioning; and friend-or-foe identification[59] and lays out three broad areas for **EMS confrontation- deterrence, deception, and destruction.** It advocates that **civilian infrastructure-communications, power and transportation, must also be targeted**[60]**.** The authors advocate shock and awe tactics, with a few **precision** strikes on **high value targets** to stun the **enemy into submission**[61]**.**

The PLA EMS concepts, doctrines and structures appear to have been **influenced by the Russian EMS capabilities.** Though **PLA EMS capabilities remain untested** in conflicts, it is evident that constant **field trials** and exercises in degraded EMS settings, together with **transformative changes** in doctrines, organisations and technology infusion like AI in EW, radio and radar systems, will present a **potent**

52 ibid
53 ibid
54 ibid
55 ibid
56 Shan Linfeng, Jin Jiacai, Zhang Ke. Dianzi Duikang Zhisheng Jili ("The Winning Mechanism of Electronic Countermeasures"), (Beijing: National Defense Industry Press, 2018).
57 Zi Yang, PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of "The Winning Mechanisms of Electronic Countermeasures"; 01 Feb 2019; https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/; accessed 25 Dec 2021
58 ibid
59 ibid
60 ibid
61 ibid

challenge for the Indian Armed Forces. More importantly, **growing interoperability and collaboration between Pakistan's military and PLA** will lead to an identical challenge form Pakistan.

Futuristic Decision Centric Warfare Concepts and Relevance in the Indian Context

- **Constraints of NCW.** Adversaries like PLA have credible sensor and precision targeting capabilities which present significant challenges. Gaining superiority over such competitors by simply using improved versions of present capabilities is neither feasible nor cost effective. NCW facilitates manoeuvre warfare concepts like **dislocation** and **disruption of centres of gravity,** and seeks to **pose multiple operational dilemmas** to the adversary by achieving a faster OODA cycle. However, this capability depends on the **agility and adaptability** of force structures, availability of **multi-domain resources, C2 structure, survivable networks,** unfettered C4ISR and automated **decision support systems. NCW centralises decision-making.** In reality, the dynamic management and **speed of decisions is hamstrung** by availability of multi-domain planning staff, unwieldy and vulnerable **division-sized formations,** degraded **communications and C4ISR, and weak mission command,** leading to poor and predictable decisions. NCW may fail to deliver cognitive and decision superiority.

- **Militaries are evolving** Decision-Centric Warfare **(DCW),** a new approach to warfare, which could deliver **decision superiority,** driven by **AI and autonomous systems. Autonomous systems** would enable force distribution and mission command. A **disaggregated** force design would make units and platforms re-composable with a C2 and communications (C3) approach called **"Context-Centric C3,"** where commanders would exert control over those forces with which they are in communication[62].

62 Bryan Clark, Dan Patt and Harrison Schramm, "Mosaic Warfare: ExploitingArtificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations", Center for Strategic and Budgetary Assessments, 2020; https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf; accessed 15 January 2022; p v

- **AI would empower decision support tools** that enable commanders to manage rapid and complex operations. DCW would address the limitations of Mission Command with a new C2 structure that **combines human command with AI-enabled machine control.** AI-enabled decision support tools would allow junior commanders to control distributed forces, adapt to environmental or adversary actions, and impose complexity on enemy decision-making. In this way, commanders would be able to execute Context-Centric C3[63], **where humans provide** flexibility and apply their creative insights, and **machines provide speed and scale** to impose multiple dilemmas on adversaries.

- **DCW** aims to **improve adaptability and survivability** by leveraging **distributed formations,** dynamic composition and recomposition, **reducing electronic emissions** and taking counter-C4ISR actions to increase the uncertainty for the adversary, degrading his decision-making[64].

- **Mosaic Warfare.** DARPA's Mosaic Warfare[65] **(MW**) concept offers an approach to implementing DCW. The central idea of MW is to create adaptability for own forces and complexity or uncertainty for the enemy, through the **rapid composition and recomposition of a more disaggregated** military force, **leveraging human command and machine control.** Implementing MW or other forms of DCW necessitates substantial **changes to force design and C2 processes.**

- **Force Design in MW[66].** The present forces and platforms are **monolithic and relatively inflexible** force configuration and **lack of interoperability** limits the ability to confuse an enemy as regards intent, so as to gain a decision-making advantage. A **larger number of smaller, manned-unmanned entities** could be more composable. For example, a section of strike-fighters could

63 ibid
64 ibid, piv
65 ibid. p vi
66 ibid, p. vii

be replaced by a strike-fighter acting as a C2ISR platform for a group of standoff missiles, sensors and EW-equipped UAVs. Such a disaggregated force would ensure an improved implementation of operational strategy by undertaking a larger number of simultaneous tasks, where unmanned systems could better enable the force to conduct feints or high-risk/high-payoff missions.

- **C2 Processes.** MW relies on a combination of human command and machine control. **Force design** changes presuppose **changes in the associated C2 processes,** since commanders would have difficulty managing the larger number of elements in a disaggregated force. **Without automated control systems,** taking advantage of force composition flexibility would not be feasible. The Commander would provide the assigned tasks, and estimates and effectiveness of the opposing forces. **The machine-enabled control system then identifies** the forces in communication that could be tasked and the commander **can then decide** the units to be made available for tasking.[67]

- **Implications for Spectrum Warfare.** A concept which relies on AI driven and automated and Context-centric C3, and relies heavily on **AI driven EMSO and SMO,** would certainly deliver EMS efficiency, drastically reduce EMS emissions and render the enemy's EA less effective.

- **Relevance in the Indian Context.** The DCW framework, while being conceptually sound, has limited relevance in the Indian context for two salient reasons. Firstly, the **level of AI and automation needed for a Cortex-centric C3** which entails human command assisted by machine-control, is not available. Secondly, the terrain in the parts of the Indian **battle-space has segmented and under-developed valleys,** which preclude rapid composition and re-composition, as well manoeuvre of disaggregated forces. The terrain imposes **certain inflexibility** and predictability, which constrain adaptability, both for own and

67 ibid

enemy forces. However, the **concept has relevance for the plains and the desert sectors,** and should be analysed and experimented. This could lead to another **challenge of having theatre specific force designs and doctrines,** whereas we do not have sector specific forces. However, AI and automation **assisted C2, man-unmanned synergy** and **AI driven EMSO,** would confer significant **advantages by themselves and should certainly be leveraged.**

Our Challenges and Constraints

EW systems in the Indian Armed Forces, ushered relatively late in the 1980s, **were non-indigenous and varied,** based on the country of origin. Technology thresholds and capabilities are varied and platform centric, with **low interoperability and integration.** The land forces have **front-centric capabilities,** which are gradually being ramped up, both for counter-insurgency and conventional operations. Constraints and challenges are many, and the more salient ones are summarised below:-

- **Legacy Equipment and Technologies.** Barring modern aircrafts and ships, most systems are legacy. **AI driven adaptive EMS capabilities** are the need of the hour. The induction of **SDR systems** has commenced in the Navy, and is underway in the other Services.

- **Propriety Systems.** Expensive and specialised EW systems with fixed characteristics serve specific functions and are **not upgradable or adaptive.**

- **Glacial Acquisition Processes.** Glacial induction processes render the systems **nearly obsolescent by the time they get inducted,** since commercial technologies in the EMS domain are evolving at an unprecedented pace. These advancements can be leveraged to achieve much shorter induction timelines.

- **Stove-piped Capability Development.** Capability development is Service-centric, platform-based instead of systems-based, and

is stove-piped. This results in a diminished **interoperability, EMI/ EMC** challenges **and equipment philosophy.**

- **Doctrinal and Organisational Evolution.** With rising cyber challenges, **Cyber and EMS** capabilities have seen partial functional convergence in the three Services. However, at the Tri-Service level, though the DCyA has been created for Cyber capabilities, there is **no structure at the apex level for EMS.** There is **no operational function as SMO** for dynamic spectrum management. **No framework like EMSO exists** for aggregation of cross domain capabilities. **Non-integration of cyber and EMS, PsyOps and deception capabilities under the IW/ IO framework** is the **biggest shortcoming.** DIA, charged with SIGINT, needs an interface with DCyA, besides SIGINT verticals of the three Services. DIA now lacks a formal interface with even the Defence Space Agency, since DIPAC has been shifted from DIA to DSA. **The land forces** have **inadequate integral EW** capabilities at the **tactical level.**

- **Workforce Challenges.** The cadre is very limited and military experts face contradictory pulls of career progression and domain specialisation. The **shortage of qualified language experts** is also acute. Both technical and language experts need to be harnessed from civil institutions and academia.

Winning the Information & C2 Confrontation

Success or failure in war is often incorrectly measured in terms of territory gained and enemies killed. A 2015 study, which has quantitatively examined 100 years of air and undersea competitions, shows that **it is often more cost effective to impose disruptions and inefficiency on adversary battle networks** than to **adopt traditional attrition warfare metrics[68].** Adversaries like China have prioritised information

68 John Stillion and Bryan Clark, "What it takes to win: Succeeding in 21st Century Battle Network Competitions", The National Interest, 10 July 2015; https://nationalinterest.org/feature/what-it-takes-win-succeeding-21st-century-battle-network-13304?amp; accessed 16 Jan 2022

confrontation, with special emphasis on systems warfare or C2 warfare. **Lines of effort**[69] to gain superiority in the information and C2 confrontation, **entailing doctrinal, organisational, technological and procedural interventions,** are outlined below:-

- **Shape the pre-conflict IE by-**
  - Streamlining and integrating the **conduct of IO/ IW** through doctrinal and organisational review.
  - Exercising the forces to deal with enemy's **information confrontation.**

- **Force a dilemma to escalate** the conflict beyond the low conflict thresholds (non-kinetic) and make it operationally imperative for adversary to kinetically attack information and C2 systems early in the conflict by:-
  - **Limiting the effectiveness** of reversible EMS attacks in **space and terrestrial systems.**
  - Dispersed, low signatures, mobile, hardened and **survivable information and C2 systems.**

- Challenge the **techno-cognitive confrontation** in space, cyberspace and EMS by-
  - Adopting policies and capabilities to **reciprocally attack** Information and C2 capabilities.
  - Develop capabilities to operate with **decentralised C2** in degraded and **contested EMS** environments.
  - **Reduce signatures and efforts** by accepting **good enough**

69 Chris Dougherty, "More than Half the Battle Information and Command in a New American Way of War"; The Center for a New American Security, May 2021; https://s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-2021.pdf; accessed 30 Dec 2021, p.1-2

targeting against **low** value targets, and adopt **rapid targeting** procedures for high-tempo operations.

- **Accelerate decision-making** by leveraging AI and bounded autonomy to reduce cognitive loads and.
- Exploit **deception** to foil adversary planning and targeting, **particularly with AI** or algorithmic systems.

- **Organise and Train for degraded MDO/ NCW:-**
  - **Multi-domain units,** across echelons of command down to the **tactical level are needed expeditiously.**
  - Ensure regular joint multi-domain training and exploit l**ive, virtual, and constructive** training to experiment and train in all domains, in a degraded environment.

Strategies for Spectrum Superiority in Competition-Conflict Continuum

Strategies to gain local EMS superiority must leverage technological disruptions. Since the adversary's EMS capabilities are constantly evolving, **adaptability** of own EMS systems needs to be accorded primacy. **EMS concepts and technologies** must **exploit our strengths, while mitigating the challenges.**

- **Border EMS Infrastructure.** Resilient and redundant **wired communications** and use of securely networked **passive receiving arrays, bi-static/ multi-static/ MIMO radars** should be prioritised in critical and vulnerable areas, being a costlier approach. **Active mono-static sensors** must have LPI/ LPD features. **Fibre networks** of CAPF and Military be **shared** to cut costs.
- **C2 and Survivable Networked Radios.** These include full MESH, ORAN (Open Radio Access Networks), MANET (Mobile Adhoc Networks) and SDR. These EM and optical based networks are

characterised by low latency, high bandwidth, **trust, security** and are adaptive, being software based. **5Gi is indigenous** and thus provides **secure** communications. 5Gi based sensor to shooter links will enhance operational tempo and its **fusion with AI** will **automate the Kill chain.** 5Gi has huge potential in remote areas.

- **Capability Development.** China's advanced commercial electronics industrial base will help field advanced EMS systems. Pakistan is likely to incrementally **adopt PLA systems to ensure interoperability.** This technological asymmetry must be addressed with **focused R&D and infusion of COTS** technologies, where feasible. **EMS asset** acquisition should be decentralised to the theatre level, supported by funds. **Technical concepts and capability requirements** for offensive and defensive EM weapons should be established as system of systems SoS rather than individual capabilities.

- **Scaling of EW Capabilities.** PLA deploys offensive and defensive EW resources **down to company level.** Our capabilities need to be scaled up at the tactical level.

- **EMS and AI Convergence.** Autonomous and cognitive EW capabilities must be developed by **harnessing AI and photonics.** Cognitive EW systems use AI to **identify hitherto unidentified** emissions and **effectively** jam the signal, using **real time decision algorithms. AI-enabled dynamic spectrum sharing is imperative,** since fixed allocations are not responsive to changes in the traffic volume. Adaptive **wide-band systems** can react to countermeasures in real time by using AI-enabled algorithms. **AI-enabled reprogramming** would also improve the adaptability of systems. **AI Enabled EMS Planning** can access cloud-based tools to accelerate planning.

- **EMS Coordination and Management.** Presently, the Army (Signals) oversees COMINT, whereas and the MI & DIA oversee SIGINT. Development of robust **EM battle management framework like EMSO** is a must. **Automated SMO** is needed for better management and coordination.

- **Robust ES and SIGINT.** EMS Superiority requires robust intelligence of **parametric data** of own, friendly, enemy and non-military systems in the EMOE; **engineering data; ORBAT data;** modelling and simulation and wargaming. Both ES and SIGINT need greater automation and AI infusion.

- **Multifunction ES and EA** systems would reduce the numbers of dis-aggregated ES and EA systems. US Digital EW System **(DEWS)** on aircrafts provides radar warning, 360 degree situational awareness, offensive targeting support and geolocation to improve survivability and enhance mission capability. DEWS **integrates** the receiver, DRFM jamming, and countermeasures dispenser with the aircraft central computer and radar, enabling **simultaneous jamming and receiving.** Such systems are needed urgently, since **they work with legacy systems** as well.

- **EP.** EP mitigates the impact of EMI from all devices in the EMOE. There is a **need to enhance** frequency agility in radios, variable PRF in radars, spread-spectrum techniques, multispectral and stealth attributes. **Critical nodes/ assets** must **be hardened** against HEL, HPM and EMP. Laser eye protection and GPS signal protection measures are needed too. EP includes EMC, emission control and operational reserve frequencies/modes.

- **Doctrinal & Organisational Transformation for EMS Warfare.** Non-lethal and non-physical warfare, waged through IW, cyberspace and EMS, calls for existing operational and strategic doctrines to be reviewed. Offensive cyber operations **(OCO)** target adversary systems and networks, **digitally affecting data by using data, for a military goal** and exclude **espionage[70]. OCO** can be **divided into "presence-based" and "event-based" operations[71].** The **former are strategic,** begin with network intrusions over time, conclude with an offensive objective, are intelligence community driven and need

70 Daniel Moore, From Spectre to Spectrum: Effective Military Offensive Network Operations, Department of War Studies, Kings College, London; https://kclpure.kcl.ac.uk/portal/files/110835374/2019_Moore_Daniel_1224743_ethesis.pdf; accessed 01 Jan 2022; p.9

71 ibid, p 2.

political oversight; whereas **the latter are directly-activated tactical-operational tools** that can be field-deployed to create localised military effects immediately[72]. **EA will** invariably be **event based,** whereas **OCO may be event or presence based,** but both need to hide abilities and excessively depend on intelligence. However, the two are quite distinct since EA is **mostly** at the **tactical or operational** levels (excluding the space domain), with usually localised effects, are reusable, need proximity and have short operational cycles. **EW and can enable OCO**, eg a small UAV can deliver EW codes which enable **future OCO operations;** and Digital Radio Frequency Memory **(DRFM)** technology allows manipulation and retransmission of **EM signals** which affect radars at the **software level, not sensory.** Such actions fall in the grey zone between competition and conflict, and exemplify just how **thin the dividing line is** between EW and CO, which will be **blurred further** as software defined systems proliferate. The author has rightly argued that **doctrinal and organisational differentiation** between **event-based and presence-based operations is necessary.** Not treating all OCO as "strategic" will facilitate integration of **EW and CO capabilities and lend flexibility at the operational-tactical levels,** allowing **field forces to undertake** event-based operations. Militaries are creating cross-domain capabilities in entities like Intelligence, Cyber, EW and Space **(ICEWS)** units to operationalise MDO, together with cyberspace and EMS **planning teams** across Army formations.[73]

- **EMS Driven Operational Concepts and Capabilities.** Matching system with system will be counterproductive and forces should become more **adaptable and less predictable** by leveraging operational concepts and technologies. EMS driven operational concepts and capabilities must include:-

  - **Degrading enemy search, sensor, communication and targeting capabilities** will help reduce own defensive weapons

72 ibid

73 US Government, 2019, Future Warfare: Army is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organisations, p. 2; accessed 25 December 2021 from https://www.gao.gov/ assets/710/700940.pdf

and enemy will require larger attack salvos, **closing the option for low threshold small-scale attacks.** Conversely, **enhanced survivability** of own weapon platforms will **reduce the number of weapons** required for attacks.

- **Small, Expendable EM Weapons.** Used individually or in swarms, could be used to signal intent and **impose costs with less escalatory** attacks which will also **be less attributable** than AD suppression[74]. This could be in conjunction with **less escalatory kinetic targeting** with small, precise, less costly expendable UAVs/loitering munitions, to gain **escalation control** in grey zone conflicts.

- **Drones and Decoys.** Expendable drones with **low power EA payloads** for jamming, hacking attacks and penetration testing are harder to detect and counter. Drones can have **EO/IR** dazzlers or **narrowly focused radar beams** to acquire accurate targeting information. Drones can also act as **decoys,** to provoke activation of fire control radars and thereby reveal geolocation and characteristics to passive radars. **Hunter-killer** manned-unmanned teams can **provoke** adversary EA systems, thus **exposing them to anti-radiation attacks** using smart munitions, with manned aircraft remaining at a safe distance[75].

- **Salience of Sensors.** Trends suggest that the ongoing transformation of **aerial combat** may reduce the utility of extreme speed and manoeuvrability, and **increase the value of attributes like electronic sensors and weapon payload.** The same holds true of **acoustic sensors.** LIDAR systems are harder to detect than radar.

- **Cruise Missiles with EMP.** Cruise missiles with HPM warheads can be launched from standoff distances to neutralise electronics-based A2AD systems.

74 Bryan Clark et al. op. Cit pp 67-68

75 Chris Dougherty, "More than Half the Battle Information and Command in a New American Way of War"; The Center for a New American Security, May 2021; https://s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-2021.pdf; accessed 30 Dec 2021, p. 37

  - **Undersea EMS expendables (UUVs)** will enable precise attacks from smaller naval platforms, reducing costs while imposing deterrence.

- **PME.** There is a need to incorporate EMS concepts and doctrine into PME and train skilled experts, eg. training to operate without GPS, radar, or radio communications. The forces must find solutions to **degraded** satellite navigation and air support communication links. In addition, troops need to be aware of danger of **targeted EW, OCO and IW, which exploits their internet activities.** Field headquarters need to reduce their electronic footprints.

- **Interoperability.** Moving away from propriety EMS platforms, adoption of open architecture would introduce modular systems that are interoperable and can be upgraded. **Making disparate communication networks of the three Services interoperable** is an urgent necessity.

- **R&D.** Research must focus on cognitive radio systems, cognitive EW systems, collaborative jamming, AI driven SMO and terahertz technologies for 6G. **Quantum technologies,** when fielded, will render the **existing EMS capabilities redundant overnight.** The following areas need immediate and focused efforts:-

  - **Quantum Antenna for Traditional ES[76].** Quantum antennas based on **Rydberg atoms** offer a **small size** of a few micrometers for even low frequencies (MHz to kHz). For multiple frequencies, there can be an array of antennas, or one dynamically changing the bandwidth. However, **cryogenics is needed** for cooling.

  - **Quantum RF Sensors (Rydberg).** Key enablers for advanced communications (LPI/ LPD), OTH directional RF, RF DF, RF-THz imaging.

  - **Quantum computing** for RF Spectrum analysers using Quantum AI/ ML. Direct analysis of quantum data from quantum RF sensors offers higher effectiveness.

76. Michal Krelina, "Quantum Warfare: Definitions, Overview and Challenges", 24 March 2021; https://arxiv.org/obs/2103.12548 accessed on 15 Jan 2022, p25

- **Quantum Timing.** Offers counter-DFRM and counter Radar jamming.
- **Quantum EW.** For SIGINT and Quantum EA, which will make the present day EW obsolete.
- **Quantum Radar and LIDAR.** While terrestrial quantum radar has size, cryogenic, cost challenges, quantum enhanced radars equipped with atomic or quantum clocks have high precision and can detect drones. Quantum LIDAR has counter drone application.
- **Space.** Quantum sensing and communications will revolutionise space capabilities, including quantum radar in the optical regime for SSA, which can detect debris (smaller than 5 cms) and small satellites, and stealthy objects.
- **Quantum Imaging.** These quantum devices are small in size and have **numerous applications in EO/ IR/ THz/ RF frequencies.** These function in fog, dust, smoke, foliage, night and defeat camouflage. Quantum range finders are stealthy, unlike the laser ones.

EMS Capability Development - Issues at the Apex Level

Salient EMS capability development issues that merit examination by at the Apex Level are:-

- Has a **Joint** EMS superiority **doctrine** been promulgated? Is **cross-domain synergy** between cyberspace, EMS and space, being leveraged to operationalise MDO/ NCW?
- Have **EMS capability enhancement programs** been prioritised in the **ICDP?** Are **adaptive** and multiple-capability systems being prioritised to enable **EMS Manoeuvre?** Is priority being accorded to technologies like SDR and DRFM? Have **unmanned and expendable EMS platforms** been prioritised? Have GPS alternatives been prioritised?
- Is the **budgetary allocation** for EMS capability development adequate?

- Is the **present defence spectrum allocation adequate?** Are the **Services using the spectrum efficiently?** Will there be a need to **relinquish or seek certain spectrum segments** in future, to support emerging technologies?
- What **organisational transformation** is needed to operationalise IW/IO? How are joint and Services organisations evolving do deliver a **EMSO** framework? Will our joint warfighting and C2 concepts result in **EMS reduction** in the battle space? Are **Multi-domain units** being conceptualised at the tactical levels?
- Is **interoperability** and EMI/EMC be ensured between the Services and with CAPFs, especially those in border guarding role?
- Are the DRDO, academia and industry aligned with the **EMS R&D priorities,** especially **Quantum technologies?**
- EMS technologies being inherently obsolescent and dual use, are the advances in **commercial technologies being harnessed to shorten the acquisition cycles?**
- How should the defence and civil **share the spectrum** dynamically? Are AI/ ML driven **SMO** capabilities being created?
- Are the workforce challenges, especially the shortage of language experts, being addressed?

Conclusion

To **reimagine military superiority** in the critical information and C2 confrontation, we need to adopt strategies that integrate information, cyber, EMSO and space into a multi-domain capability, **where EMS capabilities will play a very critical role,** since EMS provides the **connective tissue** that integrates and enables all warfighting domains- physical, information or cognitive.

***Lt Gen Sunil Srivastava, AVSM, VSM** (Retd)** is a former Commandant of the OTA Gaya and is presently, Director Centre for Joint Warfare Studies (CENJOWS), New Delhi

EMS MANAGEMENT CHALLENGES & HARMONISATION

Brig (Dr) Navjot Singh Bedi*

Abstract

EMS is a scarce limited natural resource transcending geographical and political boundaries; hence, coordination at the international level, regarding the efficient, rationale and need-based use of spectrum is the hallmark of spectrum management. Most modern communication technologies depend on the use of radio spectrum usage to facilitate proliferation of voice, video and data, which are instruments of empowerment. Though EMS extending from 3 KHz to 3000 GHz appears to be extensive, it is considerably limited as its usage is contingent to availability of appropriate technologies for communication purposes commercially.

The movement of our society and much of the world from the industrial age to the information age has been hastened largely by the liberalised availability of frequency spectrum. Countries that control the Geo-Technology domain will control all the other three domains of Geo-Strategy, Geo-Politics and Geo- Economics; nations which control these three domains will control the world.

EMS provides digital highways of connectivity required for development of business and for growth of education, healthcare and

other infrastructure. EMS is not merely about communications alone; it is in fact about improvement and growth in the fields of industry, automation, education, healthcare and other infrastructure—the list is endless. It is an end-to-end road for functioning and growth in various fields, as was evident during the recent COVID-19 crisis. With the world locked down to contain the spread of this pandemic, the governance of nations, routine administration, provisioning of essential goods and services, education and commerce was possible only due to the established communication and IT networks, which had been facilitated in no small measure by the grid of wireless networks. This is thus the importance of EMS and it's management.

National security is not restricted to securing the land, air and maritime boundaries and pursuing strategic interests but encompasses all aspects that have a bearing on the nation's well-being, of which EMS is an integral part. This precious resource of frequency spectrum thus needs to be guarded zealously and optimally utilised. EMS also has an associated economic value necessary for any nation-state to be able to leverage it and use the monetary gains for societal and development causes. Defence preparedness is also equally important for safeguarding the sovereignty of the nation, which permits all such commercial activities to take place. Thus, there is a need to reconcile both these requirements. Hence an efficient, rationale and need-based use of spectrum is the hallmark of spectrum management and regulatory mechanisms are key elements for ensuring efficient and interference free spectrum usage.

Introduction

Electromagnetic Spectrum (EMS). It is the entire distribution of electromagnetic (EM) radiation according to frequency or wavelength. Although all electromagnetic waves travel at the speed of light in a vacuum, they do so at a wide range of frequencies, wavelengths, and

photon energies. The EMS comprises the span of all EM radiation and consists of many sub-ranges, commonly referred to as portions, such as visible light or ultraviolet radiation. The various portions bear different names based on differences in behaviour in the emission, transmission, and absorption of the corresponding waves and based on their different practical applications. There are no precisely accepted boundaries between any of these contiguous portions, so the ranges tend to overlap.

Characteristics. Some of the important & typical characteristics of the EMS are:-

(a) Radio frequency spectrum does not respect international geographical boundaries as it is spread over a large terrestrial area.

(b) Use of radio frequency spectrum is susceptible to overlapping interference and requires the application of complex engineering tools to ensure interference-free operation of various wireless networks.

(c) Unlike other natural resources, radio frequency spectrum is not consumed upon its usage. It is wasted whenever it is not used optimally and efficiently.

(d) EMS usage is therefore to be shared amongst the various radio services and must be used efficiently, optimally & economically in conformity with the provisions of national and international laws.

(e) Limitation of the EMS is mainly due to the following factors:-

(i) Propagation characteristics of different types of radio waves.

(ii) Availability of technology and equipment for different types of radio frequency spectrum applications.

(iii) The suitability of frequency bands for specific applications

The information age presents us with tremendous possibilities as well as unique challenges. This is a very exciting time for the communications industry as technology is evolving quickly and new applications are being devised constantly. For a nation considered to be having the fastest-growing telecom industry, the issue of clarity in understanding the **EMS** or Radio Frequency **(RF)** spectrum and its optimum utilisation merits attention. Telecommunications today is considered one of the key factors in the development of a nation-state, be it in the field of economic, social, commercial or cultural issues. The telephone, which just used to be a communication device some time ago, has now the potential of being an instrument of empowerment. Most modern communication technologies are dependent on the use of radio spectrum usage to facilitate proliferation of voice, video and data, converged as triple play services, over the network in digital form.

EMS is a scarce limited natural resource extending from 3 KHz to 3000 GHz wherein spectrum management and regulatory mechanisms are key elements for ensuring efficient and interference free spectrum usage. EMS transcends geographical and political boundaries; hence, coordination at the international level, regarding the efficient, rationale and need-based use of spectrum is the hallmark of spectrum management. While the International Telecom Union **(ITU)** holds court as the international forum for regulating spectrum, there are organisations in India which create a fine balance in meeting the strategic requirements of Defence/ Government agencies as well as commercial requirements, both of which are in the nation's interest. It is thus imperative to have an understanding of the organisations and processes for regulating spectrum at the global, regional and national levels, for optimal projection of the spectrum requirements of the Armed Forces.

Types of EM Radiation. The entire EMS, from the lowest to the highest frequency (longest to shortest wavelength), includes all radio waves (e.g, commercial radio and television, microwaves, radar), infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays. The same is depicted in **Figure 1.1** below. Nearly all frequencies and wavelengths of

electromagnetic radiation can be used for spectroscopy. Propagation of radio waves has different characteristics in different frequency bands and these waves are influenced by the phenomenon of cosmic/man-made noises, terrain and varying climatic conditions. Though EMS appears to be extensive, it is considerably limited as its usage is contingent to availability of appropriate technologies for communication purposes commercially. An efficient, rationale and need-based use of spectrum is the hallmark of spectrum management.

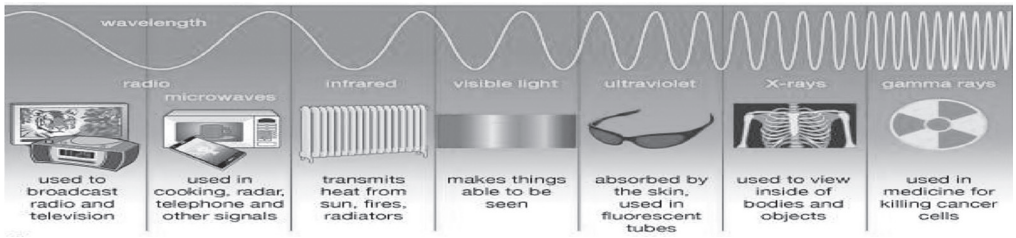


Figure 1.1: Types of Electromagnetic Radiation

Utilisation Based Frequency Distribution. Though the EMS appears to be extensive, it is considerably limited as its usage is contingent to availability of appropriate technologies for military/ communication purposes commercially. Different frequency bands have different characteristics for propagation of radio waves, which dictate its utilization for military/ commercial purposes.

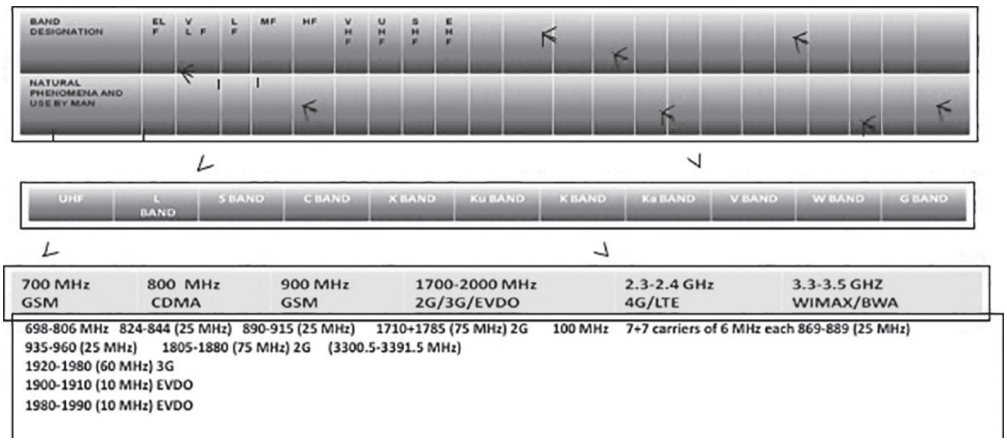


Figure 1.2: Utilisation Based Frequency Distribution

The propagation characteristics are even influenced by the phenomenon of cosmic/ man-made noises, terrain and varying climatic conditions. Figure 1.2 above depicts the 'Utilisation Based Frequency Distribution'. An efficient, rationale and need-based use of spectrum is the hallmark of spectrum management, and the same can facilitate harmonious coexistence of defence and commercial interests.

Background

In the late 90's the world has seen a convergence in telecom and Information Technology (IT), with telecom products being developed on computer platforms and multiple applications converging into a single device. The boundary lines between telecom and IT started blurring and the term Information Communication Technology (ICT) gained currency. With the advent of smartphones and tablets, mobile technology has integrated a number of these technologies with the ability to transmit wirelessly.

In mobile phones, there are no distinct data and voice channels. The introduction of voice over IP (VoIP) protocol though allows voice to be carried over the data networks, yet has a major drawbacks as this form of communication is susceptible to both EW and standard network attacks. Thus now in mobile phones, it is feasible that data-based attacks can impact the voice channels. Mobile phones, especially those with high processing power often double up as a mini computer and have replaced laptops. Mobile phone being a wireless device is the preferred internet gateway. Therefore logically it is susceptible to exploitation of the EMS.

The movement of our society and much of the world from the industrial age to the information age has been hastened largely by the liberalised availability of frequency spectrum which has, in turn, led to the proliferation of social media. The same has had an impact on the Armed Forces, providing both opportunities and challenges to both friend and foe alike. Countries that control the Geo-Technology domain will control all the other three domains of Geo-Strategy, Geo-Politics and

Geo- Economics; nations which control these three domains will control the world. In the emerging world order, India has a major role to play and in order to become a global leader, India needs to optimally utilise the EMS and harness the latest technologies like 5G and IoT.

Relevance of EMS

Previously, if one wanted to develop a village, people used to ask the government to build a road, because the moment a road was built, it opened the door for the villagers to access other parts of the country, where they could sell their produce, besides providing avenues for growth of business, employment, education and healthcare. The village thus used to develop and grow just because of the connectivity provided by the road. In the digital era, EMS provides 2G, 3G, 4G connectivity (with 5G round the corner), which are all types of a digital highways required for development of business and for growth of education, healthcare and other infrastructure. Digital connectivity is not just about communications alone; it is in fact about improvement and growth in the fields of industry, automation, education, healthcare and other infrastructure—the list is endless. It is an end-to-end road for functioning and growth in various fields, as was evident during the recent COVID-19 crisis. With the world locked down to contain the spread of this pandemic, the governance of nations, routine administration, provisioning of essential goods and services, education and commerce was possible only due to the established communication and IT networks, which had been facilitated in no small measure by the grid of wireless networks. This is thus the importance of EMS and it's management.

The EMS has been exploited with telling effect in conflicts like Yom Kippur War, Falkland and Lebanon and more recently in Ukraine, Syria, Libya, Nagorno- Karabakh and Israel-Hamas. India's adversaries are demonstrating growing capabilities in hybrid operational environments, especially aimed to degrade our capabilities in the cyber and EMS. Our C4ISR systems are critical for success in operations, ensuring the availability and reliability of communication and information systems, even in degraded environments. Concurrently, we must have the

capability to degrade and disrupt the adversary's communication and information systems. Coupled with this is the importance of availability of EMS for the nation's economic prosperity and communication technologies. Thus EMS management entails a fine balance between technology innovation, national security, growth and wealth creation & will be of special significance in the Gray Zone (a metaphorical state of being between war and peace), which is where the wars of future are likely to be fought. Such activity is most effective when malign activity is executed within legal boundaries so as not to set off any alarms or cross traditional warning trigger points. This paper explores the EMS Management Challenges & the need for Harmonisation of the scarce frequency spectrum.

Effect of Convergence between Communication and IT on EMS

With the advent of technology, multiple applications have converged into singular devices, and the boundary lines between communications and IT have started blurring. This convergence has also given rise to the commonly used term ICT. Modern day smartphones are capable of providing voice, data, video services, besides providing functions like calculator, camera, radio, news, entertainment, scanner, web browser, navigational aid, internet hot spot and so on. Mobile phone is however a wireless device and is the gateway to the internet. It is therefore susceptible to exploitation of the EMS, to carry out traditional EW functions, or to carry out cyber warfare.

ICT by its inherent attributes is able to integrate operations more effectively, provide decision support and thus an overwhelming degree of simultaneity can be achieved. If optimally utilized, ICT can fundamentally change the both the manner of conduct and the outcome of military operations. New and emerging Cyberspace and EMS threats first made their presence felt in the wars in Iraq and Afghanistan. Insurgents actively used the internet both for communication and for propaganda. At the same time, they skilfully used weapons enabled by the EMS, especially Radio controlled Improvised Explosive Devices **(IEDs)** or RCIEDs. All over the world cyber warfare through EMS is now being acknowledged

as the 5th dimension of warfare (after Land, Air, Sea and Space), as the same has the potential to tilt the balance of power, thus compounding the requirement and exploitation of EMS.

With the connectivity becoming increasingly wireless, the network technology is moving towards IP for all services. As per the TCP/ IP Model on which the whole data communication process relies, the IP Layer i.e. layer 3 and the layers above it were the standard cyber warfare gateway. However now, with the proliferation of wireless technology, the means to access & infect a computer network are now also available at physical layer in the form of Radio Frequency **(RF)** linkages. Hence simple RF level brute force jamming can be optimally exploited. With the advent of 5G and Internet of Things (IoT), the situation is getting more complicated. Technologies like mobile phone, satellites, wireless backhaul radios, software defined radio **(SDR)** etc are vulnerable to cyberattacks through wireless channels.

EMS in Ops. Operation Orchard. On 06 Sep 2007, with the launch of Operation Orchard, it which was probably the first time a converged EW and Cyber effort had taken place in modern warfare and the true potential of EMS was seen. Operation Orchard comprised of an Israeli airstrike on a suspected nuclear reactor in the Deir ezZor region of Syria, which occurred just after midnight. The Israel Air Force systems took over Syria's air defence systems, possibly using Digital Radio Frequency Memory **(DRFM)** technology to feed misleading information of a false sky-picture to the Syrian air defence radar system, for the entire period of time that the Israeli fighter jets needed to cross Syria, bomb their target and return.

Most of the telecom equipment, be it a router, a switch, or an IP radio is mostly being provided as a software service over a computing platform. Even telecom hardware based systems like telephone exchanges and satellite etc. are being managed through computer systems. The Combat Net Radio **(CNR)** is also now migrating to Software Defined radio **(SDR),** which provides an opportunity to carry out cyber warfare through exploitation of RF spectrum. Satellite phones,

surveillance devices, cellular phones, and trunked radio systems are also being used by the modern soldier in battle field. All these use a wireless access point and are thus vulnerable to cyber warfare through exploitation of EMS. This changed battle field ICT environment gives both sides enough opportunity to exploit EMS for conduct of operations. With the imminent advent of Internet of Things **(IoT),** the situation is likely to aggravate further because if IoT is to succeed, it has be wireless. Boundaries are being blurred and cyber warfare which was historically associated at strategic level (in state level conflicts) is now available at tactical and operational levels also due to the exploitation of EMS. Correspondingly, with traditionally civil services like banking, transportation, communications, power supply etc now being targeted, the common citizens sitting in the hinterland, will also be drawn into the conflict and will be connected to the outcome of the actions at the battlefield level. Thus digital attacks against vital infrastructure like banking systems or power grid, which can be launched through EMS, give attackers a way of bypassing a country's traditional defences. There is thus a strong correlation in the use of EMS by military and non-military elements of national power thus compounding the challenges of EMS management.

Blurring Domains. Both EW and cyberspace operations use wireless communication platforms, networking, digital platforms integrated with computers and multiply the effect of the other. EMS is used as a medium to exchange information between computers and this brings in the possibility of intrusion into a computer through EM spectrum. EW weapon systems are now being developed on computer platforms and are no longer discrete electronic based systems. Few examples of this latest genre of EW systems are SDR and DF systems. Traditionally EW targeted enemy communication systems through EMS and the Cyber Warfare used to target enemy computer networks. Now the dividing lines between these two are blurring and more often than not their roles overlap, thus enhancing the significance of management of EMS.

Management of EMS

The Defence requirements in the EMS need to be judiciously managed and aligned at the national, regional and global levels, for ensuring efficient and interference free spectrum utilisation. In view of the ongoing contest for spectrum allocation for commercial applications, it is necessary that Defence be aware of and have an understanding of the organisations and processes for regulating EMS at the global, regional and national levels, to ensure optimal projection of the EMS requirements of the Armed Forces. EMS is no longer merely about communication systems alone. The requirement of EMS is all-pervasive and is likely to effect and shape all platforms of war fighting in the days to come. Spectrum can be treated akin to a digital national highway, whose presence and availability is essential to drive various means of transport. It is thus extremely important to understand the EMS requirements, in order to be able to apply it or exploit it optimally for reaping military benefits.

Historical Perspective. The defence forces were earlier holding the majority of the frequency spectrum until 2006. However, with the growing demand for spectrum, primarily for mobile telephony (especially 2G & 3G services) and digital TV broadcasting, a need was felt to offset spectrum currently held with the defence forces for commercial use. This led to a review of the National Frequency Action Plan **(NFAP).** At the same time, to cater for the communication requirements of the Armed Forces, the Defence Band (DB) was identified and promulgated in 2015 wherein 09 sub-bands were earmarked exclusively for defence use, while in the remaining 42 sub bands the defence forces were asked to coexist with other commercial users. The Defence Band in the EM spectrum is a prime resource and it needs to be judiciously managed for ensuring efficient and interference-free utilisation.

The DB is however open to review and it is also possible that a few portions of the frequency spectrum, presently earmarked for Defence, might be reviewed in consultation with the MoD, if found to be lying un-utilised and might be made available for auction for commercial/ other purposes. The impending rollout of 5G and other national interests

may possibly warrant an earlier review of the DB and the Armed Forces must be prepared for the same. There is likely to be increased pressure from commercial players on the part of EM spectrum promulgated as a defence band. Defence preparedness is however equally important for safeguarding the sovereignty of the nation, which permits all such commercial activities to take place.

In view of the likely contest for spectrum allocation for commercial applications, there is thus a need to reconcile both these requirements well. At the same time, the Defence Band (DB) needs to be viewed in the light of the strategic implications of defence operations, the long gestation period in fructification of defence procurements and key reform initiatives being undertaken at the highest level. The EMS for defence cannot be taken in isolation as spectrum being a national resource has linkages of frequency spectrum for defence with legacy equipment, the future changes in technology, market structure and government policy. This paper endeavours to explain the necessity to understand and address this issue.

Knowledge regarding the various EMS regulating organisations at the global, regional and national levels and the processes that are followed is essential to understand the criticality of EMS. There is thus a need to put in place systems and procedures, that despite the peculiar constraints of the Armed Forces, they are able to overcome the challenges of spectrum access constraints, while continuing to deliver on the mandated task.

EMS Management at International Level. All nations share the EMS and reserve their right to its unlimited use. However, for international telecommunications, cooperation to support trade, transportation, communications, and mutual protection against interference, they have agreed to an International Telecommunications Convention. This serves as the basic instrument of the ITU and its supporting bodies. The United Nations recognizes the ITU as the specialized agency in the telecommunications field. The ITU maintains cooperation to improve all telecommunications. It allocates the international radio frequency **(RF)**

spectrum, registers frequency assignments, and coordinates resolving interference. Upon ratification by member-nations, ITU regulations have treaty status. Each ITU member-nation imposes regulatory measures within its administration. These measures must comply with the current **Radio Regulations (RR)** unless expressly excluded either by footnotes or by special arrangements.

National EMS Management Orgnisation. The Wireless Planning & Coordination **(WPC)** Wing under the Ministry of Communications **(MoC)** in the country plays the role of Spectrum Manager, while the Telecom Regulatory Authority of India **(TRAI)** plays the role of the national Regulatory Authority. Both these create a fine balance in meeting the strategic requirements of Defence/ Government agencies as well as the commercial requirements, both of which are in the nation's interests.

WPC. The **WPC** Wing of the Ministry of Communications, created in 1952, is the National Radio Regulatory Authority responsible for Frequency Spectrum Management, including licensing, and caters to the needs of all wireless users (government and private) in the country. It exercises the statutory functions of the Central Government and issues licenses to establish, maintain and operate wireless stations. It is divided into major sections like Licensing and Regulation **(LR),** New Technology Group **(NTG)** and Standing Advisory Committee on Radio Frequency Allocation **(SACFA)**. SACFA makes the recommendations on major frequency allocation issues, formulates frequency allocation plans, makes recommendations on the various issues related to International Telecom Union **(ITU),** resolves problems referred to the committee by various wireless users, provides site clearance of all wireless installations in the country, etc. All the allocations for use of radio spectrum are managed by different types of services (eg broadcast/ navigation etc) & exceptions to these allocations may be mentioned in footnotes for specific countries or reservations made by that country at the World Radio Conference **(WRC).**

TRAI. It was set up by an Act of Parliament in 1997. It acts as an independent regulator of the business of telecommunications in the country. Its mission is to create and nurture such conditions that

encourage the growth of the telecommunications sector in India so that the country can play an important role in the world telecommunications society. The main objective of TRAI is to form a transparent and fair policy environment that encourages fair competition. TRAI recommends the timing and need for the introduction of a service provider that is new, ensures successful inter-connection and technical compatibility between various service providers, and suggests the conditions and terms on which licences would be provided to a service provider. The National Frequency Allocation Plan **(NFAP)** forms the basis for development and manufacturing of wireless equipment and spectrum utilization in the country. It contains the service options in various frequency bands for India and also provides the channelling plan in different bands. Some of the typical frequency bands allocated for certain types of radio services in India in various areas are as given below:-

Sr No	Radio Service	Frequency Band
(a)	Radio Navigation	9 – 14 KHz
(b)	Mobile (Distress & Calling)	495 – 505 KHz
(c)	Broadcasting	526.5 – 1606.5 KHz
(d)	Maritime Mobile	2065 – 2107 KHz 2170 – 2178.5 KHz 2190.5– 2194 KHz
(e)	Fixed, Mobile, Broadcasting Radio Astronomy	610 – 806 MHz
(f)	Mobile, Fixed, Broadcasting	890 – 960 MHz
(g)	Mobile Satellite	942 – 960 MHz
(h)	Radio Location	1350 – 1400 MHz
(j)	Mobile, Fixed, Space operation, Space research	1710 – 1930 MHz

In India, allocation of spectrum to various services has been given in NFAP which covers frequency ranges from 9kHz to 3000 GHz and are being used for different types of services like fixed communication,

mobile communication, broadcasting, radio navigation, radio-location, fixed and mobile satellite service, aeronautical satellite service, radio navigational satellite service, etc.

Spectrum Regulating Organisations and Processes

The ITU Organization. The Plenipotentiary Conference is the supreme agency of the ITU. It formulates general policies, establishes budgetary guidelines, elects members, and concludes agreements between the ITU and other international communications organizations. It has three organizations: the World Radio Conference **(WRC),** the International Frequency Registration Board **(IFRB),** and the International Radio Consultative Committee **(CCIR).**

WRC may deal with all the radio communications services, or it may deal with specific radio communications services such as space, maritime, or aeronautical. Each WRC updates the Radio Regulations **(RRs)** which allocate radio spectrum use on a worldwide basis except where regional requirements differ and are agreed. Figure 1.3 below shows the three recognized regions.

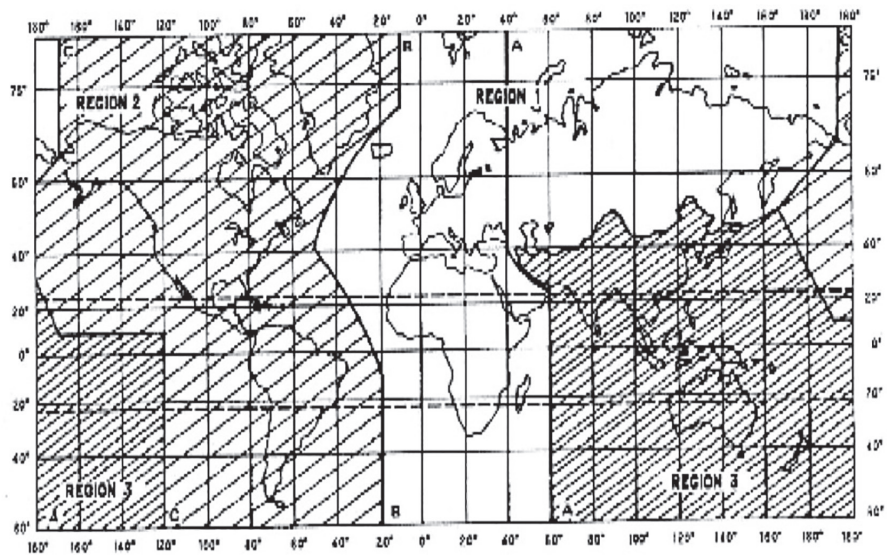


Figure 1.3: The three recognized regions as per ITU

In addition, the tropical area centred on the equator has additional provisions to offset its higher electrical noise. The IFRB records ITU member-nation frequency assignments. It advises the WRCs and member-nations on technical matters on harmful interference and radio spectrum use. The IFRB serves as the office of record of frequency assignments in priority and adjudicates interference conflicts among member-nations. The CCIR provides technical criteria on frequency sharing and examines technical and operational questions about international radio use. It also addresses technically related questions pertinent to ITU member nations and forthcoming WRCs. The findings of the CCIR serve a significant influence on the state-of-the-art and as a basis for **RRs.** However, these findings are recommendations rather than having an obligatory treaty status.

EMS Management at Regional Level: Asia Pacific Telecommunity (APT). The APT is an organisation of governments, telecom service providers, manufacturers of communication equipment, research and development organisations and other stakeholders active in the field of communication and information technology and serves as the focal organisation for communication and information technology in the Asia Pacific region. The APT now has 38 Members, 04 Associate Members and 137 Affiliate Members. Throughout the years, the APT has been able to help members in their preparation for global conferences such as the World Telecommunication Development Conference **(WTDC),** WRC, World Summit on Information Technology **(WSIS),** and the ITU meetings as well as promoting regional harmonization for these events. The APT Conference Preparatory Group for WRC **(APG)** is an important activity of the APT. The APG was started in 1996 with the objective of harmonizing views and developing common proposals from the Asia-Pacific region for the World Radio Conference **(WRC)**. The main objective of the APG is to take regional preparation to harmonize the views of the members and to develop common proposals for submission to the ITU World Radio Conference **(WRC).**

Telecom Circles, EMS Allocation Process & Harmonisation

Telecom Circles in India. The 22 telecom circles in India are shown in **Fig 1.4.**

SN	Telecom Circle Name	Circle Type
1	Delhi Metro Telecom Circle	Metro
2	Mumbai Metro Telecom Circle	Metro
3	Kolkata Metro Telecom Circle	Metro
4	Gujarat Telecom Circle	A
5	Karnataka Telecom Circle	A
6	Tamil Nadu Telecom Circle	A
7	Andhra Pradesh Telecom Circle	A
8	Maharashtra Telecom Circle	A
9	Haryana Telecom Circle	B
10	Punjab Telecom Circle	B
11	Kerala Telecom Circle	B
12	Rajasthan Telecom Circle	B
13	West Bengal Telecom Circle	B
14	Uttar Pradesh (West) Telecom Circle	B
15	Madhya Pradesh Telecom Circle	B
16	Uttar Pradesh (East) Telecom Circle	B
17	Bihar Telecom Circle	C
18	Northeast Telecom Circle	C
19	Assam Telecom Circle	C
20	Orissa Telecom Circle	C
21	Himachal Pradesh Telecom Circle	C
22	Jammu & Kashmir Telecom Circle	C

Figure 1.4: The 22 Telecom Circles in India

In Figure 1.4 shown above, Goa, Andaman and Nicobar Islands and Lakshadweep Islands are, respectively, parts of Maharashtra, West Bengal and Kerala Telecom Circles. Chennai was for some time a Metro Telecom Circles before it was merged into the Tamil Nadu Telecom Circle.

Spectrum Allotment Procedure. Any telecom company that wants to offer services in any of the 22 telecom circles in India, as explained in Figure 1.4 above, must purchase a Unified Access Services Licence **(UASL)** to operate in that circle. ASL was converted to Universal Licence **(UL)** after the 2012 Supreme Court decision on the 2G fraud delinked

spectrum from licences. The UAS, introduced in November 2003, is valid for a period of 20 years, which can be extended by an additional 10 years once, per licence per circle. As per the earlier policy, a mobile network operator who was awarded a licence to operate in any of the 22 telecom circles in India was allocated frequencies in that circle for a fixed period. After the expiry of the licence, the company was required to bid again to renew the licence. Only in certain cases were licences awarded Until Further Notice **(UFN).** The new telecom policy was announced by the Government in 2011. As a result, when an operator renews its licence, it must also pay separately for spectrum. The NTP 2011 has since been replaced by the National Digital Communication Policy **(NDCP)** of 2018.

Thus in the case of licensed telecom service providers, spectrum was initially allotted in accordance with the relevant provisions of the service licence agreements. Initially, the Government promoted additional free spectrum if TSPs could achieve a certain target number of subscribers.

Harmonisation. Harmonisation means de-conflicting defence and non-defence users by shifting their services to their respective share of spectrum to avoid electromagnetic interference.

A case in point is the harmonisation of 1700-2000 MHz Band. On promulgation of the DB, the Cabinet had directed defence and non-defence users to shift to their respective shares of allocated bands in the 1700-2000 MHz band by 23 January 2016, i.e., within a year of promulgation of the DB. This involved the relocation of Defence and Telecom Service Provider **(TSPs)** frequency assignments to their respective share of spectrum, as directed by the Union Cabinet. In this regard, Defence had submitted its harmonization plan to MoC & IT, well within the time frame. However the harmonisation process got slightly delayed due to non-availability of the harmonization plan of the TSPs with MoC & IT(now MoC). On its receipt, harmonisation was carried out pan India in five stages, staggered over a period of five months, in all the 22 Telecom circles in the country. Post completion of the harmonization in October 2016, the balance 20 MHz of spectrum as part of Network for Spectrum **(NFS)** stood released.

Methodology for Management of Defence Band

Rationale for Defence Band. The rationale for creating a Defence Band has been the national endeavour to allocate part of the national spectrum resources to the Defence Services, so that they can plan, develop, procure and operate systems so essential for the Defence forces for meeting any eventuality. Thus, a Defence Band has been identified mutually between the MoD and MoC & IT (now called **MoC**). The Defence Band covers the spectrum requirements of the Defence Services in the frequency bands up to 40GHz. However, in some sub-bands of the DB, some assignments of other ministries/ commercial services are present and would continue to exist till they are relocated outside the DB. The process of earmarking frequency for usage is done in three steps. The details and its connotation in the context of the DB are as follows:-

(a) **Allocation.** Allocation of a frequency band implies entry in the table of frequency allocation of a given frequency band for the purpose of it's use by one or more terrestrial or space radio communication services or radio astronomy services under specified conditions. In the context of the Defence Services, the identification of DB itself may loosely be construed as Allocation as WPC seeks clearance from Defence, i.e., JCES, HQ IDS, if any frequency spot within the DB, is sought by agencies other than Defence.

(b) **Allotment.** Allotment of a radio frequency or a radio frequency channel implies entry of a designated frequency channel in an agreed plan, adopted by a competent conference, for use by one or more administration for a terrestrial or space radio communication service in one or more identified countries or geographical areas under specified conditions. In the context of the Defence Band, it implies that if a frequency or frequency channel is allotted to a particular user, the user is free to develop/ procure its equipment for that frequency or frequency channel. Allotment of a radio frequency should be sought by the users before finalizing the GSQRs.

(c) **Assignment.** Assignment of a radio frequency or radio frequency channel implies that authorization has been given by an administration for a radio station to use a radio frequency or radio frequency channel under specified conditions. In the context of the Defence Band, it implies that a specific user would be allowed to operate the equipment or system under specified conditions (linked to location, time or technical conditions like power output, type of antenna, etc). Assignment of a radio frequency should be sought by the users only after the supply order for the equipment has been placed.

Safeguarding Defence Spectrum Requirements. Defence spectrum requirements are evolving as per the ongoing modernisation of the Armed Forces. Since the economic value of the spectrum cannot be ignored, it is required that the requirement of the Armed Forces be articulated holistically. This is required to be carried out in the Defence Band also as today the spectrum for the Armed Forces is no longer a 'given' thing. The spectrum identified as the Defence Band is also subject to review for development and societal reasons. In order to identify spectrum needs, the following is recommended:-

(a) Spectrum needs based on Long Term Acquisition Plan in respect surveillance, communication and weapon platforms be formulated.

(b) Utilisation of Defence Band be maximised and at the same time additional spectrum requirements for futuristic modernization be projected to MoC through MoD at the earliest.

(c) Build-up of roadmap for achieving Net centricity.

(d) Development of software tools to ensure effective spectrum management at all levels.

(e) Identify communication technologies that optimise spectrum usage in terms of bandwidth and fall within the Defence Band.

(f) Feasibility of re-use of spectrum at national and theatre levels be explored.

(g) Analysis of National Telecom Policy and policy roadmap for digital India which can impact spectrum usage at the national level.

(h) Study of adversaries EW capabilities to identify impact on own communication methodologies and it's overall spectrum requirement down to theatre level, to offset the same

(j) Spectrum requirements are subject to change. Hence, we can identify spectrum dependent systems and then identify the spectrum based on the life cycle of the platform for which it is required.

Meeting the increased requirement for spectrum dedicated to support unmanned systems likely to be used in a big way in future will require increased attention to spectrum management schemes and scheduling to promote sharing of frequencies. Additionally, technologies that increase on-board processing and compression of sensor data will assist in reducing the amount of contiguous bandwidth needed to support airborne data links. Without significant spectrum reuse and fielding of spectrum efficient technologies, unmanned systems will be constrained in their use of spectrum to achieve overall mission needs and may require highly refined scheduling plans to ensure that operations are executed within the limits of available spectrum.

Conclusion

National security is not restricted to securing the land, air and maritime boundaries and pursuing strategic interests but encompasses all aspects that have a bearing on the nation's well-being. In an information-dominated world, EMS is instrumental in providing the competitive edge among the global community, strategic and tactical superiority in conflict situations, and projection of national power and influence. In addition to capability enhancement towards national aspirations, investments are also necessary for securing these facilities against deliberate or unintentional intrusions or attacks and in ensuring safe and sustainable

operations. Wireless medium using frequency spectrum will be the preferred highway of choice where all these battles will be waged using the latest high–tech weapons. **This precious resource of frequency spectrum thus needs to be guarded zealously and optimally utilised.**

The spectrum also has an associated economic value necessary for any nation-state to be able to leverage it and use the monetary gains for societal and development causes. Telecom services are further planned to be rolled out in the country and there might be a requirement for spectrum, presently earmarked for defence, to be considered to be released for commercial purposes, in the overall national interests. Defence preparedness is also equally important for safeguarding the sovereignty of the nation, which permits all such commercial activities to take place. Thus, there is a need to reconcile both these requirements. The peculiar constraints of the Armed Forces, especially in so far as the long gestation period in fructification of defence procurements, needs to be factored into deliberations on these matters.

There is going to be increased pressure from commercial players on the part of EMS promulgated as the Defence Band. In order to obviate such a situation from arising, the three Services will have to diversify along the full spectrum, with suitable gaps for their own future expansions. There is thus a requirement to be aware of the various spectrum regulating organisations at the global, regional and national levels, analyse the Spectrum Management techniques and the processes that are followed, in order to better understand them. Knowledge regarding the EMS allocation process in India is also essential to understand the criticality of spectrum. There is thus a need to put in place systems and procedures that, despite the peculiar service specific constraints, the Armed Forces are able to overcome the challenges of spectrum access constraints, while continuing to deliver on their mandated task.

In view of the ongoing contest for spectrum allocation for commercial applications, it is necessary that defence must be prepared to optimally plan for utilization of the frequency spectrum allocated to them and ensure that the present holding is being managed well in a

judicious manner. At the same time, the need for continued retention of the Defence Band needs to be viewed in the light of the strategic implications of defence operations and key reform initiatives being undertaken at the highest level. This needs to be addressed in a holistic manner so that the defence forces are able to overcome the challenges of spectrum access constraints while continuing to deliver on the mandated task.

Though the defence spectrum requirement is a strategic need of the country, it should not be taken for granted due to pressures from other sectors. There is an urgent need to optimise the usage of the Defence Band by means of projecting for spectrum requirements to support both the present and future capacity build-up of the Armed Forces. The ready availability of requisite EMS for the Armed Forces and its effective management will be the deciding factor. Denying the war fighters' the use of any portion of the EMS would reduce flexibility and jeopardize mission accomplishment. The current Armed Forces EMS requirements are extensive and are likely to grow in the future.

Meeting the increased requirement for spectrum dedicated to support unmanned systems will require increased attention to spectrum management schemes and scheduling to promote sharing of frequencies. Additionally, technologies that increase on-board processing and compression of sensor data will assist in reducing the amount of contiguous bandwidth needed to support airborne data links. Without significant spectrum reuse and fielding of spectrum efficient technologies, unmanned systems will be constrained in their use of spectrum to achieve overall mission needs and may require highly refined scheduling plans to ensure that operations are executed within the limits of available spectrum.

The Armed Forces need to recognize the tremendous role that wireless communication, and thus, spectrum, can play in Defence. At the national level, there is always the classic guns versus butter paradigm, but security concerns must be addressed and the concerns of national

security need to be adequately addressed and should not be sacrificed at the altar of commercial progress.

***Brig (Dr) Navjot Singh Bedi** is a Brig PMO (DCN) and Commander DCA, New Delhi

References

1. http://www.itu.int/en/histor y/Pages/Constitution AndConvention.aspx

2. http://www.gsma.com/spectrum/resources/wrc-intro

3. https://www.apt.int/2019-APG

4. Tech 101: What Is Spectrum, and why is it Being Auctioned?"

5. "The History of Telecom Spectrum in India: The 1800MHz and 800MHz Auctions". NDTV.

6. http://www.medianama.com/2016/10/223-2016-spectrum-auctions-ends/

7. "Govt to auction 5G spectrum in frequencies above 3k MHz - Times of India".

8. "TRAI starts spectrum auction process with focus on 5G - Times of India".

9. https://paragkar.wordpress.com/spectrum/

10. Bedi (Dr) Navjot Singh "Appraisal of the Spectrum Requirements of the Armed Forces for Optimal Utilisation of the Defence Band", Cenjows, Dec2020, p.6-89.

11. Lt Gen (Dr) RS Panwar, China's Strategic Support Force and Its Implications for India, 16 June 2020. Future Wars; https://futurewars.rspanwar.net/chinas-special-support-force-and-its-implications-for-India-part-II/; 09 Nov 2021

12. Marcus Clay, To Rule The Invisible Battlefield: The Electromagnetic Spectrum And Chinese Military Power, 22 January, 2021. War on the Rocks. Https://Waronthe rocks.Com/2021/01/To-Rule-The-Invisible-Battlefield-The-Electromagnetic-Spectrum-And-Chinese-Military-Power/, 31 October 2021.

13. Bedi (Dr) Navjot Singh "RF Spectrum Allocation Process in India", Cenjows, July 2019, p 2 to 5.

14. US DoD EM Spectrum Superiority Strategy, October 2020. https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/electromagnetic_spectrum_superiority_strategy.pdf. 30 October 2021.

15. Bedi (Dr) Navjot Singh “5G, Iot & it’s Relevance for the Armed Forces”, Cenjows, Jun 2019, p.47.

16. In depth analysis: Spectrum auction September 2016”. TelecomTalk.info. 9 August 2016.

17. “Airtel, Voda, Idea, Jio, RCom, TTSL &Aircel apply to bid in largest spectrum auction”. 2016-09-14.

18. http://www.medianama.com/2016/10/223-2016-spectrum-auctions-ends/

19. “Govt to auction 5G spectrum in frequencies above 3k MHz - Times of India”. The Times of India.

20. “IMC 2017: Spectrum auction unlikely this fiscal, says DoT official”. Telecom,Economictimes. Sep 27, 2017.

21. “TRAI starts spectrum auction process with focus on 5G - Times of India”. The Times of India.

MILITARY USE OF EMS FOR INTEGRATED OPERATIONS

Gp Capt Puneet Bhalla*

...to understand, manage and control the electromagnetic environment is a vital role in warfare at all levels of intensity. The outcome of future operations will be decided by the protagonist who does this to decisive advantage.

Air Chief Marshal Sir Stuart Peach
Former UK Chief of the Defence Staff[1]

Abstract

Electromagnetic Spectrum is a critical enabler for operations across all physical domains and the information environment. A comprehensive understanding of the EMS and operations within it is critical to enhancing mission effectiveness and gaining and maintaining the desired degree of control within an integrated battlespace. The critical dependency on the EMS and the spectrum becoming more congested and contested has led to efforts at a more comprehensive exploitation of the EMS – integrated and effective across the full spectrum of operations, systems and domains. The modern ESM operations have evolved to include Electromagnetic spectrum management (ESM), Electronic Warfare (EW) and Signals Intelligence (SIGINT) as part of Information Operations and Communication networks. This would involve a comprehensive review

of the doctrine, organisation and force development and distribution and capability development in terms of technology, procedures and human resource.

Introduction

Technological development has been a key influencer in the evolution of warfare. This has been more evident in the last few decades, wherein an unprecedented rate of technological advancement has led to vast changes in the global security dynamics and the way military operations have been conducted. Electromagnetic Spectrum has been a critical component of military operations for more than a century. It gained prominence during the Bekaa Valley operations of 1982 as Electronic Warfare, whose success prompted a doctrinal shift worldwide in the use and denial of electromagnetic spectrum towards warfighting, to provide an advantage in the operational and tactical arena.

Advances in digital and networking technologies and their applications in the past couple of decades have led to an increasing dependence on the Electromagnetic spectrum (EMS). Also, easy proliferation of technology has led to threats becoming more diversified and unpredictable, resulting in varied types and levels of war the armed forces are expected to fight. As technological revolutions provide the capabilities for armed forces to undertake integrated operations, optimum utilisation of EMS has emerged as a critical capability for shaping the battlespace, enhancing awareness and undertaking sustainment operations, to achieve decisive results. A comprehensive understanding of the EMS and operations within it is critical to enhancing mission effectiveness and gaining and maintaining the desired degree of control within an integrated battlespace.

The EMS is a physical environment, which includes the full range of all possible frequencies of electromagnetic radiation. In the past, the use of the EMS as part of military operations has mainly been considered in a supporting role to achieve tactical outcomes and the focus has been on Electronic Warfare (EW) operations that aim at ensuring use

of the EMS for own forces, while denying the same to the adversary. However, the critical dependencies and the spectrum becoming more congested and contested has led to efforts at a more comprehensive exploitation of the EMS – integrated and effective across the full spectrum of operations, systems and domains. The US in its strategy document on Joint Electromagnetic Spectrum Operations of May 2020 has come up with a new concept called Electromagnetic Spectrum Operations (EMSO) that involves coordinated military actions executed to exploit, attack, protect, and manage the electromagnetic operational environment (EMOE) and resolve electromagnetic interference (EMI) in order to achieve the commander's objectives.[2] The UK has issued a Joint Doctrine Note (JDN) 1/18, in which it has also identified the convergence of Cyber and EMS Cyber and Electromagnetic Activities (CEMA).[3] NATO has recently recognised Electromagnetic Environment (EME) as an "operational environment" and a part of the battlespace where friendly forces manoeuvre in time, location, and spectrum to create electromagnetic effects in support of the commander's objectives.[4] Russia has displayed its prowess in controlling its EMS operations in Estonia, Georgia and Ukraine and more recently in Syria. China has identified the strategic importance and cross dependencies of electronic warfare, cyberspace operations and space and took a major institutional step in 2015 to create a Strategic Support Force, linking the three. It is investing in advanced EMS dependent military equipment and systems and in training specialist EM warriors and conducting EW operations as part of all its exercises and deployments.[5]

"Future conflicts will not be won simply by using the EM spectrum and cyberspace, they will be won within the EM spectrum and cyberspace. This will require changes to our operating concepts, military systems, and - most importantly - a new way of thinking in our Navy."

Adm. Jonathan Greenert
former Chief of Naval Operations
US Navy

As technological advancements are enabling synergising of forces, all conventional conflicts of the future, especially among adversaries with near peer capabilities, are expected to involve integrated operations. These integrated battlefields are expected to be defined by high tempo of operations, conducted in compressed time frame, necessitating quick manoeuvre and precise application of concentrated firepower, supported by efficient logistics. Advantage would be gained through multi-domain command and control, a higher degree of situational awareness and exploitation of superior technology. This would require integration of 'processes' across all operational domains of land, air, maritime, cyberspace and aerospace, towards optimisation of effort and enhancing effectiveness.

All these would be enabled through optimum exploitation of EMS, which transcends all physical domains and the information environment, making it critical to integrated operations across the air, land, sea, space and cyberspace domains. Commanders are dependent on EMS for their Command and Control of the battlefield, intelligence gathering and dissemination, communications, manoeuvring and mobility, targeting (kinetic and non-kinetic), coordinated application of firepower, position, navigation and timing (PNT) requirements and combat sustainment operations. This recognized need for military forces' critical reliance on the EMS also creates vulnerabilities and opportunities for exploitation. Hence, the EMS has become a contested arena, where advances in influencing the EMS are regularly countered through measures aimed at denial, disruption and deception.

Efficient use of EMS in Integrated Operations would entail coordinated EMS operations across the whole spectrum of military operations, comprising all synchronized military actions to exploit, attack, protect, and manage the electromagnetic environment (EME) to achieve the commander's objectives.[6] This aggregation would enable a unified approach to better identify, organize and disseminate concept of operations, user requirements, doctrines, resources, materiel and technologies, enabling Electromagnetic Spectrum Dominance in peace time, crisis and conflicts.[7] Electromagnetic spectrum management

(ESM), Electronic Warfare (EW), Signals Intelligence (SIGINT) as part of Information Operations and Communication networks are the components of EMS operations. A commander of an integrated force would have to address all four during planning and conduct of operations to attain and maintain EMS superiority during all phases of integrated operations. The freedom of manoeuvre within the EMS that this would provide would be crucial to conduct of all other missions within the operational area.

Spectrum Management. While the EMS is inexhaustible, it is limited in capacity and extends beyond geographical boundaries. An exponential increase in use of Spectrum Dependent Systems (SDS) for security and in the civil and commercial domains is leading to the EMS becoming constrained, congested and contested and requiring coordination not only within the services, but with multiple civil agencies. The dynamic nature of new age equipment is adding to the complexity of EMS environment. Spectrum Management involves planning, coordinating and managing access to the EMS during all phases of military operations so that all equipment and systems can operate without causing or suffering unintentional harmful electromagnetic interference. Harmonising the spectrum usage would involve collation of data, identification of interferences, allocation and deconfliction of frequencies and provision of consistent spectrum interference resolution by trained specialist combatants. The commander would also have to promulgate operational, technical and procedural orders towards unhindered use of the EMS in consultation with these specialists.

Electronic Warfare. Electronic Warfare is conducted to attain the level of superiority required to enable effective friendly forces' use the Electromagnetic Environment, while simultaneously exploiting, preventing or reducing the adversary forces' usage of EMS. It will require centralised planning, fully integrated with other aspects of joint operations, and decentralised execution, to ensure unity of effort while maintaining tactical flexibility. The integrated EW plan of the commander would encompass all its sub-elements. While the peacetime operations would be oriented towards obtaining data and intelligence, as the conflict

escalates, the emphasis would shift to attacks against the enemy's use of EMS. Defensive action would be achieved through adaptable, agile and flexible systems and equipment, with an ability to change their operating modes and characteristics (power, frequency, waveform etc.). Offensive EW action would aim at disruption, deception, degradation, and/or destruction of adversary's EMS dependent systems and would include kinetic and non-kinetic means, including Directed Energy Weapons (DEW). Offensive EW capability provides a non-kinetic option to a commander to influence the battlefield, in addition to the kinetic ones. However, in a modern-day battlespace it would entail a highly dynamic process, requiring near real time domain awareness and the ability of the system to provide instant solutions.

SIGINT. EMS operations cannot be undertaken without developing adequate awareness of the EMS environment in relation to the geographical location and operating parameters of all emitters. This is achieved through sensing, assessing and monitoring to ensure positive identification and tracking of all the emitters and associated platforms and weapons in the area of responsibility. This has to be supplemented by inputs from diverse agencies, processed, catalogued and stored in comprehensive libraries and updated in as near real time as possible. Enabling visualisation of Electromagnetic Order of Battle (EOB) as a subset of the overall ORBAT onto the Common Operational Picture (COP) of the commander would enhance battlespace management, provide decision support and allow synchronisation of kinetic and non-kinetic attacks in support of the broad objectives.

Communications. Effectiveness of all battleplans would be dependent on having a reliable, secure and resilient C4ISR network dependent on wired and wireless media. An ever-increasing demand for intelligence data, in terms of high-resolution video and images, is placing extensive demands on the EMS.

Achieving proficiency in conduct of these operations would require a change of perspectives of commanders and combatants related to integrated operations and the decisive role of EMS. At the

strategic level, this should be followed by a comprehensive review of the doctrine, organisation and force development and distribution and capability development in terms of technology, procedures and human resource.

Doctrine

Most current doctrines treat electronic warfare as merely an operational support function and it finds limited mention in Joint and service specific doctrines. There is a need to highlight the criticality of assured access to frequencies and bands of operations for successful conduct of operations in all other domains. Consequently, the EM environment can be identified as a battlespace, where adversaries would carry out offensive action and manoeuvre to gain control, similar to the primary objectives of operations undertaken in other domains. This would ensure that EMS operations form a fundamental part of the commander's plans in an integrated battlespace. These aspects could be promulgated in a fundamental document on EMS that provides basic principles and guidance for planning, executing, and assessing electromagnetic spectrum operations in an integrated battlespace across the competition continuum.[8] This in turn would act as a guiding document for coherent action towards relevant organisational changes, dedicated capability building and structured training, all as part of a roadmap with an implementable timebound plan.

Organisation

Based on the doctrinal review, organisational changes may be incorporated at all levels. A shift on emphasis from a services-oriented organisation to an integrated one would allow better engagement among all agencies, including government and non-governmental ones. It would reduce the bureaucratic layers and entities for managing, co-ordinating and developing systems connected with EMS, thereby promoting functional synergies. This would also help optimise the equipment, infrastructure, spectrum and manpower. A specialist directorate with adequate

empowerment and responsibilities would help address the strategic aspects of the EM environment and EMSO missions defined above. It would also draft the strategic and capability enhancement roadmap and ensure standardised EMS related training. At the operational level, the commander would be made responsible for command and control of EMS operations for which he/she would be required to issue EMSO guidance and instructions to achieve EMS superiority towards the overall objectives of integrated battle plans. Assistance for this would be provided by an EM specialist, akin to a component commander, who would also ensure synchronised employment of EMS based capability and more effective coordination of planning and execution. More specialist units need to be established and trained and these should be embedded at the operational and tactical levels for support as well as to undertake EW operations. Specialist officers at various levels would provide guidance for implementation of EW policies and instructions and supervise the conduct of all EMS operations within the AOR.

Capability Development

Capability development should aim at improving equipment and SDS' capability, augmenting spectrum availability and optimising spectrum usage. These efforts would once again gain through an institutionalised approach, especially for strategic and operational usage, as tactical systems cater to domain and service requirements. Efforts should however be made for service specific capabilities to reinforce and complement the integrated capability. Capability development should also aim for judicious use of budgetary allocations.

- There is a need to evolve to an agile, fully integrated EMS infrastructure with all domain capability. Integrated operations would require evolution and modifications of system architectures, both in hardware and software, to enable synergised EMS exploitation at strategic, operational and tactical level. However, initial action should be to build on interoperability of systems, while retaining flexibility to meet service-specific requirements.

- Integrated Operations would require development of a robust and secure integrated C4ISR architecture with sufficient bandwidth to handle data requirements. It should complement existing networks and allow for interfaces at strategic and operational levels.

- All future SDS should be designed to operate in dynamic, contested and congested EM environment. Endeavour should be made to upgrade existing systems so that they can be integrated into the advanced EM environment. Software defined equipment being developed should be modular, programmable, rapidly deployable and reconfigurable to suit mission requirements, while being efficient in its use of the spectrum. This would also address interoperability issues.

- The capability requirements should be defined in the integrated technology roadmap, to enable collaborative R&D efforts by government and non-government entities to provide indigenous solutions. A lot of EMS related innovation is taking place in the commercial domain, which should be studied for security related applications. Standards would have to be defined for all new equipment to enhance and sustain the interoperability between communication and information systems operated by various participants. Emerging and disruptive technologies and applications should be pursued for innovative approach. For example, Cognitive EW that involves use of advanced technologies like Artificial Intelligence (AI) and Machine Learning (ML) will make operations in the EM environment more potent and responsive.

- Traditional methods of EMS management and control are inadequate to address contemporary challenges of a complex and highly dynamic EM environment. It would require development and employment of advanced planning and management tools that in the hands of EMS specialists would allow commanders to better operate in the dense EM environment, deconflict and manage the very congested spectrum, enhance mission effectiveness, reduce planning cycles, coordinate effects and

collaborate with other mission command elements.[9] The US in its push for a unified approach to joint spectrum operations is investing in development of a comprehensive Electromagnetic Battle Management system. Such a system would have training tools and real-time electromagnetic spectrum monitoring embedded into it.[10]

- Unmanned Systems are becoming ubiquitous in the modern battlefield. They have vulnerabilities in terms of their reliance on EMS that could be exploited. At the same time, they could be utilised effectively as EW platforms, standalone, in buddy modes or as part of expendable swarms.

- Technology absorption in the armed forces cannot be effective without an associated review of the related command and control concepts, doctrine, and tactics, techniques, and procedures (TTP).

Human Resource Development

Effective conduct of EMS operations needs educated combatants that understand not just the technical aspects, but also the operational concepts and inter-relationship with the other warfighting domains.[11] Officers should undergo structured training in EMS operations. Exercises conducted during relevant in-service courses should include C2 aspects of EMS in support of integrated operations.

It also requires skilled operational crew to manage the EMS efficiently and in a secure manner and optimally handle the equipment to manoeuvre within the EMS. A core team of specialists, including personnel from all three services, should be developed. They should be trained in core capabilities at tactical, operational and strategic levels at designated centres that should be established for the purpose. The training should reflect the most advanced level of adversaries' capabilities and should be in line with technological advances. Their roles in integrated operations have already been discussed above.

All other operating crew, besides training for skill development on

their respective systems, need to be made aware of the fundamentals and protocols of operating through the EMS. Training should emphasise on EMS operations and management in a congested and contested EM environment.

Exercises. All joint and integrated exercises should include all aspects of EMS operations within the plans so as to align the EMS aspects with the overall objectives. These exercises would be utilised to validate concepts, procedures and capabilities. All equipment, procedures, coordination and management of EMS should be tested as realistically as possible, to include operations in congested and degraded EM environment. Besides improving competencies and awareness of participating combatants, lessons learnt from these exercises should contribute to the development and evolution of doctrines, structures, procedures and capability.

EM Ranges provide an ability to test and evaluate equipment and concepts in a secure environment. More EM ranges that cater to integrated operations, rather than service specific ones, should be established with adequate infrastructure to cater to a more expansive EMS environment and missions. Synthetic EMS training systems or EM simulators have become an inescapable necessity to train combatants to operate in a complex EMS environment. These should be able to replicate realistic scenarios and provide software to simulate contingencies. Using EW Ranges and Simulators in concert would help enhance understanding of EMS among all combatants, reduce training periods for honing of skills of operators and more effectively prepare EMS specialists in complex EMS skills and new inductions.

Conclusion

Recent campaigns have highlighted the importance of EMS in conduct of operations at all levels of conflict, spanning all defined domains of military operations. Integrated operations are complex as they require amalgamation of diverse elements within the operational area towards common defined objectives. EMS is a crucial enabler of these

synchronisation and coordination actions and efforts have to be made for assured access to the desired spectrum through technological, policy and coordination initiatives. The increasing dependence of militaries on the EMS for information advantage, decision superiority and operational advantage also makes it a crucial vulnerability to be targeted by the adversary. The Armed Forces must prepare for defensive and offensive actions to ensure availability of maximum spectrum and EMS combat elements and the freedom of manoeuvre and action within the EMS. This would require a review of the doctrines and restructuring of the organisation to give more importance to this critical element of integration and integrated operations. Investments will have to be made on capability building for the armed forces as part of a national plan involving both government and private sector enterprises. Indigenisation is a must for financial and security reasons and would necessitate R&D in contemporary and emerging technologies and applications. Technological advancements notwithstanding, human resource will continue to be the defining factor in any military operation and the armed forces should work in a coordinated fashion to achieve proficiency and awareness in order to achieve dominance in EMS.

***Gp Capt Puneet Bhalla** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi

References

1. Joint Doctrine of the Indian Armed Forces

2. US Electromagnetic Spectrum Superiority Strategy, October 2020

3. UK MoD Joint Doctrine Note 1/18, Cyber and Electromagnetic Activities, February 2018

4. UK MoD Joint Concept Note 1/17, Future Force Concept, Jul 2017

Group Captain Puneet Bhalla is a helicopter pilot of the Indian Air Force, with extensive flying experience in diverse roles, covering most regions of the country. He has also served as a member of the UN Mission to the Democratic Republic of Congo. He is an alumnus of the National Defence Academy Khadakwasla and Defence Services Staff College Wellington. His area of interest is technology and its application in support of national security. He has published papers and written articles on issues related to Outer Space, Unmanned Systems and Cyber Security.

Endnotes

1 UK MoD Joint Doctrine Note 1/18, Cyber and Electromagnetic Activities, February 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf. 12 December 2021

2 Department of Defense Electromagnetic Spectrum Superiority Strategy, October 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF. 04 December 2021

3 n1

4 Erik Bamford, Malte von Spreckelsen, Future Command and Control of Electronic Warfare, Joint Air Power Competence Centre, APCC Journal Issue 28, Spring/Summer 2019, https://www.japcc.org/future-command-and-control-of-electronic-warfare/. 29 November 2021

5 Marcus Clay, “To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power”, warontherocks, 22 January, 2021, https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/. 29 November 2021

6 n2

7 Daniela Pistoia, “Spectrum Management”, EMSOPEDIA, 30 Mar 2021, https://www.emsopedia.org/entries/spectrum-management/. 01 December 2021

8 n2

9 Mark Pomerleau, “Electromagnetic spectrum management tool coming next year”, C4isrnet, 03 Dec 2020, https://www.c4isrnet.com/electronic-warfare/2020/12/03/electromagnetic-spectrum-management-tool-coming-next-year/. 08 December 2021

10 ibid

11 Jimmy, “Hybrid Warfare, the Electromagnetic Spectrum, and Signposts for #highintensitywar”, From Balloons to Drones, 11 April 2018, https://balloonstodrones.com/2018/04/11/hybrid-warfare-the-electromagnetic-spectrum-and-signposts-for-highintensitywar/. 13 December 2021

CHINA'S ELECTROMAGNETIC SPECTRUM DOMINANCE CAPABILITIES AND CHALLENGES FOR INDIA

Brig (Dr) R K Bhutani (Retd)*

Abstract

In 2015, as part of its structural reforms, the Chinese People's Liberation Army's (PLA) took a major organisational step to fuse its previously disaggregated space, network and electronic warfare elements by creating the Strategic Support Force (SSF). Further, China strengthened its electromagnetic spectrum-enabled capabilities and these are now in near parity with the United States. However, SSF is not the only component of China's electromagnetic superiority strategy. There are number of other organisations involved in the PLA that have roles to play in the spectrum dominance. With its vast organisation, force structure combining Cyber and Electronic Warfare capabilities, China poses varied challenges to India at all levels - strategic, operational and tactical. There is publicly known information about PLA combat systems such as ships, aircraft, and missiles but comparatively little is known about PLA EW equipment, particularly the technical specifications. While protecting its systems using electromagnetic spectrum against Chinese penetration, India should develop asymmetric options to counter Chinese vulnerabilities.

Introduction

The United States Department of Defense (DoD), which has been closely

studying the military and security developments in the People's Republic of China (PRC), assessed in its 2000 report, "The PLA's emergent cyber capabilities were rudimentary; its use of information technology was well behind the curve; and its nominal space capabilities were based on outdated technologies for the day. Further, China's defense industry struggled to produce high-quality systems."[1] Two decades later, China has strengthened its electromagnetic spectrum-enabled capabilities and has brought itself to near parity with the United States. In 2015, against the backdrop of broader structural reforms, the PLA took a major organisational step to fuse its previously disaggregated space, network and electronic warfare elements by creating the SSF[2].

Adequate evidence is available, which indicates that the PLA is likely evolving its own high-level Electromagnetic Spectrum strategy. Chinese military strategists increasingly prioritise the exploitation and domination of the Electromagnetic Spectrum in their evolving military doctrines. Though the SSF has been described as the most decisive and forward-looking high-end force that will deliver the ultimate victory; the PLA propaganda machinery has kept the force's exact mission vague. During the National Day military parade in 2019, official Chinese sources described it as a well-trained force that enables the PLA to "achieve leapfrog development of critical disciplines."[3]

However, SSF is not the only component of China's electromagnetic superiority strategy. There are number of other organisations that have roles to play in spectrum management, force planning, senior level guidance for research support and provide inputs on the PLA's electronic warfare doctrines. Further, even at the operational level, the SSF is not the only command involved with the PLA's integrated network and electronic

1 "Military and Security Developments Involving the People's Republic of China 2020", US DoD Annual Report to Congress, p.1., https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-China-Military-Power-Report-Final.PDF

2 Marcus Clay, "To Rule the Invisible Battlefield: the Electromagnetic Spectrum and Chinese Military Power", War On The Rocks, 22 January 2021, https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/ , accessed on 21 December 2021.

3 Ibid.

attack missions. The Joint Staff Department's Network and Electronic Bureau is possibly also playing a part. Another entity is the Joint Staff Department Network Electronic Countermeasures Group that is attached to the Central Military Commission's Joint Operations Command and Control Center, which likely coordinates PLA Air Force, Army, Navy, Rocket Force, and SSF electromagnetic spectrum operations.[4]

Unlike the Western military thinking where the organisational structures and their hierarchical functions are well-defined and are clearly demarcated, Chinese organisations are intertwined in to a web of duplicity, either intentionally to deceive their adversaries about their actual role or functions or their way of functioning itself is complex. With a view to clearly understand the role and functions of their various organisations and determine what challenges they pose for India, it is intended to analyse the subject in the following sequence :-

- China's Electromagnetic Spectrum Dominance Strategy and Operational Concepts.
- Organisation, Force Structure and Capabilities.
- Challenges for India.

CHINA'S ELECTROMAGNETIC SPECTRUM DOMINANCE STRATEGY AND OPERATIONAL CONCEPTS

The PRC's PLA has dramatically improved its ability to operate in and control the electromagnetic spectrum during the past 20 years through a combination of civil-military fusion, industrial espionage and robust R & D investment. In PLA doctrine, the information environment includes the electromagnetic spectrum, cyberspace, and psychological environments and is also known as a Unified Network-Electromagnetic Space[5] (as shown in Figure 1 below).

4 Ibid.

5 Bryan Clark and Timothy A. Walton, "The Invisible Battlefield: A Technology Strategy for US Electromagnetic Spectrum Superiority", Hudson Institute, Center for Defense Concepts and Technology, March 2021, p.18., https://rvjinstitute.org/wp-content/uploads/2021/04/invisible_battlefield_report.pdf, accessed on 22 December 2021.

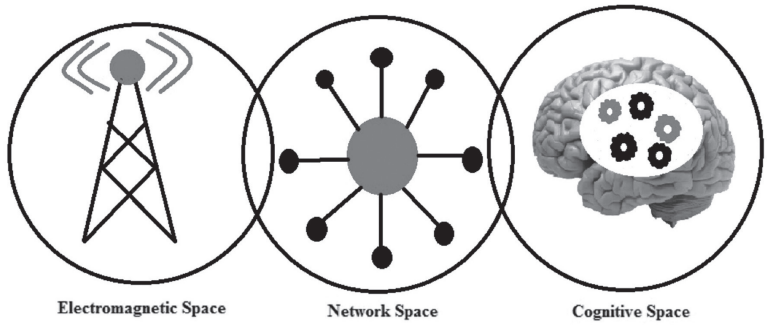


Figure 1: Network Electromagnetic Space

Since the time Xi Jinping as PLA's Commander-in-Chief first expressed his personal interest in the subject, a number of articles exploring *"winning mechanisms for informationized warfare"* have been published. *"The Winning Mechanisms of Electronic Countermeasures"* is one of the more prominent texts that has emerged to satisfy Xi's concerns. Most significantly, *Winning Mechanisms* is the only monograph since the initiation of the 2016 PLA reforms that systematically explains PLA strategists' thinking about achieving a superior position in the electromagnetic spectrum. It has been authored by a group of electronic warfare (EW) experts from the National University of Defense Technology's Electronic Countermeasure Institute. According to this strategy, the spectrum's significance can not be overstated since it is the main carrier for information in all domains of war. ***Winning Mechanisms*** **concludes that whoever controls the electromagnetic spectrum, and has the capability to deny enemies from effectively utilising this channel, will have tremendous advantages in securing victory**[6] and it describes four distinct stages in achieving electromagnetic superiority:

Meticulous Planning. Having accurate intelligence and a comprehensive understanding of enemy's capabilities ahead of battle will enable prompt assessment and decision-making. Such diligent planning will ensure

6 Zi Yang, "PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of "The Winning Mechanisms of Electronic Countermeasures", China Brief Volume: 19.Issue: 3, 01 February 2019, https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/ accessed on 21 December 2021.

that the PLA will always be ahead of the enemy in conducting sustained offensive operations, and in keeping the enemy off-balance.[7]

Multilevel Integration. This stage focuses on providing friendly forces with real-time intelligence. Battlefield intelligence is collected from radar, electro-optical/infrared (EO/IR) and electronic intelligence (ELINT) sensors on land, sea, air and space platforms so as to guide the decisions of commanders and operators in fighting jointly. This necessitates integration of platforms, systems, and "systems of systems" to ensure that friendly forces can effectively move and fight as one. Further, PLA's intelligence, information support systems and systems for reconnaissance, surveillance, communications, navigation, position, and guidance must all be hardened and protected against enemy electronic and physical attacks.[8]

Precise Release of Energy. The battlefield environment is fast changing, therefore, friendly forces cannot waste time and resources with imprecise attacks. The precise attacks would avoid collateral damage against civilian electronic infrastructure, which could have negative legal and public opinion ramifications. Friendly forces must identify and strike at "critical nodes" in enemy's networks at the onset of an operation. Critical nodes that can lead to the defeat of enemy operational systems differ depending on the opponent but are categorized in to five broad groups: reconnaissance and early warning, wireless communication, guidance and fire control, navigation and positioning, and friend-or-foe identification. The strategy asserts that destroying 10 percent of critical nodes is enough to collapse the enemy's information network. In contrast, the network would still remain intact even after 40 percent of "ordinary nodes" are destroyed. Strikes must therefore be performed in a systematic fashion, and assessments are necessary in improving upcoming attacks.[9]

Demonstration of Effects in Multiple Areas. Precise strikes alone cannot secure victory. Three main techniques/ concepts have been

7 Ibid.
8 Bryan Clark and Timothy A. Walton, op.cit., p.19.
9 ZiYang, op.cit.

identified by which the PLA intends to confront the enemy: **electromagnetic deterrence, deception and destruction.** Electromagnetic deterrence and deception, both rely on a strong psychological component. PLA strategists visualise that by demonstrating the PLA's sophisticated electromagnetic strike capability and willingness to employ such means without hesitation, electromagnetic deterrence will exploit the enemy's fear of losing expensive, critical electronic assets. Propaganda on PLA war games, intentionally leaking snippets of information about PLA's electromagnetic weaponry and publishing works on EW theories and doctrines are the means to intimidate adversaries by showing PLA's ability to strike vulnerable nodes in the enemy information network - thus compelling the enemy to think twice about an Electromagnetic Spectrum face-off with China. PLA's strategists believe that deterrence will be especially effective when the enemy commander is weak-minded. When it is disclosed that the PLA has state-of-the-art electromagnetic weapons such as high-powered microwave weapons and is prepared to use them, a weak enemy commander will be afraid and retreat. Alternatively, it may sow seeds of doubt in enemy's mind, making him indecisive thus accomplishing the goal of winning without fighting. In conjunction with these two, electromagnetic destruction will inflict substantive physical damage on enemy forces. Suppressive jamming and firepower will be employed simultaneously with a view to enhance damage to critical nodes in the early warning, communications and "latent-potential warfare system" i.e., to target civilian infrastructure (which is in contrast of Paragraph 3 above) also. The text recommends striking telecommunications systems with a view to disrupt communications between enemy's government and citizenry, foster popular discontent through disrupting the electric power system, and degrade transportation systems that support enemy's troops mobilisation and deployment.[10]

Operational Concepts

Based on *"The Winning Mechanisms of Electronic Countermeasures",*

10 Ibid.

the PLA has evolved two operational concepts to describe war fighting in the electromagnetic spectrum:

- **Integrated Network Electronic Warfare (INEW).** Introduced in 2002, INEW combines EW and cyber capabilities. It involves disruption of enemy information acquisition and transmission using EW; with attacks on information processing and decision-making through cyber warfare.

- **Integrated Information Firepower Warfare.** This concept was first revealed in 2018 and it aims to integrate kinetic and non-kinetic means into a single "information force structure." This describes a more sophisticated use of EW and cyber systems than INEW, including the employment of truly integrated capabilities, such as RF-enabled cyberattacks.[11]

ORGANISATION, FORCE STRUCTURE AND CAPABILITIES

PLA Joint Staff Department's Network-Electronic Bureau (JSD NEB)

It was created as part of a broad set of reforms during 2015 to oversee EW and cyber missions across the entire PLA, establishing operational guidance, capability requirements, and rules of engagement for network and electronic countermeasures operations. Consistent with the strategy and operational concepts as described above, PLA EW capabilities are organized into:

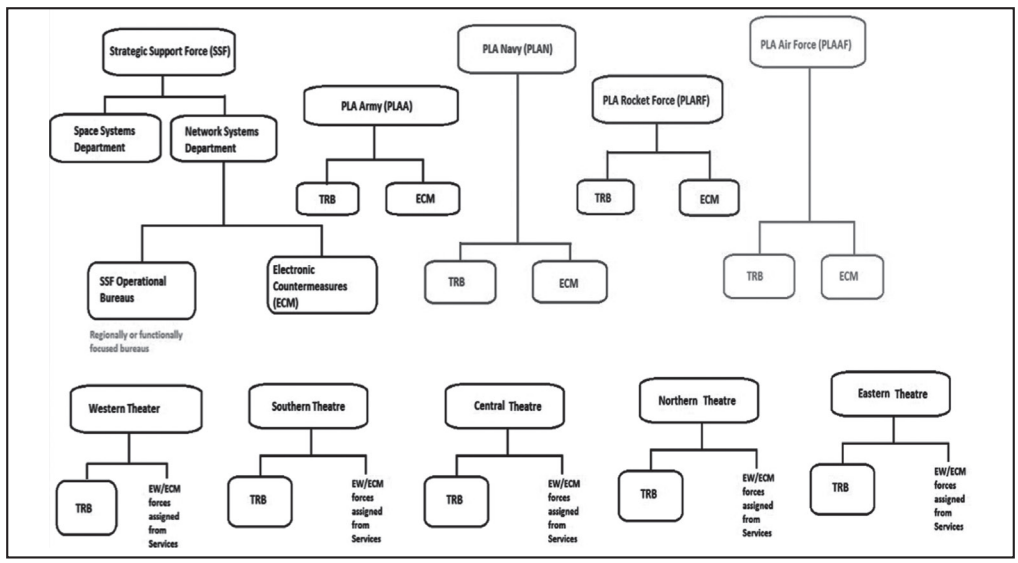
Electronic Countermeasures Units to conduct EW operations;[12] and

Technical Reconnaissance Bureaus are responsible for signals intelligence (SIGINT) collection for planning and execution of attacks and for computer network operations. These are located with each of the services.[13]

11 Bryan Clark and Timothy A. Walton, op.cit., p.19.
12 Ibid.
13 Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure", Project 2049 Institute, 11 November 2011, pp.11-13., https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (accessed on 24 December 2021).

The responsibility for developing, fielding, and operating EW capabilities differs between strategic-, operational-, and tactical- level systems as described in succeeding paragraphs.

SSF. Formed as part of the 2015 reforms to centralise space, cyber, electronic and psychological warfare missions, SSF manages and operates the PLA' s strategic-level EW capabilities. Reflecting the PLA's unified view of cyber and EW operations, the SSF is broken into two main departments: the Space Systems Department and the Network Systems Department. The SSF develops, fields, and operates its own EW units and reports directly to the Central Military Commission[14] (See Figure 2 Below).



Note: TRB = Technical Reconnaissance Bureau; ECM= electronic countermeasures. The TRBs have a service or regional focus. The SSF retains strategic EW missions and is a force provide down-echelon.

Figure 2: Organization of PLA EMSO units in SSF and Theatre Commands.

14 John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," ed. Phillip C. Saunders,National Defense University Press Center for the Study of Chinese Military A□airs and Institute for NationalStrategic Studies | National Defense University, October 2018, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf (accessed on 24 December 2021)

Operational-and Tactical-Level EW Units. These are provided to Theatre Commands by PRC military and paramilitary services. The PLA Army, PLA Air Force, PLA Navy, PLA Rocket Force, People's Armed Police, China Coast Guard, and People's Armed Forces Maritime Militia all field EW capabilities, which are generally developed by the respective services in concert with the PRC's technical bureaus and state-owned enterprises.[15]

Capabilities

PLA considers EW as a distinct set of capabilities comprising electronic reconnaissance, electronic offence, and electronic defence.

Electronic Reconnaissance. It refers to collecting and analysing enemy signals, including communication, radar, EO/IR, and hydroacoustic emissions. Electronic reconnaissance capabilities exploit the PLA's understanding of local conditions and terrain to assess the structure of an enemy battle network using widely distributed passive and multi-static RF or EO/IR sensors. For example, PLA Navy DWL-001 and YLC-29 passive detection and targeting systems are used to help protect naval infrastructure and platforms in Hainan, PRC.[16]

Electronic Offence. It addresses both electronic and physical attacks against communications, radar, EO/IR sensors, and sonars. To attack enemy battle networks, the PLA has fielded a comprehensive portfolio of EW capabilities to include:

(a) Kinetic weapons such as anti-radiation missiles;
(b) Electric weapons such as high-power microwave (HPM);
(c) Lasers; and
(d) Suppressive and Deceptive Jamming.[17]

Electronic Defence. It focuses on preventing PLA signals from being discovered, identified, or suppressed by an enemy. The range of actions captured under electronic defence is broad, which includes:

15 Bryan Clark and Timothy A. Walton, op.cit., p.20.
16 Ibid., pp. 20-21.
17 Ibid.

(a) Use of systems like multispectral decoys;

(b) Camouflage to protect radar, EO/IR, and hydroacoustic signatures;

(c) Electronic counter-countermeasures to protect PLA communications and radar from jamming or detection;

(d) Tactics to prevent destruction of Electromagnetic Spectrum systems, such as building fortifications or exploiting terrain and surface features; and

(e) Hardening against HPM effects.[18]

The PLA has been training to operate in complex electromagnetic environments since 2006, when Hu Jintao, then chairman of the Central Military Commission, emphasised in his speech about the importance of electromagnetic dominance. Mastering the electromagnetic spectrum has been a requirement in most military exercises since then. All PLA major exercises feature significant EW components, including the use of dedicated and capable adversary EW forces. The PLA has also enhanced the posture of its EW units by deploying more systems beyond the PRC mainland - on vessels and fortifications in the South China Sea; on vessels in the East China Sea, and at the PLA's base in Djibouti.[19]

Priorities for Future Developments

Employing Artificial Intelligence. As part of the 13th Five-Year Plan (2016–2020), the PLA prioritised investment and critical reforms in the areas of "innovative electronics and software," including those relevant to EW. The PLA intends to improve its cyber and EW *capabilities by using artificial intelligence to assist adversary network vulnerability analysis, emitter identification, and electromagnetic spectrum management.*[20]

Military-Civil Fusion. Reform of EW industrial base is PLA's another

18 Ibid.

19 Ibid,. p.23.

20 Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020," op.cit., pp. 141-142.

priority for which the PRC adopted a strategy of military-civil fusion in 2015. Aim of military-civil fusion is to "systematically reorganise the Chinese science and technology enterprise for ensuring that new innovations simultaneously advance economic and military development." The PRC is supporting a large pool of technical talent and generating internal research and development funding to innovate, and achieve manufacturing economies of scale, all with carryover effects for the PRC's defense sector. Military-civil fusion also aims to leverage theft of foreign technology and international partnerships, in some cases by using front companies or obscuring the military end user from foreign partners.[21] ***Digital Hail Information Technology*** is one such PRC company that benefited from military-civil integration. During the past five years, Digital Hail has rapidly increased its work for the PLA on cutting-edge decision support tools such as the Electromagnetic Spectrum visualisation and planning system.[22]

CHALLENGES FOR INDIA

While adequate information about China's electromagnetic spectrum dominance strategy, its operational concepts, the related organisation, force structure and general capabilities is available either through Western literature or is deliberately published by Chinese official think-tanks as part of their deterrence strategy. Similarly, there is publicly known information about PLA combat systems such as ships, aircraft, and missiles but comparatively little is known about PLA EW equipment, especially ground-based EW systems. EW equipment only rarely appears in Chinese military parades and even then is only identified generically as "a new type of radar jamming vehicle" or "a new type of communication jamming vehicle."[23] Even the information provided about their EW

21 Bryan Clark and Timothy A. Walton, op.cit., p.23.

22 Jiang Jie, "Private companies hope for relaxed requirements in military-civilian integration", People's Daily Online, 13 April 2017, http://en.people.cn/n3/2017/0413/c90000-9202603.html (accessed on 26 December 2021)

23 J Michael Dahm, "Electronic Warfare and Signals Intelligence", John Hopkins Applied Physics Laboratory, South China Sea Military Capability Series, August 2020, p.6., https://www.jhuapl.edu/Content/documents/EWandSIGINT.pdf (accessed on 26 December 2021)

equipment at exhibitions is also of academic value only. For example, the state-owned China Electronics Technology Group Corporation (CETC) displayed a graphic at a recent arms exhibition showing the notional composition of ground-based electronic countermeasures units. While this graphic is generic, it depicts an EW command and control vehicle communicating with EW reconnaissance stations that feed information to individual specialised jammers, each covering a different part of the electromagnetic spectrum. Individual jammers are shown creating interference in the millimetre-wave band, X/Ku-band, C-band, L-band, and S-band in support of an air defense mission.[24]

Further, *'The Winning Mechanisms of Electronic Countermeasures',* which provides an insight in to the PLA's EW top brass thinking on how to establish electromagnetic dominance in a future conflict, lacks specific details - especially in regards to examples from the PLA's own experience and its contents are quite abstract. Firstly, most examples cited come from wars conducted by the U.S. military and secondly, the writing is sometimes repetitive, and at times even contradictory (such as the inconsistency regarding whether or not to strike civilian electronic infrastructure).[25]

Thus India is faced with multiple challenges in the field of electromagnetic spectrum against China:-

- **Organisational.** Integrating Cyber and EW functions, China has developed fully functional and networked organisations - with SSF to handle PLA' s strategic-level EW capabilities and separate operational and tactical-level units provided to theatre commands and individual services. India is still in a nascent stage with a Defence Cyber Agency evolved recently and its joint and integrated functioning with other services is yet to be known publicly.
- **Conceptual.** China has a well-defined strategy for achieving superiority or dominance in electromagnetic spectrum and its

24 Ibid., pp.6-7.
25 Zi Yang, op.cit.

operational concepts for war fighting in this domain are derived from it. India has yet to declare its doctrine for integrated and joint application of Cyber and EW capabilities.

- **Operational-cum-Technological.** With a view to operate unhindered in its own Electromagnetic Spectrum and prevent the enemy from controlling it or interfering into our own operations, the complete layout and technological capabilities of China's Cyber and EW systems should be known, which is not the case. It is extremely challenging because of various difficulties:-

  - The PLA jamming or ELINT detection threat is not from a single EW system but from the sum total of different EW systems: ground-based; airborne; or ship-based.

  - A relatively new Y-9JB aircraft is considered as most capable and is known to carry KG-600 or KG-800 jamming pods for electronic attack/ standoff jamming missions.[26]

  - All large Chinese unmanned aerial vehicles (UAVs) are also capable of carrying jamming pods or signals intelligence packages. The Chinese Wing Loong II UAV, similar to the US Predator UAV, is reportedly equipped with an "integrated electronic warfare mission system".[27]

  - Determining specific EW capabilities are inherently challenging as such capabilities are located in a single, relatively small antenna that is difficult to discern from commercial satellite imagery.

  - EW capabilities that cover large parts of the frequency spectrum is consistent with the PLA's design approach to other complex systems-of-systems such as communications and radar capabilities.

  - PLA adopts frequency diversity that allows it access to the

26 J Michael Dahm, op.cit., pp. 15-16.
27 Ibid., p.16.

electromagnetic spectrum in the face of threats from enemy jamming or destruction.

- Fixed signals intelligence facilities include sites that may be used to monitor, locate, or jam foreign SATCOM signals and an High-Frequency Direction Finding (HFDF) site that enhances the PLA's regional HF triangulation capabilities.[28]
- Electronic jamming may be synchronised with other ELINT detection and kinetic attack.
- China's expertise in cyber espionage and cyber attacks is well-known and it can breakthrough any cyber network defences. With China's highly-trained cyber warriors and further botnets spread in different corners of the globe, it will be extremely difficult to locate and attribute the origin of attacks.

- **Training.** The PLA has been training to operate in complex electromagnetic environments since 2006 and mastering the electromagnetic spectrum has been a requirement in most military exercises since then. Indian Army and the Air Force have been training and conducting joint EW exercises but the scope has to be enlarged to include all services and joint agencies/ commands in different theatre commands as soon as these are established.

In India, cyber initiatives are mainly concentrating on countering threats to critical national infrastructure, government agencies and financial institutions like banks and insurance companies, as also corporate entities. The National Technical Research Organisation (NTRO) has been entrusted with the responsibility for cyber security in the country and it does not come under any ministry but operates directly under the Prime Minister's Office.[29] With Defence Cyber and Space Agencies having been

28 J Michael Dahm, op.cit., p.18.

29 Maj Gen P K Mallick, VSM (Retd), "The PLA's Developing Cyber Warfare Capabilities and India's Options", Strategic Study India,Occasional Paper No – 02/2021, https://indianstrategicknowledgeonline.com/web/PLA%20CYBER%20CAPABILITIES%20AND%20ITS%20ADAPTION%20IN%20WARFARE.pdf(accessed on 26 December 2021)

formed, EW and Cyber Warfare must be treated together as is being done by the United States and China. India needs to have a comprehensive war fighting strategy for electromagnetic spectrum encompassing ELINT/ SIGINT, electronic offence and electronic defence. India may not have enough resources to determine the complete electronic order of battle (ORBAT) of the Chinese PLA, for which it may have to seek the help of the United States that has enormous reconnaissance and surveillance capabilities. Electromagnetic hardening of own equipment will allow the armed forces to function unhindered in hostile electromagnetic environment but firstly it is a very costly affair and secondly a smart enemy will always find means to penetrate the defences. Thus India should have its own offensive electromagnetic spectrum strategy and develop means to implement it. Countering complex Chinese EW networks will require an integrated system-of-systems approach that integrates kinetic and non- kinetic means to deny PLA designs to gain and maintain battle space information advantage.

While developing own state-of-the-art EW systems from ab-initio will take time, India can always look up to its time-tested friend Russia for such equipment as it got S-400 from the latter. Russian EW forces employ Murmansk-BN, RB-109 A and Leer-3 EW systems:-

- The **Murmansk-BN** is an electronic surveillance and attack complex capable of monitoring and jamming communications and sensors in the high frequency/very high frequency/ultra-high frequency (HF/VHF/UHF) bands. With a reported range of up to 5,000 kilometers, the system is capable of disrupting satellite or airborne communications and sensors.[30]

- The **RB-109A Bylina** (mounted on five trucks) conducts command and control (C2) of EW systems at the brigade level. It is reported to have an AI-enabled C2 algorithm that facilitates automated decision-making and commanding the execution of electronic

30 Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", RKK-ICDS, Public of Estonia, September 2017, p.15., https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf (accessed on 26 December 2021)

attack by other units while minimising potential adverse effects on friendly communications and radar systems.[31]

- The **Leer-3** consists of a mobile vehicle command post that controls three Orlan-10 UAVs. The UAVs are equipped with RF receivers and transmitters capable of jamming mobile phones and some radios and transmitting SMS messages to mobile phones. The ability to transmit SMS messages provides an opportunity to target an adversary's information-psychological sphere by deceiving or demoralising adversary forces and civilian populations.[32]

Conclusion

In the Indian academic circle it is considered as a conventional wisdom to state that China is far superior to India in the field of EW and cyber warfare. It is for the simple reason that India does not have an officially stated doctrine for integrating these two aspects of warfare. Further, the individual services have been practising EW and coordinating with each other since almost three decades but cyber threat being of recent origin, all Indian initiatives are related to protecting the country against cyber-attacks/ espionage. Cyber offensive may not form part of India's official stance because of ethical and legal reasons. However, electromagnetic spectrum being a common ground for cyber and EW both, one cannot segregate the two. Hence India should enunciate its own strategy to dominate the electromagnetic spectrum, using both offence and defence.

More importantly, as the Chinese military continues to modernise, its reliance on electromagnetic spectrum for military operations will grow manifold and therefore Chinese PLA's vulnerabilities will increase in that proportion. Therefore, India should develop asymmetric options to counter Chinese vulnerabilities in the electromagnetic spectrum. Further, PLA's strategists rely on electromagnetic deterrence and

31 Ibid. pp.15-16.
32 Bryan Clark and Timothy A. Walton, op.cit., p.29.

deception with the belief that a weak enemy commander will be afraid and retreat, thus accomplishing the goal of winning without fighting. Indian valour at Galwan Valley has proven that Indian commanders are capable of replying them in the same coin. India should have its own electromagnetic deterrence strategy and demonstrate it too.

***Brig (Dr) R K Bhutani (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi.

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

US RESPONSE TO ELECTROMAGNETIC SPECTRUM THREATS AND CHALLENGES: LESSONS FOR INDIA

Air Cmde T Chand (Retd)*

Abstract

EMS is an important enabler of all war fighting domains today. The growing impact of the Cyber and Space domains has put the EMS at the Centre stage. US, Russia and China have well developed EMS operation capability. US which was considered a leader in the EMS capability has of late assessed that its near peers adversaries Russia and China are closing in fast and might surpass its capabilities if timely action is not taken. China with its EMS dominance strategy called The 'Winning Mechanisms of Electronic Countermeasures' and creation of its SSF is of grave concern to the US and others.

Therefore, the US has initiated a slew of measures to ensure its leadership and dominance of the EMS. Its new EMS Superiority Strategy 2020 has addressed most of the concerns. The loopholes in implementation of the earlier strategies have been plugged after the GAO study and Report.

China's EMS capabilities are of special concerns to India especially in view of the unresolved borders and China-Pakistan nexus. India has reportedly a well-structured EW capability. Many measures initiated by the US for maintaining EMS superiority are of relevance for India too.

There is perhaps a need for India to adopt a well thought out strategy for the country as a whole. Necessary review of the existing capabilities is needed for overcoming suboptimal preparation.

US pioneered the fundamental research for understanding and exploitation of the Electromagnetic Spectrum (EMS), right from early days. World War II saw the major applications of the EMS by the armed forces and also adoption of measures to deny its use by the adversaries. Since World War II, holding an edge in the EMS has provided the US distinct military and economic advantages. Nevertheless, as technology has become diffused during the Fourth Industrial Revolution, US ability to maintain the advantage within this spectrum has diminished as peers gain capability. At present, the US and its allies are alarmed by this situation. In certain areas, if the US is unable to strengthen EMS capabilities, there is a likelihood of adversaries achieving parity or even dominance of the spectrum in a matter of years[1]. US-Soviet Union competition during cold war took the EMS exploitation to a much higher level. China also continued to develop its capabilities and have of late shown its prowess to the rest of the world in many ways. The integration of all its EMS related capabilities in the form of SSF has given a force multiplication effect to the Chinese armed forces. Alarmed by the Chinese capabilities, US has redoubled its efforts to maintain its superiority and has adopted yet another new Electromagnetic Spectrum Superiority Strategy 2020 to achieve its goals.

China's capabilities are a major cause of concern for India as well. Chinese activities and deployment along India's northern borders has raised alarm on many occasions. While Indian armed forces have evolved their EMS capability and denial measures, there are many lessons which could be learnt from the US response to the EMS threats and challenges faced by its armed forces.

1 Ernest "Doc" Gunasekara-Rockwell, "Electromagnetic Defense Task Force, 2018 Report", LEMAY PAPERS, https://www.academia.edu/37985797/Electromagnetic_Defense_Task_Force_2018_Report, 13 December 2021.

Spectrum Warfare is the control, development, and use of advanced Electromagnetic (EM) spectrum technologies, both offensive and defensive, for strategic advantage and mission success in military conflicts and intelligence gathering[2]. All computer networks, guidance systems, sensors, electronic jammers, radios, phones, and radars are a part of electromagnetic environment, often through wireless routers and satellites, it has become increasingly essential for countries to have both advanced technologies and a well-considered approach for attaining Spectrum Warfare viability. Adoption and use of these EMS technologies in the field can vary but the need for advanced Spectrum Warfare capabilities has escalated across air, sea, ground, and C4ISR platforms as commercial telecom technologies have improved, and become less costly worldwide. While Spectrum Warfare threats have grown, the research and development of new EM technologies capable of countering those threats has been limited to relatively few defence electronics firms. These firms specialise in developing and producing next generation Electronic Warfare (EW) capabilities, including Electronic Support (ES), Electronic Protection (EP), and Electronic Attack (EA) technologies for the Defense and intelligence agencies.

US: EMS Threats and Challenges

The US DOD defines Electromagnetic Warfare as 'Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy'. Electromagnetic Warfare was previously called Electronic Warfare (EW) as described in JP 3-85. The Electromagnetic Battle Management is defined as the dynamic monitoring, assessing, planning, and directing of operations in the electromagnetic spectrum in support of the commander's concept of operation which is also called EMBM (JP 3-85)[3].

2 BAE Systems. https://www.baesystems.com/en-us/definition/what-is-spectrum-warfare, 08 December 2021.

3 DoD Electromagnetic Spectrum Superiority Strategy 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF, 08 December 2021.

Traditional EMS threats, such as nuclear-EMP and geomagnetic storms, have regained prominence once again. In 2018, the Electromagnetic Defense Task Force (EDTF) of the US DOD, published four key findings: namely; EMP and Geomagnetic Disturbance (GMD) are significant and continuing threats to the military and civil society; Risks include but are not limited to nuclear power station resilience, military installation resilience, and exercise realism and training (education); Emerging 5G technologies and the design of regional and continental networks can present strategic threats; Directed energy and high-powered microwave systems can pose threats to human biology and hardware dependent on electronics noting that EMS management is struggling to maintain pace with rapid technical evolutions within the spectrum.

The task force evaluated the functioning of the societies, it became apparent that along with cyber, the most unique and effective way to affect large segments of a modern nation without a retaliatory attack was to use the EMS to disrupt life sustaining elements such as water, food, sanitation, communications, transportation, and especially the electric power infrastructure upon which all such systems depend. During the war gaming, the task force also found that certain EMS phenomena may potentially bypass traditional strategic deterrence and present challenges to the health and economies of states[4].

China reportedly, possesses 'Super EMP Devices' that could cause a prolonged blackout resulting in large number of deaths. US is thus vulnerable to an Electromagnetic Pulse (EMP) attack from adversaries such as China, and urgent action is needed to invest in defending the country from it[5]. Peter Vincent Pry, the executive director of the US Task Force on National and Homeland Security, stated during a virtual forum hosted by the Universal Peace Federation on 23 November 2021, "That China poses a real threat of possibly being able to gain advantage with an EMP attack, which would be

4 ibid

5 Michael Lee, "US vulnerable to Chinese electromagnetic attack, experts say", Fox News 24 November 2021, https://www.foxnews.com/us/us-vulnerable-to-chinese-electromagnetic-attack-experts-say, 12 December 2021/

used in conjunction with cyberattacks and physical sabotage, and non-nuclear EMP[6]." The U.S. electric grid and other infrastructures such as communications and transportation systems and water and sewer services, could all be crippled by such an attack, experts like Pry warn. In addition to possession of super EMP Devices, China recently tested a new hypersonic glide vehicle reportedly could deploy the EMP and cause a prolonged blackout that would disable infrastructure and disrupt the military's communications[7].

According to studies by the Department of Defense (DOD)[8], near-peer adversaries China and Russia are aware of the importance of the Electromagnetic Spectrum (EMS) and have taken steps to improve their capabilities to threaten US ability to use and control the EMS. China is taking steps to enhance its capabilities to use the EMS through strategic, organisational, and training methods. Russian electromagnetic warfare forces, have also demonstrated their effectiveness against US and other militaries. Studies undertaken by the US DOD have also highlighted internal challenges that may affect the department's ability to ensure superiority, or operational control, in the EMS. These include issues related to: Governance and organization, Technology acquisition and development, EMS operational concepts, Spectrum management, and Staffing and Training[9]. Almost every aspect of modern society is facilitated by the electromagnetic spectrum. The U.S. military "faces almost impossible odds of winning future competitions if the electromagnetic spectrum domain is insufficiently dominated by western interests," warned the U.S. Air Force Electromagnetic Defense Task Force in its 2019 study report[10].

US Response

6 ibid
7 ibid
8 "DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority", GAO Report to the Committee on Armed Services, House of Representatives, December 2020. https://www.gao.gov/assets/gao-21-64.pdf, 16 December 2021.
9 ibid
10 Marcus Clay, "To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power", War on the Rocks, 22 January 2022. https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/. 24 December 2021.

Defence Secretary Lloyd Austin approved the implementation plan for the DOD's 2020 Electromagnetic Spectrum Superiority Strategy on 15 July 2021 which has five strategic goals, which are: Develop superior EMS capabilities; Evolve to an agile, and fully integrated, EMS infrastructure; Pursue total force readiness in the EMS; Secure enduring partnerships for EMS advantage; and Establish effective EMS governance. Through the Department's deliberate and cooperative pursuit of these goals, Defence Forces will possess the resources, capabilities, and interoperability necessary for decisive military overmatch[11]. The authorized plan is an important step toward modernizing EMS operations that will enable almost every aspect of modern warfare, including the DOD's Joint Warfighting Concept and All Domain Operations.[12] This announcement came after the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems (CITIS) added to its markup of the fiscal year 2022 National Defense Authorization Act a thirty-first mission area called "spectrum operations" and a statutory requirement for the Pentagon to ensure necessary appointments for the 2020 strategy's implementation[13].

Currently, US Strategic Command leads EMS operational advocacy, while the EMSO-CFT (Electromagnetic Spectrum Operations Cross-Functional Team) works to achieve the 2020 strategy's overall goals, which include: Develop Superior EMS Capabilities; Evolve to an Agile, Fully Integrated EMS Infrastructure; Pursue Total Force EMS Readiness; Secure Enduring Partnerships for EMS Advantage; and Establish Effective EMS Governance[14]. The US DOD is also modernizing, it's Defence Information Systems Agency (DISA). The DISA is actively working for development of a new Joint Electromagnetic Battle Management System[15]. Earlier, Former President Donald Trump

11 "DoD Electromagnetic Spectrum Superiority Strategy 2020", https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF, 14 December 2021.

12 Brad D. Williams, "Secretary Austin Approves Spectrum Superiority Strategy Implementation Plan, 05 August 2021", All Domains, https://breakingdefense.com/2021/08/secretary-austin-approves-spectrum-superiority-strategy-implementation-plan/, 08 December 2021.

13 ibid

14 ibid

15 ibid

took steps in 2019 to begin addressing the EMP challenge, by signing an executive order that directed government-wide coordination to defend against an EMP attack. US DOD is also increasing cooperation with the Japan in space, cyberspace, the EMS, and AI as well as cross-domain operations[16] besides cooperating actively with Taiwan, Vietnam, Singapore and India.

Recently, US GAO (Government Accountability Office) made five recommendations, advising that DOD should identify processes and procedures, reform governance structures, assign leadership for strategy implementation, and develop oversight processes. DOD concurred with the first two recommendations and partially concurred with the last three recommendations. In response to these three latter recommendations, DOD stated that it will take action once the department has developed and the Secretary of Defense has reviewed organizational reform recommendations[17].

Earlier, US national and international policies focused on managing spectrum to stimulate economic growth through commercial applications. Federal policymakers are making a large amount of spectrum available for commerce across many radiofrequency ranges in large contiguous spectrum blocks for fifth-generation (5G) and future broadband technologies. At the same time, DOD's requirements for spectrum access continue to grow to test, train with, and employ emerging national security capabilities. The DOD recognizes the importance of the EMS especially for reaping the benefits of the 5G technology for security agencies as well. The DOD believes that the traditional model of static frequency allocation is not sufficient, and a new model is needed to address the growing demand for access to an increasingly congested and constrained EMS[18].

16 David Vergun, "U.S. Bolsters Indo-Pacific Alliances in Face of Threats" 05 December 2019, DoD News, https://www.defense.gov/News/News-Stories/Article/Article/2032957/us-bolsters-indo-pacific-alliances-in-face-of-threats/, 12 December 2021.

17 "DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority", GAO Report to the Committee on Armed Services, House of Representatives, December 2020. https://www.gao.gov/assets/gao-21-64.pdf, 16 December 2021.

18 "US DOD Electromagnetic Spectrum Superiority Strategy 2020", https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF, 20 December

While, EMS maneuver focuses on gaining advantage over adversaries, spectrum sharing focuses on mitigating interference through agreement. Increased spectrum sharing remains a critical priority for the DOD to meet the growing demands for spectrum access from both commerce and Defence Forces. This sharing should include implementation of dynamic and bidirectional sharing for facilitating access to commercial spectrum while addressing the cybersecurity risk of an information sharing infrastructure outside of the DOD Information Enterprise. It also envisages pursuing machine to-machine technologies that enable cognitive cohabitation in the spectrum. International and domestic spectrum policy and regulations are expected to evolve to enable spectrum sharing to keep pace with rapidly changing technologies and increased mission requirements[19].

Lessons for India

Freedom of action in the EMS, at the time and place, of our choosing, is a prerequisite to the successful conduct of operations in all domains. EMS environment in India is also contested where enemy activities detect, disrupt, exploit, degrade, deny, deceive, or destroy EMS capabilities for the purpose of military advantage. It is congested as military and civilian EMS-dependent systems continue to be added to the spectrum and the extent of unintentional interference keeps on increasing. The EMS is also constrained by domestic and international regulations which causes the magnitude of spectrum available for military use to decrease.

Both India and the US have a common adversary, China. EMS Threats and Challenges posed by China to the US are also applicable for India. India shares a long 3488 km long unresolved border with China. Therefore EMS threats posed by China become even more serious for India. Close defence cooperation between China and Pakistan and extent of interoperability developed by their defence forces revealed through their joint exercises also poses a serious EMS

2021.

19 ibid

threat from China assisted Pakistan as well. China has adopted an EMS dominance strategy called The 'Winning Mechanisms of Electronic Countermeasures' which expresses in detail the PLA EW ideas and stratagems on achieving electromagnetic dominance, which is defined as "guaranteeing the information activity needs of friendly forces in the EMS, while rendering the enemy's information activities in the EMS ineffective[20]." The strategy specifically emphasizes the use of offensive electronic measures to achieve such goals. The PLA's strategy is divided into four principles and stages: First, "gather one's strengths and advantages to achieve a superior starting position; Second, pursue multi-level integration; Three, employ precise release of energy; and four, demonstrate effects in multiple areas". The fourth and final stage is the most important one in securing victory, and it is the focus for the majority of EMS stratagems[21]. Chinese strategists consider national and military decision-makers as key targets for strikes under its electronic warfare operations and other targets include "national information infrastructure, strategic early warning systems, the military information system, and communications systems within the adversary's national financial, energy, and transportation systems[22]."

US response to Chinese EMS threats and challenges have many lessons for India too. There is perhaps an urgent need to recognise EMS threat as a national threat and prepare a whole of government response to it. EMS challenges go well beyond the military battlespace. The EMS is needed for commercial mobile broadband technologies for facilitating economic growth and prosperity, which also restricts the spectrum available for the Indian Defence Forces. It is worth remembering that EMS exploitation provide capability, capacity, and potentially persistent

20 Zi Yang, "PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of The Winning Mechanisms of Electronic Countermeasures." The Jamestown Foundation China Brief, Volume: 19 Issue: 3, 01 February 2019. https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/. 26 December 2021.

21 ibid

22 Marcus Clay, "To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power", War on the Rocks, 22 January 2022. https://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/. 26 December 2021.

access to targets at the speed of light, where many other capabilities require extended time, resources, and movement of forces to employ. A study akin to the US Electromagnetic Defence Task Force (EDTF) would help India to understand this dormant but all pervading EMS threat in its entirety and enable the MoD to prepare a comprehensive response quite akin to the US 'DOD Electromagnetic Spectrum Superiority Strategy 2020'23. There is perhaps a need for transitioning from the traditional consideration of Electromagnetic Warfare (EW) as separable from spectrum management to a unified treatment of these activities as Electromagnetic Spectrum Operations (EMSO) as planned by the US. The purpose of the comprehensive MoD response should be to align MoD EMS policies with the objectives of the National Security Strategy (NSS), National Defense Strategy (NDS), and national economic and technology policy goals, in whatever forms they are existing.

EMS superiority brings important advantages to any cost imposition strategy. By developing innovative asymmetric EMS capabilities, MoD can protect expensive friendly capabilities from disruption or attrition, while simultaneously denying or degrading the effectiveness of adversaries' sophisticated systems. Because many EMS capabilities are employed, not expended, concerns about cost may be reduced, which in turn affords decision makers more sustainable options. This is especially significant as India and its adversaries all increasing investment in space-based capabilities and dependencies. India must exploit adversaries' EMS vulnerabilities through advanced EW to offset their capacity.

India's policymakers are making a large amount of spectrum available for commerce across many radiofrequency ranges for 5G and future broadband technologies. At the same time, MoD's requirements for spectrum access continue to grow. The traditional model of static frequency allocation is not sufficient, and a new model incorporating spectrum sharing is needed to address the growing demand for access to

23 "DoD Electromagnetic Spectrum Superiority Strategy 2020", https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_Spectrum_Superiority_Strategy.PDF, 14 December 2021.

an increasingly congested and constrained EMS, in India too. Spectrum sharing offers a new model for greater freedom of action within the EMS. Spectrum sharing is the simultaneous usage of a specific frequency band in a specific geographical area and time by a number of independent entities where harmful electromagnetic interference is mitigated through agreement.

Successful engagement in the International Telecommunication Union (ITU) treaty processes, including the World Radio-communication Conference (WRC), will help to maximize India's EMS access to meet wartime and peacetime national security objectives. India should also ensure EMS exploitation in congruence with COMCASA standards for facilitating interoperability when required. This would require interoperable data sources and architectures.

EMS Superiority requires effective intelligence collection, analysis, and validation of the following key areas such as : parametric data, which encompasses all EMS sensors, communications, datalinks, radars, jammers, directed energy, electro-optics, and infrared systems; engineering data, which describes the performance, characteristics, and signature information of the associated equipment, weapons, and platforms; order of battle data; combat support data; and modeling and simulation support. Modeling and simulation fidelity must support all levels of operations, up to and including campaign modeling and support to operational war gaming. Validated intelligence data and accurate and current assessments underpin the success of EMS dependent systems.

EMS Operations or EW operations in India like most other countries tend to be very secretive and have the risk of remaining sub optimal. Therefore, a GAO like study and analysis of the Indian Defence Forces and the MoD would be in order to ensure superiority or at least parity with the fast growing capabilities of the adversaries especially China.

***Air Cmde T Chand (Retd)** is a Senior Fellow, Centre for Joint Warfare Studies (CENJOWS), New Delhi.

EMS CAPABILITY DEVELOPMENT STRATEGY FOR MILITARY DOMINANCE: INDIAN JOINT FORCES

Brig Rajeev Ohri, VSM

Abstract

The two majortechnology disruptions which have impacted militaries all over the world are ***convergence of compute and communications and high data rate communication capability from wired to wireless domain.*** *The erstwhile Combat Net radios, which were the only means of exercising Command and Control,are now getting replaced by Software Defined Radios, 4G/5G mobile communications, high bandwidth capable Satellite handsets with inbuilt information processing capability for Navigation, Decision Support and military utility applications. This has resulted in major enhancements in Mobility, precision, battlefield transparency, shared situational awareness and overall Shortening of OODA loop.*

If UAV/ drones have revolutionised warfare, then the backbone of this revolution is EMS domain. From a spectrum perspective, all flow of information takes place in the EM Spectrum, which has expanded, from HF/ VHF to the extremities of Light Waves. Therefore, denial of spectrum to adversary, control of vital Info flow, electromagnetic sovereignty and extraction of vital data and intelligence from spectrum have become synonymous with national power. In other words, spectrum has become a domain of warfare as is evident from organisation changes carried out

by leading armies of the world.The Electromagnetic Spectrum (EMS) aspects need to be understood from Indian defence forces context in conjunction withexisting pillars of our information philosophy.

EM Spectrum: Key aspects

Spectrum Joint Force. Spectrum has emerged as a premium and expensive resource on which not only defence forces, but our National Critical Infrastructure is also relying. The high cost of spectrum is indicative of the information potential of this resource. Protection and management of this national resource for own use and denialof this resource to adversary therefore needs a consideration from a national perspective.While Army, Navy and Air Force were raised to protect our land, sea and air domains, EM Spectrum domain requires a force, which holistically looks at protection of National Information Infrastructure including defence. Therefore,there is an urgent need to create a separate specialist force for protection, management and denial of EM Spectrum domain. Creation of PLASSF is a step taken by China, which meets this emerging requirement.

Military Civil Fusion. The uniqueness of EMS domain is that there is a large relevance in not only military but also in civil domain. It cuts across the three services and has major implications in internal security also. The technical advancements carried out by India needs to be synergised for creating EMS sovereignty. For achieving this capability, creation of an umbrella organisation which channelizes R&D, Academia, Industry and Military is imperative at National level.

Spectrum Evolution. The rapid expansion of use of spectrum has impacted counter capability requirements to be developed at a much faster pace. For full spectrum degradation capability, modern forces need capability against Communications, Radars, Mobiles, GNSS, Satellites, UAV/Drones and any other EM emission used by the adversary. In addition, development of Strategic Counter Space capability needs focus.

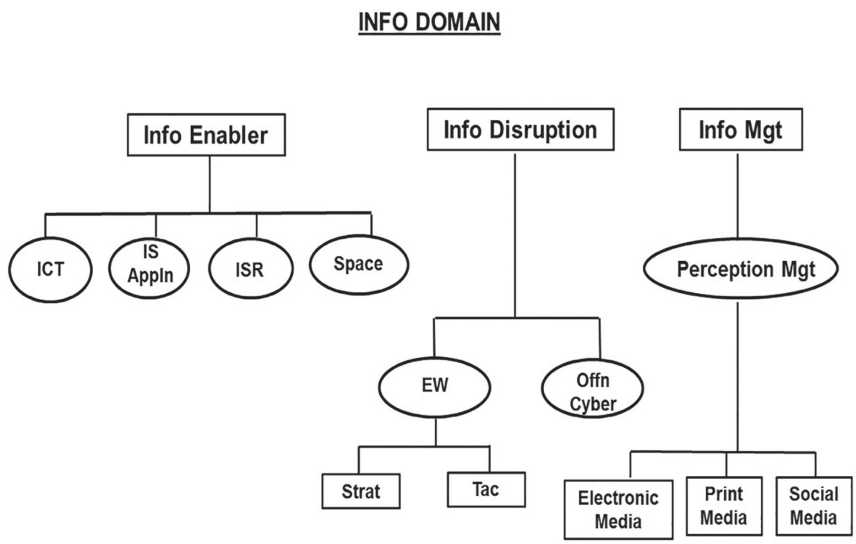
Space Domain. Leading powers have invested heavily in developing

Space capability, which enhances C4ISR, IMINT, Navigation and Synchronisation signals for networks. Space provides a global reach besides overcoming terrain and weather challenges. Developing Space degradation capability through non-attributable EMS capability will be appropriate **asymmetric solution** particularly for our Northern adversary.

Cyber EMS Convergence. The convergence of computer and communication in Software Defined Radio, mobile and emerging technologies opens up new challenges and opportunities in EMS domain. Cyber vulnerabilities in wireless domain will require new skill sets and upgradation in EMS capabilities. Answer to counter unmanned systems also lies in building converged cyber and electronic warfare capabilities.

EMS Capability Development Strategy

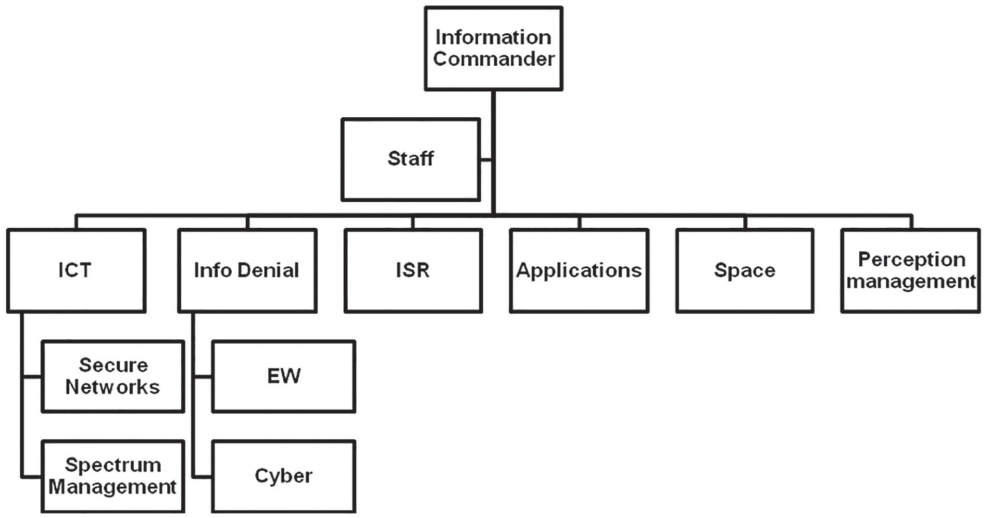
Information Domain. In Indian context, akin to the trilogy where we have concept of Creator, Preserver and Destroyer, the logical grouping and categorisation of Information domain needs to be on **Info Enabler**, **Info Disruption** and **Info Management** capability. The relevant emerging



technologies can be grouped under these three verticals as under :-

EM Spectrum Framework. In order to build a national EMS capability, it is important that there is seamless exchange of spectrum intelligence exchange between national agencies and field formations. This capability is recommended on lines of Geo Intelligence framework. The huge spectrum intelligence gathering capability of field units can be utilised by multiple agencies through this framework. This will also facilitate in removing overlaps in multiple agencies undertaking similar spectrum related tasks but also overcome the technology challenges faced by field formations.

Information Command. In the backdrop of Info and EMS emerging as key domains of national importance, it will be prudent to consider creation of an Information Command as umbrella organisation for the defence forces addressing the emerging challenges and futuristic requirements of armed forces. This command under the CDS can be the bridge between National and Defence Information agencies. This will also address the requirement of umbrella organisation for Military Civil Fusion besides creating strategic counter capabilities. All Information enablers (ICT, ISR and Space), Information disabler (EW and Cyber) and Information Management (PM) to come under this organisation for synergistic development and application of National Info Warfare. This organisation can be a separate force on lines of PLASSF with leadership having exposure and understanding of Cyber and EW issue. The organisation and structures pertaining to Info domain in Operational Joint Theatre Commands can be modelled on similar lines. This will be imperative for ensuring seamless communications and protocols for inter and intra joint theatre commands as and when these are implemented on ground. Suggested structure of Information command is as under :-



Military Information Service. Information and EMS domain requires a specialisation oriented de novo look at HR management. Application of Kinetic warfare templates on this domain will be counterproductive. In view of the limited HR availability and major capability thrust required to create and sustain evolving defence information infrastructure, there will be a requirement to induct non-combatants for effective management of the backend infrastructure and processes. This will enable combatants to handle the EMS challenges in combat zone. Creation of a non-combat **Military Information Service** under the Information Command will be a step in right direction. This will assist in not only taking on backend Information domain tasks but also bring Military Civil Fusion to a logical conclusion.

Information Security. The high capacity data transfer capability shift from wired to wireless has brought to fore the requirements of over the air security protocols. Security development and testing agencies need to find de novo solutions for this evolving dimension, else defence forces will be left behind in exploitation of wireless capacities which have huge

potential and applications in military domain. Moreover, in a joint force concept, interoperability will hinge on seamless information security.

Spectrum Management. One of the key areas which will gain importance will be smart spectrum sharing and management technologies. The demand for this premium resource from multiple agencies is going to increase by the day. Evolved solutions will facilitate a collaborative and deconflicted spectrum usage philosophy. R&D in this domain will pay rich dividends in future. EMI/EMC aspects will also gain prominence with enhanced density of emitters and intense dependence on EM radiations by multiple stake holders in combat zone. Expertise in combat zone spectrum management is a requirement which is on the anvil.

Software Defined Radio. Indigenous SDR waveforms and security solution is imperative for command, control and ISR of our joint force. Success of future information predominant conflicts will hinge on these critical technologies. It is important that jointness is achieved at development stage for smooth interoperability in joint operational scenario.

Mobile Technologies. The form factor, processing capability, data capacity and multi utility applications of mobile segment has direct relevance in military domain. Somehow, in absence of a military grade mobile technology with inbuilt Electronic Protection features, this high utility,relatively low cost technology has not been exploited for military purposes. It is time this challenge is thrown open to industry to make this technology available to military for C4ISR in a contested EM space in the form required. This will be a good alternative to SDR technology since, infrastructure for creating military mobile in Indian context with non-expansionist ideology is relatively easy to implement.

Decoupling Dependence on China. It is important that industries in ESM domain decouple their dependency on China. Recent efforts towards indigenisation and creation of fab manufacturing facilities are steps in right direction. However, our hardware manufacturing has to

quickly match up to the emerging large scale EMS requirements, which are increasing by the day. .

Training Transformation. In order to leap frog in EMS domain, there will be requirement of training transformation. While the leadership has to adapt to hybrid approach of handling kinetic and non-kinetic domain, the execution has to adopt a specialisation approach. Multinational collaboration and cooperation will be key for a faster transition. Collaboration based on core strength, infrastructure sharing, common training protocols need consideration.

Conclusion

The evolving global conflict scenario indicates a clear shift from pure kinetic to hybrid warfare where info and EMS has gained importance. Since this domain is common to not only the three services, but affects National Information Infrastructure it is important that EMS domain be viewed from that perspective. Nation states with ability to synergise all stakeholders of this domain have better probability of success in dominating EMS space.

The solution space for EMS dominant conflict lies in finding indigenous, simple workable solutions. The ever evolving technology poses challenges of fast obsolescence and high cost. Tendency to run after every new technology needs to be curbed. It is proven that only robust and tested EMS solutions withstand the rigours of combat communications. Therefore, development of smart indigenous EMS eco system which meets interoperability and jointness requirements is need of the hour. Organisation, structures and training need to be put in place for facilitating the same.

Brig Rajeev Ohri, VSM, a Signals Officer, is presently posted at MCTE Mhow

THE CONVERGENCE DILEMMA: CEMA OPERATIONS IN THE INFORMATION ENVIRONMENT

Lt Gen Rajeev Sabherwal, PVSM, AVSM, VSM (Retd)*

"The EMS and cyberspace as a specific information environment are fundamental to military operations, so that we must treat it on a par with the traditional domains of land, sea, air, and space. In fact, future conflicts will not be won simply by using the EMS and cyberspace, they will be won within the EMS and cyberspace."

Former Chief of Naval Operations, US Navy,
Admiral Jonathan Greenert

Abstract

In the Information Age, technology has brought about a convergence within the Information Environment, particularly Electromagnetic Warfare and Cyberspace Operations that present an opportunity for our Armed Forces to integrate capabilities to enhance operational effectiveness and to ensure effects are coordinated across the entire Information Environment to gain an advantage and achieve operational success. The capabilities in the Information Environment that lend themselves to be converged are the ones which actively utilise the Electro Magnetic Spectrum for their activities which are called Cyber Electro Magnetic Activities (CEMA). CEMA today is comprised of Cyberspace Operations

(CO), Electromagnetic Warfare (EW), SIGINT, Spectrum Management Operations (SMO) and Communication Operations.

As the Indian Armed Forces move towards a joint all-domain command and control set up, steps should be taken to address the electromagnetic challenges posed by our adversaries especially China. The Indian military must adapt and adjust; it cannot afford to remain wedded to current organizational structures or equipment that fought the last war.

Introduction

In future military operations, Indian Armed Forces will need to adapt to an extremely complex operating environment and a vast number of operational variables, requiring the use of a range of weapon systems to produce both kinetic and non-kinetic effects. Therefore, besides the physical operating domains (i.e. land, air, maritime and space), the ability to achieve dominance in the nonphysical/ virtual domains (Cyberspace, Electromagnetic Environment (EME), Information Environment) will be decisive for achieving both military and non-military objectives.

Since the inception of warfare, the aim of every conflict has been to impose own will over the adversary. Traditionally, all wars were fought on the physical dimensions or domains of land, air and sea. Consequent to the launch of 'Sputnik' by the USSR in 1957 and Space emerging as a new zone of competition amongst the space faring nations, the Space Domain too was incorporated as one of the physical domains of warfare. Emergence of Information Age in the 1980s, saw the advent of 'Information' as one of the elements of National Power along with Diplomatic, Information, Military and Economic Domain being termed as one of the domains of warfighting where warfare could be waged. In 2010, some nations started terming Cyber as the fifth domain of warfare[1]. Lately, some books and publications have also termed

1 https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain The Economist accessed

Electromagnetic Spectrum Domain as worthy and logical contender to the list of warfighting domains[2].

Today, our military is neither at peace nor at war, we operate in a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict. In this Continuum, Cyberspace and Electro Magnetic Spectrum (EMS) play a significant and pivotal role in waging of Multi Domain Operations by our Joint Forces. It would therefore, be prudent to get a better understanding of the operating environment and information environment to comprehend how cyberspace and EMS domains fit into the same.

Operating Environment (OE). Today's warfare is increasingly inclined towards multi domain operations which includes Hybrid, Grey Zone, Contact, Non-Contact warfare where the Operating Environment consists of the following domains of war fighting:-

(a) **Physical –** Land, Air, Sea and Space.

(b) **Virtual –** Cyber, Electro Magnetic Spectrum (EMS) and Information.

(c) **Human –** Social and Cognitive.

Information Environment (IE). The information environment is broadly defined as the aggregate of individuals, organizations and systems that collect, process, disseminate, or act on information. It is a virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems. The Information Environment has three interrelated dimensions:-

(a) Physical dimension.

(b) Informational dimension.

(c) Cognitive dimension.

on 12 Jan 2022.

2 https://www.japcc.org/electromagnetic-spectrum-cross-domain/#:~:text=The%20Electromagnetic%20Spectrum%20(EMS)%20can,interact%20with%20all%20other%20domains. The Electromagnetic Spectrum: The Cross Domain accessed on 12 Jan 2022.

Cyberspace and the electromagnetic spectrum are part of the information environment. However, EW and Cyberspace Operations have always been considered independent and exclusive to each other. Whilst EW has been an important component of military operations since the advent of radio at the beginning of the 20th Century, Cyberspace Operations have gained prominence and significance of their own in the past two decades only. Being disparate disciplines, Cyber warriors operated at the bit level and Spectrum warriors operated below them targeting EMS. However, ever since the Information Age brought about the convergence of communicating and computing on discrete devices like the smart phones and SDRs, turning them into smart entities, we find the boundaries between the two fields have begun to blur. Today, both Cyberspace Operations and EW tend to dominate fields of EMS that transmits packets of information.

EW and Cyberspace Operations are today becoming analogous as their technical characteristics and operational outcomes converge. Cyber warriors can provide effects that deny or degrade spectrum and Spectrum warriors can create effects that allow for the control and exploitation of the network. However, the Indian Military continues to treat both in separate silos with separate organisations and doctrines. Traditionally, both have been part of the Information Operations campaign and exist in the Indian Army IW Doctrine 2010 as two pillars of Information Warfare along with Psychological Operations, Military Deception and Operational Security.

Differences and Overlap

Traditionally, Electromagnetic Warfare, more commonly known as Electronic Warfare (EW), is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy; the ultimate aim being to deny the opponent the advantage of and ensure friendly unimpeded access to,

the EMS. On the other hand, Cyberspace Warfare or Cyber Warfare, are operations conducted in and from computers and the networks against government and military networks in order to disrupt, destroy, or deny their use.

An analysis of the above rendering clearly indicates that both Cyberspace Operations and EW aim to perform similar operations against the adversaries. A comparison between EW and Cyber Warfare in terms of operational functions and how they are perpetrated against the adversaries, shows that each of the EW fields has a parallel operation in the arena of Cyber Warfare.

Comparison of Electronic Warfare and Cyber Warfare Functions[3]		
Operational Function	**Electronic Warfare**	**Cyberspace Operations**
Intelligence collection	**Electromagnetic Support (ES)** – recce, monitor and DF enemy transmissions to get Tech int and Op Int.	**Cyber Network Exploitation (CNE)** - operations to obtain intelligence that is resident/ transiting through an adversary's computer systems or networks.
Degrade enemy's operational capability	**Electromagnetic Attack (EA)** – Degrade adversaries' capability to exploit EMS through jamming/ deception	**Cyber Network Attack (CNA)** - operations to degrade or deceive the adversary's computer systems/ networks
Protect own operational capability from enemy's electronic interference	**Electromagnetic Protect (EP)** – Protecting own use of EMS from enemy jamming	**Cyber Network Defence (CND)** - actions to protect own computers/ networks against hostile CNA/CNE.

The convergence of EW and Cyber Warfare, is not restricted to technical aspects only, but their similarities extend operationally too, with cyberspace operations being used to provide EW effects, and vice versa. Therefore, whilst Cyberspace operations attempt to deny an adversary

3 Cyber Electro Magnetic Activities (CEMA) by Andrea Pompili; available at https://www.emsopedia.org/entries/cyber-electro-magnetic-activities-cema/; accessed on 28 Dec 2021

access to their computer networks using various techniques of CNA, it is EW that complements the same by affecting the communications between networks using EA techniques like jamming and deception.

Today's military forces use wireless computer networks to coordinate operations, use air and ground sensors to detect and locate the enemy, use radios to communicate with each other and use electronic jammers to blind enemy radars or disrupt their communications. With wireless routers or tactical radios part of almost every computer network, cyberspace and the electromagnetic spectrum now form one continuous, coherent environment. The electromagnetic spectrum and cyberspace as a specific information environment are fundamental to military operations, hence we must treat it on a par with the traditional domains of land, sea, air, and space.

In the TBA, the most identifiable convergence of EW and Cyberspace Operations occurs when we try and transmit malicious code to inject it into an adversary's network. In such operations, radios can transmit data packets on Wi-Fi networks, or monitor the transmissions even if these are not open networks. A MANET being operated by the adversary in the TBA is a perfect example of such a network where both EW and Cyber Operations can effectively complement each other.

Another primary and traditional difference between EW and Cyber Operations was how the adversary's systems were targeted to enter his networks and devices. EW targets adversary systems like a radio/ radar initially through search, and DF functions. Consequently, his systems and devices were further degraded, negated or spoofed through jamming and deception. In Cyber Operations however, traditionally malware was injected into the enemy's computer network via a USB drive, a software-based malicious code or breaching of an air gap.

Today's communication and networking systems, both civil and military, are increasingly based on communication infrastructure

which does not fully rely on static wired connectivity. Rather, they are increasingly dependent on EMS for their functioning like end point interconnectivity. These systems continue to use their computing capabilities to process data and information, manage functionalities, and run their Network Management Systems (NMS). These computing systems have hardware vulnerabilities which include DSP, FPGA, CPU, GPU and software vulnerabilities like operating systems and applications. Therefore, in the TBA, networks that make use of wireless interface and provide vulnerabilities that can be suitably exploited in order to accrue operational dividends.

Right since the Second World War, electro-magnetic attacks have been used to disrupt enemy radios and radars, but today, the access and manipulation of the EMS and/ or the data and information in it opens up innumerable additional options for exploitation. In other words, EMS today is the common operating arena for both Cyber and EW with both trying to accomplish similar tasks which results in multidiscipline effects. The cyberspace and EMS create a common operational environment that could be named as the Cyber Electromagnetic Domain. This domain is not meant to equate the terms cyberspace and electromagnetic spectrum, but rather to highlight that there is significant overlap between them and as future technologies evolve this convergence is going to increase significantly. In this domain, harmonised, coordinated and integrated information technical activities take place. These activities could be called Cyber EW or Cyber Electro Magnetic Activities (CEMA) or Cybertronics.

CEMA

CEMA can be broadly defined as all offensive, defensive and information activities that shape or exploit the electromagnetic environment and the enabling activities that support them.[4] Based on this definition CEMA

4 Ibid 3

could be used for active and/or passive operations as under:-

(a) **Active.**

(i) **Eavesdropping.** Gathering information which could be further used for exploitation both within and outside the network.

(ii) **Spoofing.** Entering a closed wireless node as a trusted source bypassing all security measures.

(iii) **Hijacking.** Entering a wireless node bypassing all security controls/ barriers to redirect the enemy data traffic and gain control of it.

(b) **Passive.**

(i) **Cyberspace Operations** Interrupt/ deny a function temporarily or permanently thus degrading the performance of the network.

(ii) **Man In the Middle (MITM) Attack.** Degrade/ modify the performance of one or more nodes by inserting/ activating a malicious code or a dedicated data bit stream.

Based on the current CEMA concept, the Cyber Electro Magnetic operations broadly consist of (but are not restricted) the following operations:-

(a) Electromagnetic Warfare.

(b) Cyberspace Operations.

(c) Spectrum Management Operations.

(d) SIGINT.

(e) Military Communications.

(f) Some countries especially in the NATO have also included 'Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR)' and Navigation Warfare (NAVWAR) under the umbrella of CEMA.

TTPs

Most of us are aware of the term 'Tactics, Techniques and Procedures' (TTPs) in Cyber Intelligence/ Cyber Crime parlance. Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks. Generally speaking, tactics are the vectors used by cybercriminals to carry out their activities, that is, the strategy in the most general terms. Techniques are the methods that will be used by the attacker to help achieve their goal, for example, phishing. Procedures, are the specific, preconfigured steps to be used by a cybercriminal in their efforts to ensure that they achieve their aims, for e.g., installing a malware file and so on.

Our definition of CEMA and the understanding of its operations clearly reveals that it can be also considered as a chain of activities that combine endpoint wireless attacks with cyber-attacks to the exposed services, with the purpose of creating an impact inside one or more selected internal sub-systems, to obtain the needed operational advantage. CEMA, therefore, fits into the concept of kill-chains i.e. the sequence of TTPs typically followed by a threat actor to execute an attack.

CEMA Operations in the Indian Context

CEMA operations can be gainfully employed by our armed forces in all theatres and at all levels. Moreover, as technology continues to evolve in this domain its activities would continue to increase. Some of the key areas where CEMA finds ready application today are discussed in the succeeding paragraphs.

Space. In the tactical arena, one operation which readily lends itself to CEMA are the space operations. Satellite systems consist primarily of a space segment and a ground segment with both transmitting data to each other through the EMS. Both Cyberspace Operations and EW can affect space operations[5]. The Space Segment consisting of the satellites and all its payloads is controlled by ground control stations through RF transmissions by radios to maintain stable orbits, manage onboard sensors and other payloads. An adversary could transmit RF data to the satellite to potentially degrade the system payloads, remote control the onboard sensors and critically hamper the mission. He could also target the ground control stations by sending malicious cyber codes so as to ultimately gain control of the satellite or to degrade critical systems onboard. Between both options, he is likely to go for the former direct route rather than via ground control stations, since satellites receive commands routinely on the RF channels. The criticality to the space domain in all its segments has led to its gaining unprecedented importance by all Armed Forces with USA launching its sixth independent Branch - Space Force in 2019, China integrating the same along with Cyber, EW and other IW functions to create SSF and for India raising of the Tri-Services Defence Space Agency.

Cellular Systems. Typical cellular systems consist of a handset communicating with the nearest cellular tower through the EMS. Whilst 1G/ 2G/ 3G systems were basically designed for voice with some data consideration, the 4G/ 5G systems are primarily designed for data and work on IP protocols. This lends the modern cellular systems vulnerable to both cyberspace and EW attacks. An adversary can send packets of data stream and launch a MITM attack or carryout eavesdropping to collect intelligence. EW jammers could also degrade the cellular network through various EA systems like jamming and deception.

5 Convergence of Cyberspace Operations and Electronic Warfare by Congressional Research Service Aug 13, 2019
https://crsreports.congress.gov/product/pdf/IF/IF11292 accessed on 08 Jan 2022.

IoT. Internet of Things is an emerging revolution where we find a shift from an internet for interconnecting end user devices to internet for connecting physical objects like sensors, shooters, or objects without requiring any human intervention. Such systems typically run on low latency, high speed and on wireless media. Most IoT devices communicate on RF transmissions like Wi-Fi and other protocols and are thus vulnerable to a host of cyber and EW threats like DEW, eavesdropping, physical attack jamming, intrusion and EMP. It is important to understand that regardless of IoT devices being connected to a closed network or to the internet, they are a target in the TBA both for cyber operations and EW.

Software Defined Radios (SDRs). In recent years, the development of radio communication technology has experienced a huge paradigm change, the emergence of Software-Defined Radio (SDR) technology in which previously hardware- based features became software-defined and users may also introduce new application waveforms on-the-fly. These new radios converge communicating, computing and routing functions into one and are thus prone to both Cyber and EW threats. The common Cyber threats could be MITM, eavesdropping, spoofing etc and the common EW attacks could range from jamming to deception. Because SDR terminals can be designed to transmit in a wide range of frequencies, the potential for disruption of a wireless network or other wireless networks in the area by creating harmful interference is very high by an SDR terminal, which has been taken over.

CEMA in an Information Environment

The importance of information came to fore in the Indian Armed Forces during Op VIJAY due to number of reasons, important ones being absence of intelligence in discerning the incursions by the adversary for months, lack of situational awareness between the Services and the interception of telephonic communication between General Musharraf and General Aziz. Recognizing the importance of information superiority

in military conflicts, number of agencies like the NIB, NTRO, CERT etc were raised which dealt with various offensive and defensive operations in the Information Environment. Operations in the information environment attempt either to limit or distort a potential adversary's access to information, thereby limiting their situational awareness and potentially altering decision making ability of the adversary. Cyberspace Operations and EW are both tools to achieve similar ends. However, the raising of Cyber organisations by the three Services and HQ IDS has led to a separation of cyberspace operations as conceptually and operationally distinct, focusing more on the use of tangible hardware and software to create effects rather than exploiting information itself to achieve the operational ends. In the early stages, most of the armies across the world followed stove piped approach to realize the structures and doctrines of Cyber and EW capabilities. But as technologies and these two domains have evolved, with commonalities running across several areas some countries like the US, UK and China have started converging all organisations of the Information Environment under one converged head of CEMA. However, such integration remains inconsistent across the countries and services.

On the contrary, there is near unanimity that the Information Environment today has several operations like Cyberspace Operations, EW, EMSO, SIGINT and Communication Networks exist within it and thus lend themselves to be controlled and commanded under one headquarter. A new unified Information Warfare Agency/ Command may be the answer to remove operational stove pipes that exist between cyberspace, EW and other elements of Information Environment. Apropos, the erstwhile raising of Defence Information Warfare Agency (DIWA) under the HQ IDS now seems to be the right step taken by us in the past. However, with Cyber gaining prominence all over the world India has Defence Information Assurance and Research Agency (DIARA) and now it is called as Defence Cyber Agency (DCyA). These

moves resulted in only one element of IW to be diligently pursued and not the integrated and synchronised efforts of all elements to come into play. Indian Army has done much better in this regard by creating a single head 'DG IW' with EW, Strategic Communications (erstwhile PI), Cyber and Psy operations clubbed under it. A de novo review to integrate all agencies under a new IW Agency/ Command is the need of the hour.

CEMA in the TBA. Several nations have put in concerted efforts to bring electronic warfare, information warfare and cyber capabilities into their tactical formations under one integrated grouping. To better support tactical commanders, these Armies (US, UK, etc) added such capabilities to Brigade Combat Teams (BCTs). In addition to providing equipment, abilities and authorities to BCTs, they also deployed CEMA teams to support the Corps and below formations.[6] India should now integrate CEMA dets with the IBG formations at Corps and below level to start with, and based on the lessons learnt raise similar CEMA organisations for the rest of the formations based on their operational needs.

Conclusion

The modern military forces today operate in both physical and non-physical environments, relying heavily on networked communication systems that work both in the cyberspace and the Electromagnetic Spectrum (EMS), thus creating an overlapped operating environment. This reliance on network connectivity makes cyberspace, space and the EMS the 'centre of gravity' for Multi-Domain Operations (MDO).

In future, Indian Armed Forces too would be waging MDO as part of the integrated theatre operations. The multi-domain approach will require not only combination, but more importantly integration of

6 Army CEMA Teams Advance Information, Electronic and Cyber Warfare by Kimberley Underwood https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare accessed on 08 Jan 2022

capabilities across different domains, which means that operations like CEMA in the cyberspace/ EMS would become serious contenders to become the primary choice of the commanders.

Whilst CEMA ensures synchronised and integrated cyber electromagnetic operations are conducted across the domains, the Indian Armed Forces have yet to fully acknowledge the convergence between cyber warfare and electronic warfare, whether doctrinally, operationally or organisationally. Our thinking about the relationship between cyber warfare and EW and other activities in the electromagnetic spectrum are, at best, evolving. This needs serious integrated thought and consideration by all Services at all levels. A formal doctrinal clarity in terms of a Joint Doctrine on CEMA would be most beneficial.

***Lt Gen Rajeev Sabherwal, PVSM, AVSM, VSM (Retd),** is a former Signal Officer-in-Chief and Commandant, Military College of Telecommunications Engineering, Mhow.

NEXT GENERATION WIRELESS TECHNOLOGIES AND ATMANIRBHARTA IN EMS MANAGEMENT

Prof Radha Krishna Ganti*

Abstract

The Electro Magnetic Spectrum (EMS) is getting congested and this is going to get worse with the advent of next generation of wireless technologies. Managing EMS and dominating its usage is critical, and this would require India to design and build its own EMS systems incorporating the latest technological advances in wireless technologies. Some of these technologies involve 6G systems, mm Wave and THz communications, AI/ ML techniques, software defined radios and quantum systems. There is enough expertise across the country to design and build these next generation EMS systems. However, a top down approach has to be taken to engage various stakeholders for achieving this goal. In this paper, we take a brief look at the emerging technologies and their impact on EMS management. We also look at the possible issues that the research organisations and companies can face while building these EMS systems and propose some possible solutions for the same.

Introduction

Electromagnetic spectrum (EMS) is an important natural resource and its access is fundamental to operating any wireless system. The usage

of EMS is changing over time and in particular depends on the nature of technology utilising the spectrum. A few decades back, wireless systems were a luxury and the spectrum usage was limited to specific applications either civilian or military. During this time, the un-impeded access to the spectrum meant that the wireless systems were not optimised and EMS management was not very critical. Currently, because of the comforts offered by wireless services, there has been an explosive growth in the usage of wireless devices. With the advent of newer technologies, wireless communications systems (Cellular, WiFi, Bluetooth, Satellite TV) have also become commoditised and the EMS is getting congested. Current technologies have been developed with the goal of optimised utilisation of spectrum and some of the newer technologies have reached fundamental limits in terms of spectral efficiency. Even with all these advancements, the demand for spectrum is so high that the quantum of spectrum that is available is diminishing and more spectrum at higher frequencies is being sought after.

Military communications have to operate in this congested space, defend against newer and smarter adversaries and provide communications to the troops in an effective manner, which is a significant challenge. Also, unlike other fields, in the area of wireless communication, we observe that the technological advances in the commercial sector happen(ed) at a much faster pace compared to the military sector. This provides an opportunity to the military to absorb and utilise these newer and efficient wireless technologies and effectively manoeuvre the congested EMS to its advantage.

In this paper we look at some emerging technologies that are going to define the wireless landscape for the next few years. We, will briefly review some key technologies like 5G/ 6G, AI/ ML in communication systems, Quantum communications, mmWave/ THz communications, Software defined radios and in particular look at how these new paradigms are going to affect EMS management. We will look at the local expertise available in the country and also look at the challenges in R&D and building EMS systems.

Technology Roadmap

Wireless communication technologies have developed at a breakneck speed in the last few decades. This has been fuelled by consumer demand, market economics and the need to be always connected to the internet. These advances, which enabled higher data rates, lower latency, better power consumption and improved spectral efficiency are a result of decades of fundamental research done in universities and research labs. In the area of wireless communication, one can confidently state that the system implementation by industry followed rigorous theoretical research (and not vice versa), the result of which is quite evident. We will now briefly look at some key technologies that are going to define the wireless landscape in this decade.

5G and 6G cellular communications

Cell phones are now an ubiquitous mode of communications for billions of people around the world. Each generation of cellular standard has a life cycle of about 10 years and generally incorporates the latest technological advances in wireless and communication theory. 4G cellular systems mark the beginning of the introduction of OFDM and MIMO technologies along with advanced error correction codes for an all data network. These technologies have been tested extensively and proved to be effective in 4G, after which these technologies have been boosted and incorporated in 5G (and will subsequently be incorporated in 6G). Some salient features of these technologies are:

- The BW of operation in 5G has increased to 100 MHz in the sub 6 GHz bands.
- Millimetre bands (26 GHz and 28 GHz) are supported in 5G, and can support 400 MHz of bandwidth in these bands.
- 5G uses LDPC and Polar codes as forward error correction codes, the best FEC that is known till date.
- 5G standard can support upwards of 64 antennas (Massive

MIMO), and provides mechanism for beam scanning and autonomous beamforming.

- Support very low latency communication along with the ability to serve millions of devices per square kilometre.
- There are plans to incorporating satellite communications in its upcoming revisions of the 5G standard at 3GPP.

5G cellular systems are able to achieve very high spectral efficiencies, *i.e.,* a high ratio of bit rate to the amount of spectrum used using the above technologies and carefully designed silicon. A 5G phone is expected to operate in hundreds of band combinations (frequency of operation), since the same phone has to work in roaming mode across countries and various operators. We make the following observations:

- The spectrum bands in which civilian cell-phones are capable of operating is increasing to cover most of the spectrum, which typically is used for military and space applications.
- A cell-phone is a very efficient multi-band/ multi-technology communication device that is capable of high bit-rates over good distances. These devices incorporate the above technologies and tuneable/ sophisticated RF in a hand held form factor at a reasonable price for the consumers.

Going forward, it is easy to see that most of these cellular technologies can directly or in-directly be used for military communications, providing an edge in both spectrum efficiency and costs. Also, from an EMS perspective, we observe that the cellular spectrum now spans till mmWave frequencies for 5G and will extend till sub-THz for 6G, providing newer opportunities and challenges for EMS management for the defence forces.

AI/ ML in communications

In the last decade, advances in optimisation theory coupled with

increased computational power and availability of methods to collect large data lead to the resurgence of neural networks and machine learning (ML). AI/ ML have been successfully been used for image and video analytics, data analysis for forecast and prediction. While the AI/ ML techniques have been used in wireless communication (at least to a smaller extend) as sub-modules for optimisation, there is a new trend in the last few years to use AI/ ML to design and operate wireless systems.

- AI/ ML for spectrum management: Currently, wireless systems operate in pre-determined frequency bands. It is well known that such operation leads to in-efficient usage of spectrum particularly if the usage is sparse (in time and space). A holy-grail of wireless communications is to identify and opportunistically use spectrum that is not used, in accordance to pre-determined rules. This problem is very hard to solve with conventional tools and AI/ ML seems to provide better solutions to achieving a true cognitive spectrum sharing system. If successful, this would truly change the way spectrum is assigned, used and managed. AI/ ML combined with game-theory is going to play a critical role in defining the engagement rules for spectrum and realising these systems.

- In the current wireless systems, hundreds of parameters such as transmit power, modulation (MCS), reference signal locations can be tuned to achieve better spectral efficiency. Tuning these parameters for improving the overall performance of a network is a non-trivial optimisation problem. A lot of work is being done to utilise the tools and techniques from AI/ ML along with data-collection (performance data) in the network to optimally tune and adapt the networks in a real-time manner.

- AI/ ML is also being used to design new modulation and newer FEC schemes that adapt to the channel in a real-time manner. This would vastly improve the efficiency of the systems and will allow the systems to be deployed in much harsher channel conditions in a reliable manner. Also, AI/ ML is being actively used

for adaptive protocol design and analysis.

AI/ ML is going to play a key role in the next generation wireless standards. In the studies that lead to 6G at ITU, AI/ ML for communications is touted to be one of the defining features.

Quantum Communications/ Computing

Quantum communications (QKD) provides a new manner of securing the communication channel from eaves-droppers. While currently, the QKD technology over optical fiber is mature, extensive work is being done to provide similar capabilities over wireless systems. If successful, these techniques will provide a secure method of communication on existing wireless channels.

Many optimization problems in wireless communications (to improve the efficiency of the system) are hard problems in the classical domain. For example, multi-user scheduling/ detection, optimal spectrum allocation are exponentially complex with increasing system size. However, some of these problems can be solved easily using quantum computing, thereby providing optimised wireless systems. Quantum computers/ computing techniques would provide a new tool to solving computationally hard problems in the wireless domain in the next decade for network optimisation.

MmWave and Terrahertz Communication

There is a huge paucity of spectrum in the sub-6 GHz for civilian usage. This is mainly fuelled by ever-increasing demand for higher data rates and the increasing number of devices. This lead the industry to explore higher frequency bands, which are typically used by military and space agencies. At the higher frequencies, at least for now, there is a large amount of spectrum that is available that can be utilised to meet the data requirements.

One of the first products in the mmWave frequencies is the WiGig (802.11 ad) WiFi at 60 GHz. The specification and products

have been released around 2016. There was a limited proliferation of these devices in the market, mainly because of the niche use cases that this product offered. However, this marked the beginning of mmWave devices for commercial applications and provided impetus to developing mmWave RF and circuits in CMOS technology.

The usage of mmWave frequencies (20 GHz-50 GHz) was envisioned for IMT-2020 by ITU and became part of the 5G standard with upwards of 400 MHz of bandwidth per channel. Currently, there are several large scale deployments of mmWave 5G networks across the world. The handsets (more expensive ones) also incorporated the mmWave technology to work with the networks. Usage of these high frequencies lead to a resurgence of small form factor phased arrays, which provide electronically steerable pencil beams for communication. Currently, a lot of research work is being done to build better silicon devices to handle mmWave frequencies and corresponding protocols to work with phased arrays. As this technology gets more mature in the next few years, we are going to see phased arrays everywhere and a plethora of devices and applications that operate on large bandwidth and provide high throughput.

Researchers are also currently investigating sub-THz communication (100-180 GHz) to further increase the available bandwidth, mainly for “almost” line-of-sight communications. Sub-THz frequencies offer a sweet spot between visible light frequencies and Radio frequencies, to cater to limited mobility and yet maintain communication link. Devices and new technologies are being explored to build systems capable of operating in these frequencies. In addition, these Sub-THz technologies along with phased arrays can also be used for imaging purposes, such as scanning machines in airports. Free-space optics and visible light communication has also gained prominence in the last few years and several prototypes have been built that show the feasibility of multi-gigabit communication using visible light wavelengths over large distances. It will be interesting to see if the teraHertz gap will be closed in the coming decade.

We observe that in the coming years, there will be commercial technologies available in the entire spectrum (from few 100 MHz to THz) with the goal of providing high band-width wireless links. Again, this makes EMS management and coordination more complex, but provides newer avenues of wireless communication. It would be worthwhile to point out that managing the spectrum would also require development and deployment of spectrum sensors to provide an accurate map of spectrum utilisation in the areas of interest across various bands. Such a network would help monitor and manage spectrum efficiently.

Software Defined Radios

Over the last few decades, radio hardware has changed significantly from simple analog systems to a complex combination of digital and analog systems. The systems used to be designed for a specific combinations of bandwidth, frequency and protocols. In the last few decades, there has been an effort to come up with generic hardware that can be used to transmit and receive at tuneable frequencies, various band widths and more importantly, the baseband processing can be performed on a generic computing device such as a processor (or in some cases an FPGA). This has been possible primarily because of

- Availability of generic RF front end IC's that can work over a wide frequency ranges and have a good bandwidth.
- Increased compute power of processors and flexible FPGA's which can interface with the generic RF front ends.

This combination of flexible RF and high compute power (in a small form factor) has led to a boom of software defined radios (SDR), which provide the users flexibility in term of waveforms and technologies that can be deployed. Even the handhelds (cell phones) have SOCs in which most of the processing is done in generic DSPs with special purpose hardware accelerators. Going forward, it makes sense to develop advanced generic hardware that can support various transmit and

receive protocols at different frequencies. In combination with AI/ ML, this provides users with access to powerful hardware that can be utilised to provide the optimised communication link across multiple frequency bands. While standards are necessary for inter-operability, with the advent of SDR and newer RF technologies, the development of custom protocols would become easier without compromising on the quality.

In this Section, we have seen some possible technologies that will play a significant role in wireless communication in the coming decades. We make the following observations:

- The operating spectrum for wireless communications will widen considerably, and encompass frequencies from a few MHz to THz. While government policy might restrict the legitimate use of some of these frequencies in a region, there will be no technological barrier in utilising this entire spectrum. Spectrum is going to get more congested with many more players and automated EMS management capabilities are going to become more critical.
- The RF and computational hardware is becoming more generic, yet powerful enough to run different protocols and modulation schemes. This hardware combined with AI/ ML would help in building perfect platform(s) for next generation wireless systems. The concept of application/ use-case specific communication systems and development in silos is going to become redundant.
- The development of all these technologies is happening at a very rapid pace and would most likely become faster with the advances in semiconductor technologies and computational platforms. The development of these next generation technologies is multi-faceted, costly (at least in the beginning) and requires expertise in various domains such as signal processing, embedded systems, VLSI, RF ICs, thermal engineering, antennas, AI/ ML and quantum systems.

Wireless Research R&D and Expertise in India

India has a vibrant research community and start-up ecosystem that works in wireless and communication systems. There are strong research teams in various institutions which work on cutting edge wireless problems. Some focus areas of these research groups across the country are:

- Communication algorithms and theory
  - o Physical layer waveform development
  - o Information theory and coding
  - o MIMO system theory
  - o Queuing and Networks
  - o Cellular and drone communication
  - o Antenna theory
  - o Computational electromagnetics
- Systems and hardware
  - o Software defined radios
  - o Custom RF designs
  - o Phased array systems
- IC design and device development
  - o RF IC design
  - o Digital ICs
  - o Processor development
- AI/ ML
  - o Theory of AI/ ML
  - o Optimisation theory

- Large data analysis with applications
- Game theory

- Quantum
  - QKD
  - Computing
  - Communications

In addition to these research groups, there are several start-ups and established companies which specialise in the design and development of various modules and software stacks for commercial wireless systems. There is also significant expertise in system development and manufacturing in government organisations like Sameer, CAIR, LRDE, DEAL, ISRO, CDAC, CDOT and BEL. A recent success story is the development of indigenous Shakti processor by a research group at IIT Madras. This processor is based on open source RISC architecture, manufactured in SCL Chandigarh and is comparable with existing commercial processors. There are Indian wireless companies, who have designed, manufactured (outside the country), and demonstrated wireless SOCs for LTE and DVB. Also, the capability of Indian software companies to build and execute large complex software projects is well known. *Hence*, *it can be stated without doubt that there is enough expertise within the country to design and build advanced wireless and computing systems along with the required software.*

Building the System

In the earlier Section, we argued that India has the expertise and capability of building and executing complex wireless systems across multiple organisations. If so, why does India not have indigenously developed EMS management capabilities?

Some possible reasons for this are:

- Indigenously developed Coordinated EMS Management solution with advanced capabilities might not have been a high priority for the armed forces till date.
- The expertise is spread over multiple organisations and these organisations are only doing R&D and developing sub-systems or small modules without a bigger picture. This leads to missing pieces in the puzzle.
- Most Indian start-ups and wireless companies are focused on developing products for civilian consumption for funding their day-to-day operations. They might not be focusing on developing EMS solutions for defence because of lack of funding and the absence of a clear road map for their developed products in the area of EMS.
- There are some fundamental technologies and manufacturing processes that we don't have expertise or access to.

Building an indigenous EMS system which leverages the latest technologies such as THz, AI/ ML and quantum computing would require a top-down approach. Next generation EMS management (and dominance) is a complex problem that involves various sub-systems and domains. The first step in building this system is to identify the underlying core technologies that are required to achieve the goal and engage with the required organizations for achieving the required goals. It should also be observed that achieving this goal would require both fundamental research work as well as product development and integration.

Large, focused research projects with an "end goal"

Most of the research funding to the universities is generally focused on solving smaller problems or developing sub-modules. This helps

mitigate risk and help in providing funding to more researchers. However, for developing complex systems, such as newer generation wireless systems, we observe that it is better to provide large quantum of funding to a few large groups. This kind of large funding provides a sense of ownership to achieving the end-product/ goal and helps to:

- Force researchers (across institutions) to collaborate on the solution from the beginning. This is a much better approach rather than individual development in silos and having an integration effort at the end which rarely works out.
- Provides financial flexibility to the research groups to take risk in trying novel options and involve industry (which is expensive).
- Develop solutions which are close to higher TRL levels for ease of adoption. Most of the smaller research projects flatter in the last stages of taking the developed technology higher TRL levels (close to production) as this involves substantial resources.
- This helps to train and develop substantial manpower with expertise in developing a particular end-to-end technology.
- Substantially reduces the overhead and makes it easy to track the progress.

The coordinating agency should recognize and understand that

- There is an inherent risk in any research project even of a large magnitude. In some countries with advanced technological capabilities, it is common to fund two large groups to develop the same technology. This results in competition (implicit) among the different groups and substantially increases the success rate.
- University research groups (however big they are) are more suited to developing newer and cutting-edge technologies and can seldom develop finished products that can be deployed in the field in one shot. The defense funding agencies should recognize this

from the beginning, be flexible, and have a plan to develop the field ready product over multiple stages, possibly with the involvement of industry.

- At the planning phase, it is very important to identify the required end goals. If the technology is being developed for the first time in the country, it should be noted that all the bells and whistles in a product are not possible in the first go and a phased approach should be adopted. The outcomes of such complex projects should not be evaluated in a black and white approach, but a softer and flexible approach should be adopted[1].

- While there should be good oversight on the project financials, there should be significant flexibility in utilizing the funds and hiring of manpower. For example, it is very common for funding agencies to divide the approved funds into categories like Capital, Consumables, Manpower, and Contingencies and enforce strict walls between them. It should be understood, however well the project is planned, it is very difficult (almost impossible) for researchers to predict exactly the equipment and manpower that is required. Many of the successful projects are those for which such flexibility is provided with high-level oversight and tracking. In addition, flexibility should be provided to the research groups to engage and provide funds from the project to the Indian companies from the beginning (this is not easy/ possible with the current rules).

Engaging Indian Startups and Companies

It is very difficult for startups/ commercial companies to work on cutting edge technologies without appropriate funding. Most of the companies (in India) focus on current commercial technologies and venture into advance technologies only when there is a customer demand. Technologies

1 In DARPA, some 90 percent of its projects fail to meet their full objectives.

like THz, AI/ ML for communications, Quantum computing are possible candidates for the next-generation standards. These technologies would require significant investment and it is too early and expensive for smaller companies. Some issues to be considered in this process are as follows:

- As with the research labs and institutions, it is good to fund a few companies with larger quantum of money rather than spreading the funding too thin. This will help them develop and own end-to-end technology.
- Most of the times, it is expected that the startups and companies put in their own money for developing prototypes for demonstration. Many a times, this is not feasible for smaller companies and startups, particularly when demonstrating newer technologies such as THz or Quantum which are very expensive. The coordinating agency should have some basic evaluation criterion and provide funding to these companies to build and demonstrate prototypes. While the funding should be considerable (as mentioned in Point 1), care should be taken so that the companies deliver most of what they promised in appropriate time lines.
- Once the prototype stage is completed, evaluated, and certified, the startup or the company should be provided orders for the final deployment. Appropriate aid should be provided to help the company manufacture the final products. The final IP should belong to the company, or the startup that invested time and developed the prototype. It is not a good idea to provide the manufacturing rights to other organisations without appropriate royalty.
- Defense procurements have stringent requirements in terms of technical compliance, and it is very difficult for startup companies to meet and demonstrate all the compliance requirements. To encourage the startups, particularly in wireless communications, it is important to enforce these requirements in phased manner.

- Provide easy access to the spectrum for field testing and also provide required platforms, space for testing these EMS systems. The testing procedures should also be planned as there will be considerable effort to developing these test systems also.

Engaging the Indian companies, startups, and research labs to build the EMS management systems incorporating the latest technologies (as described in the previous Section) should begin sooner than later. Building these complex systems take time and starting early provides a global advantage. During the same time, it is important to increase participation in standardization activities, understand the spectrum requirements for these new technologies and influence the global spectrum allocations.

***Prof Radha Krishna Ganti** is an Associate Professor, Dept. of Electrical Engineering, IIT Madras, Chennai

SPACE BASED ELECTRONIC WARFARE: A STRATEGIC FORCE MULTIPLIER FOR INDIA

Lt Col Vivek Gopal

Figure 1 Satellite Launch by ISRO [1]

Abstract

The modern challenges of dealing with the high-end capabilities of peer and near-peer adversaries, especially in confrontations requiring operations in Anti-Access/Area Denial (A2/AD) environments, have brought EW back to the forefront. This means that nations must re-invest in modern EW capabilities, and build enough capacity in these capabilities to compete with peer competitors. India needs to rewrite its EW Doctrine under the newly defined paradigm of Space-based EW. Space with its potential for militarization and with EW in particular needs

our immediate attention and aggressive pursuing. Benefits accrued from a COMINT/ ELINT payload in LEO/ MEO has benefits far more enriching than a conventional land-based EW system. This brief intends to address the steps that India needs to take to establish a National Space Operations Strategy leading onto a central apex organization to control and coordinate the militarization of space. While suggesting the roadmap in terms or realizable aims and action points, a global landscape in terms of Space based electronic warfare is also mentioned to put things into a better perspective.

Introduction

India is graduating towards a joint theaterized concept of operations which requires the integrated forces (battle groups) to be geared for multi domain operations (MDOs) based on an evolving and dynamic battlefield. Spectrum has become heavily contested and hostilities will always see forces operating in a degraded Electronic Warfare (EW) environment in the future. Ground based EW systems, although necessary and potent suffer from the drawbacks of lack of persistence targeting, limited coverage of the areas of interest and the fingerprint left behind due to emissions (if active). Space EW steps in to augment the ground-based systems by means of overcoming the drawbacks of ground based ELINT systems with the main advantage of persistent targeting and covering a very large footprint with a variety of payloads. India needs to step up to the challenge by means of devising a **National Space Operations Strategy** which will address the issues by means of cross-pollination of ideas and technologies across various domains and work alongside the Defence Space Agency to implement and operationalize the concepts.

Future military operations will be powered by modern, networked C4I systems which are distributable, survivable, secure, resilient and tailorable enabling a more lethal force. This also presents a larger attack surface for EW operations. One cannot expect the future wars to be won using legacy technologies. Spectrum is the new manoeuvre space and

has to be safeguarded to ensure furtherance of own operations tactically and strategically.

Perspective of Space Operations in India

India's entry into the space age was a consequence of the big commitment to 'Big Science' during the post-independence period under the vision of Nehru. [2] ISRO, the Indian Space Research Organization has been associated with the Indian space program right since inception in 1969 and has focused on the 'soft diplomacy' route with majority projects aimed at constructive civilian use. Courtesy the initiatives by this organization, among the spacefaring nations of the world, India can safely be stratified as a second-generation nation alongside China, Japan, Germany, France and Brazil. Countries such as United States and Russia with their industrial complexes have continued to dominate the space domain situating themselves in the top rung. Australia, New Zealand and UAE are also tailing behind and are the third-generation spacefaring nations. The year 2022 represents a significant milestone for India's space industry as it heralds the fifth decade since the establishment of the Department of Space (DoS). ISRO has led the space related activities from the front and has had several remarkable achievements, including successful space missions and development of technologies to foster India's self-reliance and progress. [3][4]

Technocrats (read NITI Aayog) in the government realized that the growth in the domain of space is directly linked to the growth of the country's economy. To that extent, the Make in India initiative has a strong component of 100% foreign direct investment for satellite construction and operations under the aegis of the Department of Space (DoS) which is the main policy making body. Space industry, with the entry of private players and advances made by various countries is no longer a preserve of a few, leading to democratization of the entire process.

There is an inescapable requirement to engage in cross-domain activities with regards to operations and it is the domain of space

which can result in asymmetric advantages against any adversary. Cross-domain synergy has been described in the Joint Operational Access Concept or JOAC[i] as "The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others—to establish superiority in some combination of domains that will provide the freedom of action required by the mission." [5] Among the various domains, space, with its advantages presents itself in the forefront of such fused activities; hence its importance.

"Currently, India's space economy constitutes almost two percent of the global space economy, which is estimated to be worth 423 billion USD." [6] A presentation by Indian delegation to 58th session of STSC - UNCOPUOS Vienna, Austria April 20, 2021[7] brought out the six decades' worth of contributions made in the space domain and the milestones reached in the space programme. To cover a few of these milestones, there were a total of 80 launch vehicle missions, 111 satellites placed in orbit (53 belonging to national requirements) and 342 satellites launched from 34 countries.

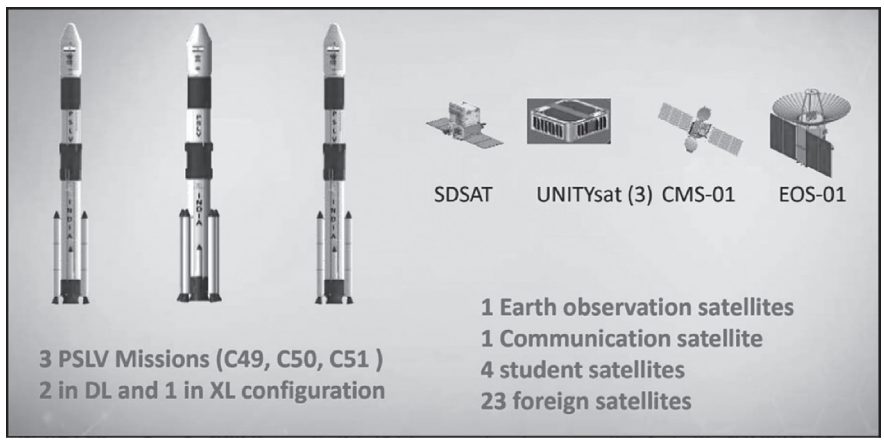


Figure 2 Missions Accomplished (March 2020 – 21) [7]

i The Joint Operational Access Concept (JOAC) describes in broad terms the vision for how joint forces will operate in response to emerging anti-access and area-denial (A2AD) security challenges. Version 1.0 of the document was released on 17 January 2012.

It is evident that the space programme for India is mainly driven by the civil use-cases. Despite the recent segregation of the military programmes under the aegis of the Defence Space Agency, no major endeavour is known towards space-based EW except for ISR capabilities in terms of the CARTOSAT series of satellites.

Space which was earlier a niche domain has now taken the shape of a disruptive arena where safeguarding interests have become paramount. Deterrence in space can only be achieved if one has an aggressively motivated offensive space strategy. While the launch of ICBMs or SLVs can always be assigned motives of tacitly exhibiting aggression, EW in space is one domain where Electronic Support (ES) measures can provide the offensive capability in today's 'information-ised' world. India with considerable space assets has no choice but to protect them by means of developing capability to take punitive action against such misadventures & impose a heavy cost penalty. While the focus should be on dual-use technology, India should always be prepared to tweak the technology for an offensive-defence role when warranted.

This brief aims to bring into perspective the need for space-based EW measured against the global landscape and advances made by the leading spacefaring nations (major focus on USA, Russia, China). To take it further, the paper also presents the way forward to establish a National Space Operations Strategy by focusing on the key areas where impetus is mandatory.

Need for Space Based Electronic Warfare

The world's leading military powers are placing increased importance on advancements in technologies and communications, such as artificial intelligence, cyber capabilities, 5G networks, and the Internet of things. EW as a domain too has garnered impetus due to the interplay of all such evolving technologies and space-based EW has reached disruptive significance poised to change the future landscape of military conflict.

MDOs will result in parallel engagements on land, sea, air, cyber and space domains. The debate between the semantics involved in Weaponization versus Militarization[ii] is historical since the launch of Sputnik by erstwhile USSR. However, EW as a domain in space occupies a place in both the aspects owing its spread in passive as well as active means to achieve the intended aim by definition. How EW is used in the domain of space, can have effects, on the deterrence & escalation dynamics alike.

Modern day EW can be traced back to Circa 1904-05 with the Russo-Japanese War. However, if taken in the Indian context, we can go as far back as the Mahabharata. To kill Dronacharya would have been impossible and hence the deception tactics (rumour/ false propaganda in today's parlance or manipulation of information as part of EW tactics) of spreading the news of the death of Ashwathama (an elephant who shared the name of Dronacharya's son) exposed his vulnerability had resulted in Dronacharya's death. One century later, EW has resurfaced as the prime contender in today's operations. The contested space domain & ever shrinking EM spectrum has exposed a wider attack surface for EA scenarios. Space as the latest dimension added to warfare has been invigorated with Revolution in Military Affairs (RMA) leading to a Revolution in Space Affairs. EW as a domain, with the advances in technology has transcended into space with countries vying to monitor, control & seize every initiative to achieve ascendancy over the adversaries. A good analysis of how space is helping EW for ground forces has also been done by Mark Pomerleau [8].

ii Space can be thought to have been Militarized right since the Sputnik era and the launch of the communication satellite. Space weaponization is generally understood to refer to the placement in orbit of space-based devices that have a destructive capacity.

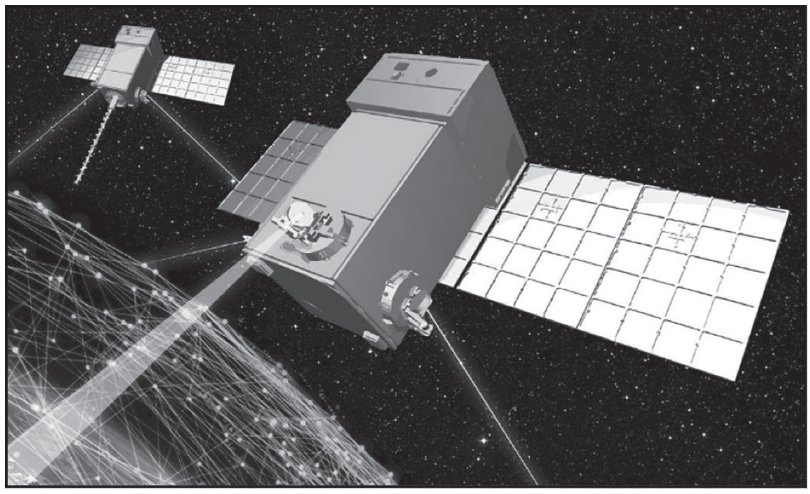


Figure 3- Space-based Sensors for EW [8]

EM spectrum is the new manoeuvre space & freedom of action in this domain while denying the same to the adversary can tilt the balance in favour of the technologically advanced force. Similarly, space EW will ensure the safeguarding of one's space assets which are of prime (national) importance and also portray a nation's might (power projection) in the geo-strategic environment. The need for Space based assets is also greatly influenced by the techno-geo-strategy. Speaking of the theory of offensive realism (propagated by Mearsheimer), China has openly displayed its intent to capitalize on the space domain trying to surpass giants such as USA & Russia. The geopolitical and strategic imperatives to counter the encirclement tactics of China is motive enough to invest time and energy towards developing space assets thereby countering the non-contact warfare approach advocated by the PRC. With Chinese initiatives such as the Beidou constellation (ground station at Ngari in Tibet being the closest to India) and ASAT test in 2007, India needs to adapt its modus operandi to keep pace as well as counter the rise of the dragon as an immediate threat.

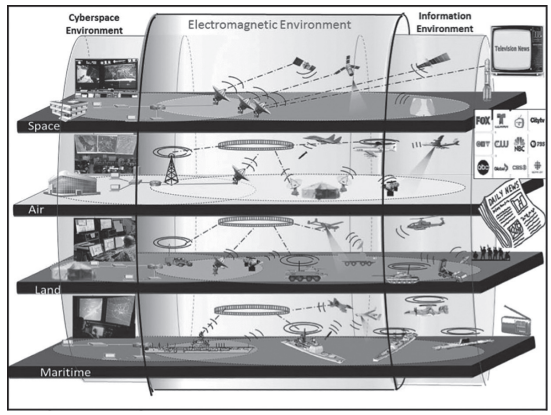


Figure 4- Contested EM Environment [9]

Space domination can be graded as one of the pertinent factors in support of foreign policy and national interests, thereby contributing to the overall comprehensive national power. Pakistan's space capability is following the Circa 2047 vision with an overshadow of 'assistance' by its all-weather ally China [10].

With a growing dependence on space-based operations & proliferation of space-based assets, there is a need to address the challenges being faced with respect to the security of these assets in various orbits. A study [11] by Centre for Strategic and International Studies (CSIS) shows how the space weapons can be categorized viz., Space to Earth, Space to Space & Earth to Space. Drawing a parallel for EW in space, as also shown in the same study, jammers & directed energy weapons (DEW) are capable of effects in all the three categories[iii]. Unfortunately, what has been covered are the attack capabilities of EW, while the passive & more potent features of ISR, direction finding & persistent targeting has not been elaborated as part of weaponization. Naysayers & experts may beg to differ on this concept which might seem at a cross with the generic definitions of ES, Electronic Attack (EA) &

iii See Appendix 'A' for a table quoted from the same study regarding the electronic weapons in space.

Electronic Protection (EP) or how EA is used as an attack strategy, while ES is merely passive (although passive measures used aggressively can reap immense dividends). One may also give credence to the fact that active defence is not offense.

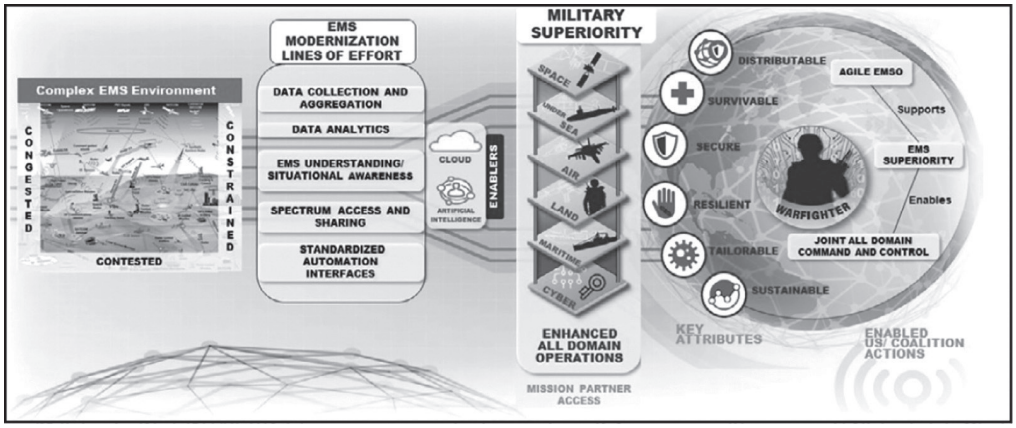


Figure 5- Electromagnetic Spectrum Operations Visualization [12]

Global Landscape: Counter Space Capabilities & Space Based Electronic Warfare

"EW is the art of the invisible" [13]. A definition of space electromagnetic warfare as given in a publication [14] by the Defence Technical Information Centre or DTIC is as given below.

> *"Space Electromagnetic Warfare – Knowledge of spectrum awareness, manoeuvre within the spectrum, and non-kinetic fires within the spectrum to deny adversary use of vital links. Skill to manipulate physical access to communication pathways and awareness of how those pathways contribute to enemy advantage."*

The same DTIC report also mentions the most critical objective of space EW being the gains in the cognitive dimension. "Decision superiority, deterrence, dissuasion, compellence, and assurance manifest here. Neutralizing an adversary spacecraft offers limited military value if such actions fail to influence the perceptions or decisions of the enemy [14]."

While counterspace capabilities can be broadly divided into the realms of kinetic physical, non-kinetic physical, cyber and EW, this paper will cover EW and merely touch upon the others. Russia, China and USA have been covered and in addition Australia, France and North Korea.

EW is a viable option for counterspace because of its flexibility: its temporary application at the point of impact and effects on adversary satellite are temporary, unless it employs very high power to burn the electronics. Also, it does not generate any orbital debris. EW is an extremely attractive option for any space faring in the future intending to protect its assets in space. With greater reliance being placed on ISR and GNSS for operations, EW will be a very potent weapon [15].

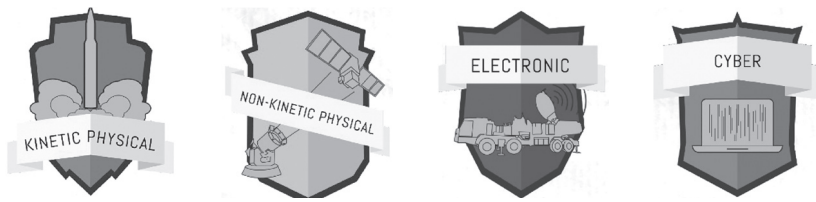


Figure 6- Symbolic Representation of the Realms of Counterspace Capabilities [11]

Russia- The birth of Space EW can be traced back in Russia to the era of the US led SDI[iv] project. OREST-02 was one of the projects which was shelved later. In terms of counter space capabilities Russia has

	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	○	-	●
MEO/GEO Direct Ascent	○	-	-	●
LEO Co-Orbital	●	○	-	●
MEO/GEO Co-Orbital	○	-	-	●
Directed Energy	●	○	?	●
Electronic Warfare	●	●	●	●
Space Situational Awareness	●	●	●	?

Legend: none ● some ○ significant ● uncertain "?" no data "-"

iv Strategic Defence Initiative or its popular nickname of the 'Star Wars Programme'.

made significant progress. Whether it is RPO[v] or EW capabilities, Russia has made investment in jamming PNT[vi] signals as well as communication uplink and downlink signals. To counteract the technology prowess by US forces, Russia has made efforts to combine EW into military operations. Russia has also taken several initiatives to drive the EW programme towards significant Space Situational Awareness or SSA capabilities. All its efforts are towards seeking parity with the US forces in this domain. Some examples of the Russian prowess in the field on Space EW can be gauged from the developments of the Peresvet system, Tirada series of satellite EW system and the Bylina systems. Peresvet is the Russian solution to the fourth dimension included in their definition of EW which includes "countermeasures to foreign technical reconnaissance". Capabilities of Tirada EW system have been covered as part of [16].

In Russian, the name Bylina has been used for a C2 system which are operating in different parts of the radio spectrum (Bylina-KV and Bylina-MM). Open-source information places them as weapons against communication satellites. News released in 2016 talks of another satcom jamming system – KRBSS expanded as "Electronic Warfare Complex to Counter Satellite Systems in Low Circular Orbits". This system deployed in the Arctic, was probably designed to target LEO satellite constellations such as Iridium, Globalstar, and OneWeb. Krasukha-4 (Russian poisonous plant – Belladonna or Deadly Nightshade) which has been quite prominent in recent skirmishes is aimed against radar-based surveillance satellites. On-board two Kamaz-650 trucks, both Krasukha -4 and its erstwhile model, Krasukha – 2 are part of the EW complex Moskva -1 (1L267). This project traces its genesis in the 1990s. Another EW Space defence project called the Divnomorye (name based on a Black Sea resort in southern Russia) started development in 2013 and was claimed to be ready for deployment by early 2016. There have been reports of its deployment in 2018. Touted as an improved version of

v Rendezvous and Proximity Operations
vi Position Navigation and Timing signals

the Moskva -1, it can be used for ELINT as well as a command post [17]. Russia has also constructed three ground-based SIGINT sites intended to pick up and analyze foreign satellite EM emissions over Russia. These will complement the country's Space Surveillance System (SKKP). These facilities are built under the project name 'Sledopyt'. Another such EW complex to protect Russian satellites against EA measures is called the 'Tobol'. Whether the projects have been delayed or have been made operational is not yet known [18]. There have also been rumours surrounding the top-secret nuclear-powered satellite 'Ekipazh' specifically meant for space EW. KRET (Concern Radio-Electronic Technologies), is under the Rostec State Corporation, and is the largest holding in Russia's EW industry. Important stakeholders in the Russian EW systems are Vladimir Design Bureau of Radio Communications (VKBR) with its subcontractors i.e. Vladimir Radio Equipment Factory, the Radio Research and Development Institute (NIIR), NPP Istok, the Moscow Radiotechnical Scientific Research Institute (MNIRTI), and NPO PM-Razvitiye. REB-K units in the Russian defence forces are the operators of Russian EW systems.

China- The PRC space capabilities and developments would require a separate paper to do justice, however, the noteworthy EW related

	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	●	●	●
MEO/GEO Direct Ascent	○	○	-	●
LEO Co-Orbital	○	?	-	●
MEO/GEO Co-Orbital	○	-	-	●
Directed Energy	●	○	-	●
Electronic Warfare	●	●	●	?
Space Situational Awareness	●	●	●	?

Legend: none ● some ○ significant ● uncertain "?" no data "-"

aspects are covered subsequently. The PLA experimented with electronic reconnaissance satellites in the mid-1970s. The satellite was launched from Jiuquan in July 1975 on an FB-1 launch vehicle,

which was specifically designed to meet the weight and orbital accuracy requirements of electronic reconnaissance platforms. The FB-1 launched two more experimental satellites in December 1975 and August 1976. For unknown reasons, the program was discontinued. Publications by the Chinese Academy of Military Sciences bring out the fact often professed by the PLA – Those who can rule space, will rule the Earth. The data available in open source suggests of several developments that have been undertaken by China in terms of Counter Space capabilities. SSA is one of the many functions where impetus has been laid down

> *"Space attack and defence operations are [a type of] direct military confrontation activity carried out mainly in outer space by the opposing sides. Space warfare takes military space forces as the main operational strengths, takes the opposing sides' direct attack and defence as the basic form of expression, and takes seizing and maintaining dominance of outer space over a certain scope and within a certain time as the basic goal. It is the form of space-domain military struggle sharpest in confrontation and highest in intensity." [21]*

in China. The reconstitution & reconfiguration of the PLA giving rise to the PLASSF with cyber & EW domains included is a major step highlighting the inclination of PLA towards defensive (active defence) and offensive capabilities. The tests (RPO) which took place after the launch of the 'SJ'[vii] series of satellites can be extrapolated for military use, mainly jamming capabilities of adversarial space vehicles. The DIA report of 2019 [19] also brings out the Chinese SATCOM and SAR jamming capabilities. Similar analysis has been done in an ORF occasional brief [20].

vii The notorious Chinese inspector satel¬lite, dubbed Shijan-17 (SJ-17), was rel¬atively quiet this past year but did make a few stops near other satellites as it moved around the GEO belt. According to CSIS analysis, SJ-17 performed three enduring rendezvous proximity opera¬tions (RPOs) nearby other Chinese satel¬lites, Chinasat 6B, SJ-20, and Gaofen 13 (GF 13).

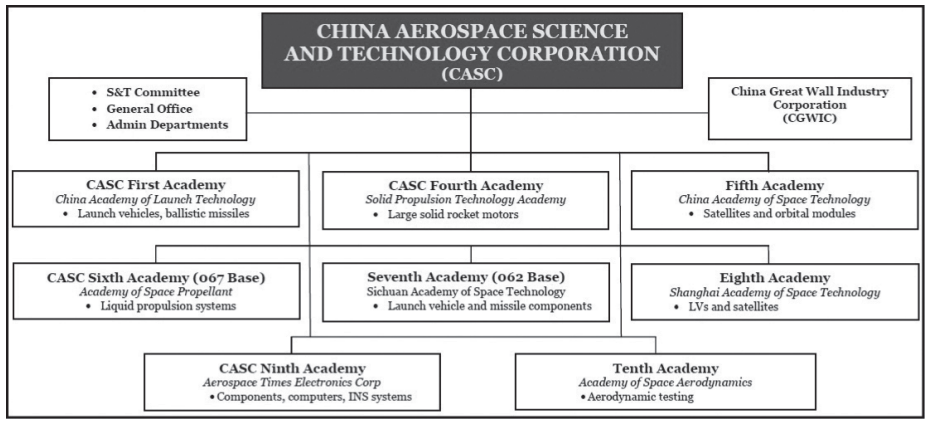


Figure 6– China Aerospace Science& Technology Corporation [22]

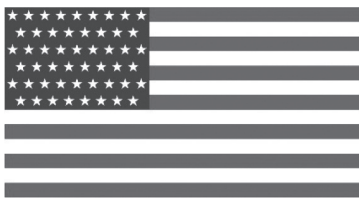
Open-source data also confirms of the PLA utilizing TDOA[viii] based techniques for geolocation using clusters of three to four satellites. CASC[ix] 509th Institute and SWIEE[x] have accounts of PLA direction finding and tracking methodologies. While information is sparse, indications exist that at least some funding has been dedicated toward developing a space based ELINT capability as China clearly believes that to exert itself regionally, it has to develop capabilities in electro-optical, SAR and ELINT. Further details regarding the military satellites, stealth satellites and ELINT are covered in papers published by the Chinese Journals. [23] [24] [25]

Chinese and Russian military doctrines present the view of space as an inseparable part of modern warfare and view counterspace capabilities as a means to reduce adversarial military effectiveness. While US established the Space Force, both these countries reorganized their militaries in 2015 to provide impetus to space operations. [26] [27]

viii Time Difference of Arrival – a direction finding method used commonly in EW.
ix China Aerospace Science & Technology Corporation.
x Southwest Institute of Electronic Equipment.

China in the domain of EW is gaining near-parity with the US forces. This includes both soft and hard kill measures as part of the EM spectrum dominance strategy under the umbrella of the overarching 'informationised' & 'intelligent-ised' concept of integrated network and electronic warfare [28]. Integration between these domains has been professed as "the only way to simultaneously 'decapitate and blind' the adversary while 'crushing their bones and damaging their body' to sustain the People's Liberation Army's advantage and accelerate the operational tempo." [29] A high-level spectrum policy is also being formulated as per certain reports [30]. The exploitation of space by China in terms of EW can be sensed from reports where scepticism has been seen with activities related to China in space [31] [32] [33] [34]. Another wholesome account of Chinese ELINT & SAR/ Optical imagery capabilities has been covered in the article at [35].

United States (USA) - Through the EW Counter Space System (CSS) and the Navigation Warfare (NAVWAR) programme, US forces are



	R&D	Testing	Operational	Use in Conflict
LEO Direct Ascent	●	○	-	●
MEO/GEO Direct Ascent	-	-	-	●
LEO Co-Orbital	○	?	-	●
MEO/GEO Co-Orbital	○	?	-	●
Directed Energy	●	○	?	●
Electronic Warfare	●	●	●	●
Space Situational Awareness	●	●	●	●

Legend: none ● some ○ significant ● uncertain "?" no data "-"

presumably at the top when it comes to EW employed in various domains including space. Defensive and offensive space control are amalgamated into the SSA programme for USA and investments have been made right since the 1960s towards developing a substantial capability. Very little information is available on NAVWAR in the open domain, however, it is estimated that since its inception in 1990s, heavy investments have been made to bolster the capabilities as part of SSA and counter space

activities. Similar is the case for the CCS established in 2003. US forces have also conducted various exercises in which activities were done in a GPS denied environment. The US forces are taking the lead and making an all-out effort to ensure that all space assets get unified under a central agency and that the parochial attitudes of individual services are set aside. The setting up of the Space Force (erstwhile US Airforce Space Command) with a Title 10 role (Title 10 of the United States Code **outlines the role of armed forces in the United States Code**. It provides the legal basis for the roles, missions and organization of each of the services as well as the United States Department of Defence). amplifies the point [36]. The United States has employed its technological prowess for the development of several weapon systems to maintain ascendancy over adverserial forces in all domains. US forces are heavily reliant on PNT signals and network centricity, even for expeditionary forces. It is launching several satellites every year to extend its military capabilities. In December 2020, the US launched the NROL-44 satellite as part of the plans of the US National Reconnaissance Office (NRO[xi]. The Advanced Extremely High Frequency Spacecraft (AEHF-5)[xii] was easrlier launched in 2019 [37]. U.S. Space Force now controls the GPS Block III satellites aimed to provide resilient PNT signals for its forces worldwide. “The newest satellite from the latest generation of more accurate systems is among a larger group of 24 GPS payloads on orbit that are capable of using a new military PNT signal, M-code.” [38]

Space Delta-3, formerly the 721st Operations Group, at Peterson Airforce Base, is the unit which controls Space-based EW for the US forces to dominate the space domain. “Space Delta 3 includes both offensive and defensive space control operations. Offensive space

xi The NROL-44 is a geosynchronous signals intelligence (SIGINT) satellite weighing more than 5 tons and is outfitted with a huge parabolic antenna, which unfolds to a diameter of more than 100 meters in space.

xii The AEHF-5 provides jam-proof communications, including real-time video streaming between the control and the deployed forces.

control is intended to prevent an adversary's hostile use of space capabilities, while defensive space control focuses on identifying and geolocating interference with U.S. capabilities, thereby protecting space capabilities from attack or interference."[39] The U.S. military also relies on satellites for SIGINT, and is reported to have up to three giant 'Mentor/ Orion' satellites parked in GEO for the purpose of collecting radio emissions with radio reflecting dishes estimated to be 100 meters in diameter.[40]

France - France too has made the transition of the satellite control to their military and delinked it from their civil space programme. They have a well-defined Space Defence Strategy.

Iran - Islamic Revolutionary Guard Corps (IRGC) conducted two major exercises in 2020, which Iranian sources claim included "space operations" using jamming drones and radar units from the IRGC Aerospace Force. In February 2021, Aerospace Force Brigadier General Mehdi Hadian hailed Iranian electronic warfare capabilities in recent exercises, with a focus on offensive and counter electronic warfare against enemy air power [41]. In March and May 2020, there were reports of Iranian GPS circle spoofing. GPS circle spoofing differs from other spoofing attacks in that it causes transponders to show various erroneous positions forming odd ring-like patterns around a central location. Previously observed in China, the March 2020 incident involved a potential GPS spoofing device in operation at Iran's Army Command and Staff College [42]. The May 2020 incident also involved the circling phenomena with GPS-based reporting systems from vessels and fitness trackers in Tehran. Iran has publicly claimed in the past to have the capability to spoof GPS receivers.

North Korea - U.S. Army published a new manual titled North Korean Tactics in July 2020 which details North Korea's electronic

warfare organizations, capabilities, techniques, and tactics. [43] North Korea continues to exercise its downlink jamming capabilities. In April 2020, North Korea announced that it was preparing to deploy a new "GPS jamming device" for use against South Korea. [44] Many open-source reports in the past year highlight jamming focused on commercial radio broadcast frequencies and civilian GPS signals rather than military targets. The report at [43] also highlights the Electronic Warfare Jamming Regiment focused on electronic jamming and signals reconnaissance.

UK - The United Kingdom continues to integrate space into its military structure. In 2021, the country announced building the Royal Air Force Space Command in Scotland. The first commander of the United Kingdom's Space Command was also announced in February 2021 and the command is scheduled to be operational and capable of launching its first rocket by 2022.

Australia - part of the Project 9358 (includes the JP 9102 Australian Defence SATCOM System project), Australian Defence Forces are exploring options of the deployment of ground-based EW sensors. After the 2020 Defence Strategic Update, this project aims to fill the void in capabilities in EW related to space. Australia's military use of the space domain rests on communications between Earth and satellites. The country's armed forces use satellites for navigation, communications and Signals Intelligence (SIGINT). Central Australia is home to the Pine Gap Earth Station near Alice Springs. Pine Gap receives raw SIGINT from US satellites as they pass over Asia and the Middle East. These SIGINT satellite constellations include Advanced Orion, Improved Trumpet, Mercury and the Space-Based Wide Area Surveillance System. Not surprisingly, no information appears in the public domain on the datalink frequencies used to transmit raw SIGINT to Earth. [45] [46] The Wide Area Space Surveillance (WASS) system of the Australian Defence Forces [47] is how ground stations can be used to monitor the space activities. The capability consists of using over the horizon radar network to keep track of orbital debris and satellites in LEO. Called

the Jindalee Operational Radar Network or JORN, radars are placed at three locations manned by BAE and controlled by the Australian Airforce Number 1 Remote Sensor Unit.

The not so very distant Nagorno-Karabakh conflict drives home some pertinent aspects as regards space-based EW. “First, an integrated air-defence system is critical; Second, the role of electronic warfare should be accentuated; and third, the human factor is key, and it underpins the other two factors.” [48]

Space EW Strategy Development Matrix

Since the First Gulf War, Space has gained prominence in executing operations and is a reflection of the foreign policy and strategic interests of a nation [49]. Similar views as regards strategy for Space has been echoed by IDSA in their policy brief [50] which states that geostrategic viewing of the space related activities links it closely to a projection of a nation’s comprehensive power & extension (read symbolic) of foreign policy. Emphasis is therefore necessary to develop capabilities for satellite hardening as well as EW measures to safeguard these national assets in orbit. Strategy, and in turn policy, will be a derivative of the questions asked which underscore the requirement of EW in Space. To quote from an AFCEA[xiii] whitepaper [51], a wonderful set of intriguing questions put forth have been replicated as under.

(a) What are the implications of a contested space environment on ISR developers and users?

(b) Are we treating Space and our use of Space correctly?

(c) Are the future requirements for the use of space by both the Intelligence Community and Defence Department driving us to the same position on Space ISR or to radically different positions?

xiii AFCEA - Armed Forces Communication and Electronics Association.

(d) Should we adopt a strategy and policy position that approaches space differently, for instance, as a kinetic or non-kinetic warfighting domain?

(e) What are the implications of continuing with the current Space posture and not making a change?

(f) What shorter term actions should we take within our current bounds?

Based on the questions posed earlier, certain strategic goals come to fore when it comes to formulating and implementing a Space EW strategy. To state a few, not in order of precedence are as follows.

(a) **Agility** - Developing agile EW options aiding EM Spectrum operations. These agile options include the development of state-of-the-art ES and EA measures.

(b) **Resilience** - Enhance the delivery of own signals in the contested domain. Robust EP measures will ensure that our own forces are not hampered by the adversarial attempts to eavesdrop into our communication and PNT signals. Case in point of the resilient GPS signals by the Block III satellites of the United States.

(c) **Transparency** - Provide an integrated picture at the theatre level. This will ensure coordination of the resources at the highest level and the judicious employment of EW resources which are not too proliferated owing to the cost prohibitive technologies involved. Tools such as the EW planning and Management Tool or EWPMT[xiv] are a great asset in this effort.

xiv Provide a suite of software tools and applications by delivering six capability drops (CD) that enhance the manoeuvre commander's cyber-electromagnetic activities (CEMA) element's ability to plan, coordinate and synchronize electronic warfare (EW), spectrum management (SM), and Cyber operations (CO) across the 2/3/6 staff sections.

(d) **Synchronize** – All sensors to be in sync to help in the analysis of the emerging operational scenario. The endeavour undertaken as part of the 'Project Convergence'[xv] by the United States is a glaring example of this synchronization.

(e) **Establish** - A National Space Operations Strategy thereby transition from outdated technology towards seizing high ground with novel sensors and technology.

(f) **Accelerate and Innovate** - Accelerate the deployment of Space based EW assets and innovate by rapid prototyping of payloads.

(g) **Develop** - A conducive environment for development partners to nurture the capability and grow at an accelerated pace. This development can be aided by the correct fusion of military-academia-industry. There is an inescapable need to innovate, optimize and cultivate talent.

The **Terminal Objective** of such an exercise of strategizing should yield in establishing policy and procedures for enabling Space-based EW components and assets. Work towards commonality in operating procedures and equipment which helps to leverage the advantages accrued out of the space-dimension of warfare.

Way Ahead for India

Indian activities in space underwent a metamorphosis after March 2019, when the then Prime Minister announced to the world about India's Anti-Satellite Test (ASAT). This heralded the inclusion of India within the gamut of select nations after United States, Russia & China. The latent capabilities existing with India were transformed into a harbinger of the

xv Project Convergence is the US Army's campaign of learning, experimentation and demonstration aimed at aggressively integrating the Army's weapons systems and command and control systems with those of the rest of the Joint Force

materialization of a strong deterrent capability. Project Shakti as it was dubbed resulted in a change in the way the world viewed India and the message conveyed was that of a transition towards a Space hard power wielding nation [52].

Space domain is the characterized by a Disruption in Military Affairs which has had connected effect on the C4ISR capabilities transforming to C6ISR (including Cyber and Combat Intelligence) [53]. These capabilities, based on their resilience drive the military decision-making process in consonance with enhanced situational awareness – hence, the importance of Space-based EW as a pivotal counterspace capability and the measures to preserve the assets in orbit. Nearly 15 military satellites presently are being used for varied purposes by India, the last being the GSAT-7.

The ten Air Marshal Chaudhari, Vice Chief of Air Staff while addressing the **e-Symposium on 'Space Technologies for National Defence'**, organized by FICCI, in association with Society for Aerospace, Maritime and Defence Studies (SAMDeS), brought out the need for an independent military space programme which so far has been dependent on ISRO's civil space programme [54]. It was also mentioned that indigenous capability to observe, track and identify non-cooperative objects in outer space is an inescapable requirement looking towards developing a common operating picture. This accentuates the requirement of SSA or Space Domain Awareness of which EW is a key component.

The electromagnetic environment has become exceedingly dynamic. Nations are pushing the envelope when it comes to developing advanced C4ISR capabilities and are become more reliant on PNT signals and satellites for operations. India too is trying to keep pace with these advances. Defence Space Agency in India has issued a RFI in January 2021 to look at collaborations to thwart threats in this niche domain of Space-based EW [55] [56].

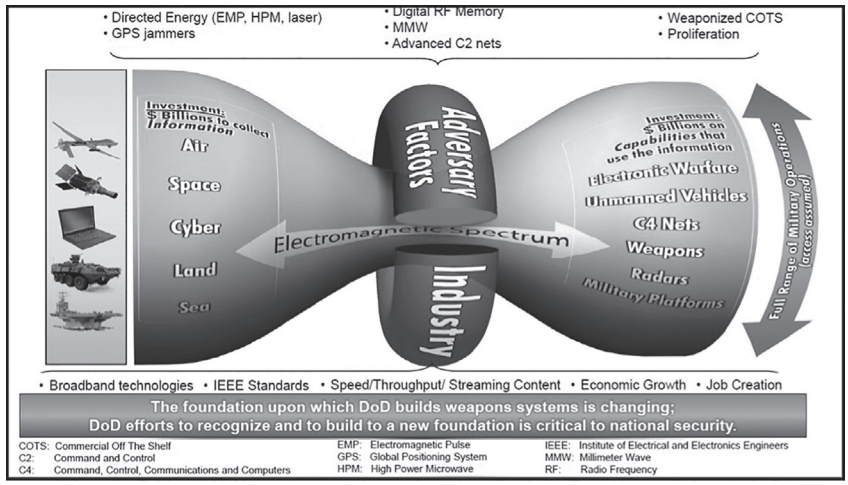


Figure 7– Rapidly Changing EM Environment [57]

The steps for the way towards attaining parity in the EW domain in the long run will involve meeting certain aims which can be listed as follows.

(a) **Aim 1**. Develop Agile Electromagnetic Spectrum Operations.

(b) **Aim 2**. Enhance the Delivery of Resilience of Position, Navigation, and Timing (PNT) Information. How much the anti-jamming properties of NaVIC (IRNSS – Indian Navigation Constellation) can be utilized is yet to be seen.

(c) **Aim 3**. Formulate a Single Point National Level Organization Authority. Establishing a Spectrum Warfare Wing has been proposed in a Centre for Land and Warfare Studies or CLAWS occasional brief [58].

(d) **Aim 4**. Develop and Provide state-of-the-art Communication Capabilities. This will involve accelerated and proliferated use of software defined radios and a resilient waveform [59] to name a few.

(e) **Aim 5.** Accelerate and Synchronize Fielding of Satellite Systems with Variable Payloads. These payloads in LEO can help in ISR capability along with direction finding EW satellite payloads. ELINT and SAR payloads also need to be increased in number alongside the constellations of cubesats.

(f) **Aim 6.** Develop a Regional Electromagnetic Spectrum Information System on the lines of the U.S. developed GEMSIS[xvi]. [60]

Implementation Strategy

Having seen the strategy and aims, it is the implementation part of the entire process which is going to bear fruit or lead us to a sustainable end state. Some pointers towards the implementation of the Space-based EW strategy are covered in the succeeding paragraphs.

Action Point I. Like any other domain, alignment with the other doctrines already in place is a necessity which brings us to the fact that there is an emergent need to revisit the EW concepts and **evolve a doctrine** which encompasses the future battlefield scenarios and ways to fight. Space based operations will see a flux with the cyber operations (read cloud-based and Artificial Intelligence), termed as Cyber Electromagnetic Activities (CEMA) interplaying with the classical EW domain. Organizations such as Defence Space Agency, Cyber Command and a dedicated EW organization need to come together to fuse the capabilities thereby aligning the objectives. As a recommendation, the taxonomy of a proposed Space Doctrine/ Publication may be adapted from the Joint Publication 3-14 of the US Forces, issued in October 2020.

Action Point II. Space is a contested, congested and competitive domain. No longer is it the sole playing field for a select few nations. Establishing an 'Aerospace Command' has been marred with a myopic

xvi Global Electromagnetic Spectrum Information System (GEMSIS).

view by the stakeholders. The powers that be, should take cognizance of the similar verticals established in the leading space faring nations to **migrate to a well-structured, agile & responsive organization**. With the lack of established and fundamental doctrine, India must look inwards to other organizations to establish doctrinal principles to enable the space warfare plans, execution, and assess training for the same.

Action Point III. Technology absorption which involves the subsets of **funding research and development**, reverse engineering, developing infrastructure and a wholesome contribution by the military-industry and academia.

Action Point IV. Industry Participation for Research Collaborations and Building Technological Capabilities is inescapable. India has set up the autonomous body, Indian National Space Promotion and Authorisation Centre (IN-SPACe) under the Department of Space (DoS). **IN–SPACe** will act as a link between the ISRO andprivate sector companies, assessing how best to utilise India's space resources and increase space-based activities. Similarly, the recently established **ISpA** or the Indian Space Association is a positive step towards nurturing private sector participation in Space. ISpA, IN-SPACe along with **NSIL** or the New Space India Limited concern of ISRO can together with joint effort (consortium approach) augur well for the future in this domain. **Incentivization as done for the drone sector** by means of **production linked incentives** should be catered for the Space industry.

Action Point V. Establish programmes such as the **school and college level** NASA space challenges and Grand challenge programme by the NITI Aayog to foster talent in the domain of satellite technology. Simultaneously **invigorate the start-ups**. Measures that have been initiated to invigorate the Space industry including startups is surely going to provide a ray of hope for a new strategic trajectory for India. Reliance on nanosatellite constellations to achieve what the cost-prohibitive smallsats or the 1000 kg satellites cannot. **Rapid prototyping**

using fast track procedures and faster launch capabilities are the hallmarks of a well-established Space domain. Programmes such as **Rapid Agile Launch Initiative**, that is, use small satellites to test sensor capabilities.

Action Point VI. Developing an EW Mindset. One of the most essential facets towards developing an EW force lies in mentally and cognitively training the mind to understand the concepts and implement ideas in unorthodox and out-of-the-box ways.

Action Point VII. Partnership with International Space Agencies. Despite the skepticism surrounding the military utility of the Quad, the collaboration between the members for developing better payloads, miniaturization and sharing of research work and data can immensely benefit the cause.

Action Point VIII. Use of Disaggregated Systems – This would entail the stratification of assets at the strategic & tactical/ operational levels and act as a major countermeasure to widespread EA activity by the adversary.

VIII. Conclusion

Military space power is the ability to accomplish strategic and military objectives through the control and exploitation of the space domain. Security, deterrence, and violent competition are the signs of a warfighting force, and military space forces are no different. Progress in the domain of Space EW will reconfigure the rules of deterrence & alter the dynamics during a heightened skirmish. It is high time that we had a comprehensive National Space Operations Strategy to cater to a rainy day in space.

Unlike doctrines, ancient treatises & eponymous texts such that of Sun Tzu which have compiled generations of military experience into comprehensible learnings, space as a domain is new. However, it should always be recalled that the underpinnings remaining the same,

it is the application of these learnings that have to be translated into actionable steps extending to the domain of space. Space requires an unprecedented forward-looking approach & out of the box thinking to apply concepts; to forge its own future, while being costly, safeguarding the outer space & the world as we know it against untoward & irresponsible actions. Space has emerged as an inescapable warfighting domain & EW within space inseparable for continued asymmetric advantage & psychological preponderance.

Like China, there is a need to have a national agency to coordinate all the activities pertaining to the militarization of Space. By leveraging the power of Space-based operations, India can afford to exert its presence much beyond its shores in-line with the aim of graduating to become a regional power by complicating the regional dynamics (read China). Over the next decade India must aim at advanced precision strike assets, integrated with persistent space-based surveillance. India's external behavior is characterized by exerting itself as a potent regional power while always preparing itself for a two-front war. The developments of the recent past have tilted the attention focus towards China while the Af-Pak issue continues to simmer.

Do we want to take the lead, be up there with the leading nations or merely be reactive? This is something we need to answer and decide now. EW has always aimed at developing technology that causes entropy to set in thereby imposing a cost penalty of the adversarial forces. A reactive force will always have catching-up to do. Space with its potential for militarization and with EW in particular needs our immediate attention and aggressive pursuing. Benefits accrued from a COMINT/ ELINT payload in LEO/ MEO has benefits far more enriching than a conventional land-based EW system. Naysayers may be skeptical with respect to the costs involved in development, as budget involved is substantially more due to the complexities involved in micro-electronics, launch costs and associated overheads. However, if we are to keep in mind the **'Nothing Ever Goes Unnoticed'** paradigm of EW, then

the space-based operations are to be viewed as a life-insurance policy which pays dividends when life is at stake.

*Lt Col Vivek Gopal a Senior Instructor at MC EME Secunderabad is a prolific writer on technical subjects

Appendix 'A'

	Electronic		
Types of Attack	Uplink Jamming	Downlink Jamming	Spoofing
Attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack
Reversibility	Reversible	Reversible	Reversible
Awareness	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	May or may not be known to the public
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible
Collateral Damage	Only dirupts the signals targeted and possible adjacent frequencies	Only disrupts the signals targeted and possible adjacent frequencies	Only corrupts the specific RF signals targeted

Types of Counterspace Weapons

Source: T. Harrison, K. Johnson, and M. Young, "Space Threat Assessment 2021," Csis.org, 2021. https://www.csis.org/analysis/space-threat-assessment-2021 (accessed Oct. 14, 2021).

References and Endnotes

[1] India, "Title: India a World Leader in Space Technology: Jitendra Singh | Technology News," Google.com, 2011. (accessed Sep. 14, 2021).

[2] Y. S. Rajan, "Development of space technology: Indian experience and future prospects on JSTOR," Jstor.org, 2021. https://www.jstor.org/stable/24094541?read-now=1&refreqid=excelsior%3A6ff997983c9518bd65a5389f5e4e9104&seq=1#page_scan_tab_contents (accessed Sep. 14, 2021).

[3] "Chapter 10. India's Space Enterprise — A Case Study in Strategic Thinking and Planning," Anu.edu.au, 2021. http://press-files.anu.edu.au/downloads/press/p34191/mobile/ch10.html (accessed Oct. 20, 2021).

[4] "vikaspedia Domains," Vikaspedia.in, 2013. https://vikaspedia.in/education/childrens-corner/science-section/space-programmes-of-india#:~:text=The%20Indian%20Space%20Research%20Organisation,formed%20on%20August%2015%2C%201969.&text=Since%20inception%2C%20the%20Indian%20space,transportation%20system%20and%20application%20programmes. (accessed Sep. 14, 2021).

[5] "Joint Operational Access Concept (JOAC)," 2012. Accessed: Oct. 20, 2021. [Online]. Available: https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.

[6] C. Giri, "India's Catalytic Reforms for Space 2.0 Era," 2021. [Online]. Available: https://media.defense.gov/2021/Mar/07/2002595035/-1/-1/1/GIRI.PDF.

[7] "Indian Space programme: 2020 Updates & Priorities Presentation by Indian delegation to 58 th session of STSC -UNCOPUOS Vienna, Austria," 2021. [Online]. Available: https://www.unoosa.org/documents/pdf/copuos/stsc/2021/tech-06E.pdf.

[8] M. Pomerleau, "Here's how new space tech is helping electronic warfare forces on the ground," Defense News, Apr. 13, 2021. https://www.defensenews.com/electronic-warfare/2021/04/13/heres-how-new-space-tech-is-helping-electronic-warfare-forces-on-the-ground/ (accessed Oct. 23, 2021).

[9] M. V. Spreckelsen, "Electronic Warfare – The Forgotten Discipline | Joint Air Power Competence Centre," Joint Air Power Competence Centre, Dec. 13, 2018. https://www.japcc.org/electronic-warfare-the-forgotten-discipline/ (accessed Oct. 23, 2021).

[10] A. Minhas, "Space Weapons: A Rapidly Evolving Threat to South Asian Strategic Balance," 2018. Accessed: Oct. 04, 2021. [Online]. Available: https://ndu.edu.pk/ndu-journal/2018/16-Space-Wpns.pdf.

[11] T. Harrison, K. Johnson, and M. Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons," Csis.org, 2021. https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons (accessed Oct. 04, 2021).

[12] A. Rosner, E. Coyle, and K. Pugh, "Agile Electromagnetic Spectrum Operations," presented at the Agile Electromagnetic Spectrum Operations -Increasing the Agility of Spectrum Maneuver for DoD, Dec. 2020, [Online]. Available: https://disa.mil/-/media/Files/DISA/News/Events/2020-Virtual-Experience/AFCEA_Agile_EMSO_Rosner_Coyle_Pugh_11-3-20_Final_PAO_Approved.ashx (accessed Oct. 20,2021)

[13] K. Atherton, "What's the frequency, Putin? 5 questions about Russia's EW capability," C4ISRNet, Jun. 04, 2018. https://www.c4isrnet.

com/electronic-warfare/2018/06/04/whats-the-frequency-putin-5-questions-about-russias-ew-capability/
(accessed Oct. 27, 2021).

[14] Space Force Washington DC, "Space Capstone Publication: Space Power. Doctrine for Space Forces," DTIC, 2020. https://apps.dtic.mil/sti/citations/AD1129735
(accessed Oct. 27, 2021).

[15] "Global Counterspace Capabilities | Secure World," Swfound.org, 2021. https://swfound.org/counterspace/ (accessed Oct. 27, 2021).

[16] "Российские военные смогут подавлять враждебные спутники с Земли," Interfax.ru, Jan. 04, 2018. https://www.interfax.ru/russia/594392 (accessed Oct. 23, 2021). Translated as "Russian military will be able to suppress hostile satellites from Earth" comments on the Tirada system.

[17] "The Space Review: Russia gears up for electronic warfare in space (part 1)," Thespacereview.com, 2020. https://www.thespacereview.com/article/4056/1
(accessed Oct. 23, 2021).

[18] "The Space Review: Russia gears up for electronic warfare in space (part 2)," Thespacereview.com, 2020. https://www.thespacereview.com/article/4060/1
(accessed Oct. 23, 2021).

[19] Defence Intelligence Agency, "Challenges to Security in Space," January 2019, p. 20, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[20] Kartik Bommakanti, "'Soft Kill' or 'Hard Kill'? The Requirements for India's Space and Counter-Space Capabilities", ORF Occasional Paper No. 224, November 2019, Observer Research Foundation.

[21] China Aerospace Studies Institute, "In Their Own Words: Foreign Military Thought Science of Military Strategy," 2013. [Online]. Available: https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d.

[22] Project 2049 Institute, "China's Evolving Space Capabilities: Implications for U.S. Interests," Project2049.net, Apr. 26, 2012. https://project2049.net/2012/04/26/chinas-evolving-space-capabilities-implications-for-u-s-interests/ (accessed Oct. 24, 2021).

[23] Huang Hanwen, "Conceptual Study on Stealth Satellites [卫星隐身概念研究], Aerospace Electronic Countermeasures [航天电子对抗], June 2010, pp. 22-34.

[24] For space-based electronic reconnaissance systems, see Yuan Xiaokang, "Satellite Electronic Reconnaissance, Antijamming," Shanghai Hangtian, October 9, 1996, pp. 32-37, in FBIS-CST-97-011; and Yuan Xiaokang, "Some Problems of Space Electronic Reconnaissance," Hangtian Dianzi Duikang, March 1996, pp. 1-5, in CAMA, Vol. 3, No. 4.

[25] Pan Changpeng, Gu Wenjin and Chen Jie, "An Analysis on the Capabilities of Military Satellites to Support an ASBM in Offense and Defense Operations" [军事卫星对反舰导弹攻防作战的支援能力分析], 2006, No. 5.

[26] "Challenges to Security in Space." [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[27] V. Samson and W. Office, "Global Counterspace Capabilities: An Open Source Assessment," 2020. [Online]. Available: https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

[28] M. Clay, "To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power - War on the Rocks," War on the Rocks, Jan. 22, 2021. https://warontherocks.com/2021/01/to-rule-the-

invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/ (accessed Oct. 22, 2021).

[29] Office of the Secretary of Defense, "Office of the Secretary of Defense annual report to congress: Military and security developments involving the people's republic of china i," 2020. [Online]. Available: https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-China-Military-Power-Report-Final.PDF.

[30] 张思远, "余志锋：为打赢信息化局部战争冲锋，再冲锋 – 中国军网," Www.81.cn, 2020. http://www.81.cn/201311jxjjh/2020-06/08/content_9830067.htm (accessed Oct. 22, 2021). - Yu Zhifeng, associate professor of the School of Electronic Warfare, National University of Defence Technology an influential scholar warrior is key to the "Development Strategy in the Field of Electronic Warfare".

[31] Reuters Staff, "China denies it is behind hacking of U.S. satellites," U.S., Oct. 31, 2011. https://www.reuters.com/article/us-china-us-hacking-idUSTRE79U1YI20111031

(accessed Oct. 21, 2021) - "At least two U.S. environment-monitoring satellites were interfered with four or more times in 2007 and 2008 via a ground station in Norway, and China's military is a prime suspect, according to the draft report to Congress."

[32] Reuters Staff, "China denies it is behind hacking of U.S. satellites," U.S., Oct. 31, 2011. https://www.reuters.com/article/us-china-us-hacking/china-denies-it-is-behind-hacking-of-u-s-satellites-idUSTRE79U1YI20111031 (accessed Oct. 04, 2021).

[33] TZVI JOFFRE, "U.S. warns of GPS interference, communications spoofing in Persian Gulf," The Jerusalem Post | JPost.com, 2019. https://www.jpost.com/middle-east/us-warns-of-gps-interference-communications-spoofing-in-persian-gulf-597998 (accessed Oct. 04, 2021).

[34] Y. BUTT, “Effects of Chinese Laser Ranging on Imaging Satellites,” Science & Global Security, vol. 17, no. 1, pp. 20–35, Jun. 2009, doi: 10.1080/08929880902864376.

[35] ANI, “China’s eye in the sky: An Analysis of China’s satellite surveillance,” @bsindia, Oct. 30, 2019. https://www.business-standard.com/article/news-ani/china-s-eye-in-the-sky-an-analysis-of-china-s-satellite-surveillance-119103000151_1.html (accessed Oct. 24, 2021).

[36] M. Donovan, “US military must avoid a ‘Kasserine Pass’ failure for space power,” C4ISRNet, Jul. 19, 2021. https://www.c4isrnet.com/opinion/2021/07/19/us-military-must-avoid-a-kasserine-pass-failure-for-space-power/ (accessed Oct. 22, 2021).

[37] AEHF Satellite - N. Strout, “Space Operations Command takes over final AEHF satellite,” Defense News, Dec. 08, 2020. https://www.defensenews.com/battlefield-tech/space/2020/12/08/space-operations-command-takes-over-final-aehf-satellite/ (accessed Oct. 23, 2021).

[38] N. Strout, “Space Force declares operational acceptance of fifth anti-jamming GPS III satellite,” C4ISRNet, Jul. 15, 2021. https://www.c4isrnet.com/battlefield-tech/space/2021/07/15/space-force-declares-operational-acceptance-of-fifth-anti-jamming-gps-iii-satellite/ (accessed Oct. 23, 2021).

[39] “Space Delta 3 focuses on electromagnetic spectrum,” Peterson Space Force Base, Feb. 16, 2021. https://www.peterson.spaceforce.mil/News/Article/2504236/space-delta-3-focuses-on-electromagnetic-spectrum (accessed Oct. 23, 2021).

[40] “Jonathan’s Space Report,” No. 369, August 22, 1998, www.planet4589.org/space/jsr/back/news.369

[41] T. Harrison, K. Johnson, and J. Moye, “April 2021 A report of the CSIS Aerospace Security Project.” [Online]. Available: https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS_Harrison_

SpaceThreatAssessment2021.PDF.

[42] D. Goward, “GPS circle spoofing discovered in Iran - GPS World,” GPS World, Apr. 21, 2020. https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran/ (accessed Oct. 28, 2021).

[43] “ATP 7-100.2 North Korean Tactics Headquarters, Department of the Army,” 2020. Accessed: Oct. 28, 2021. [Online]. Available: https://irp.fas.org/doddir/army/atp7-100-2.pdf. – See Chapter 9 on Electronic Intelligence Warfare (EIW) or chonja chinungjon

[44] Editor, “N. Korea readies deployment of new GPS jamming device / Link to funeral prep - Daily NK & IBT - RNTF,” RNTF, May 2020. https://rntfnd.org/2020/05/01/n-korea-readies-deployment-of-new-gps-jamming-device-link-to-funeral-prep-daily-nk-ibt/ (accessed Oct. 28, 2021).

[45] Dr. Thomas Withington, “Space Savers - Armada International,” Armada International, Sep. 09, 2021. https://www.armadainternational.com/2021/09/space-savers/ (accessed Oct. 23, 2021).

[46] C. Kadib, “Defence launches new project to guard space domain,” Defenceconnect.com.au, Jul. 29, 2021. https://www.defenceconnect.com.au/intel-cyber/8486-defence-launches-new-project-to-guard-space-domain (accessed Oct. 23, 2021).

[47] R. ACT , “Department of Defence,” Defence.gov.au, 2021. https://www1.defence.gov.au/project/wide-area-and-space-surveillance (accessed Oct. 22, 2021).

[48] B. Ho, “The Second Nagorno-Karabakh War: Takeaways for Singapore’s Ground-Based Air Defense,” Air University (AU), Aug. 25, 2021. https://www.airuniversity.af.edu/JIPA/Display/Article/2743721/the-second-nagorno-karabakh-war-takeaways-for-singapores-ground-based-air-defen/ (accessed Oct. 06, 2021).

[49] Admin PSF, “Space Weapons: A Rapidly Evolving Threat to South Asian Strategic Balance (Review) - Pakistan Strategic Forum,” Pakistan Strategic Forum, Jan. 14, 2021. https://pakstrategic.com/2021/01/14/space-weapons-a-rapidly-evolving-threat-to-south-asian-strategic-balance-review/ (accessed Oct. 24, 2021). – Original article written by Ahmed Saeed Minhas, ISSRA National Defence University, Pakistan and available online at https://ndu.edu.pk/issra/issra_pub/articles/ndu-journal/NDU-Journal-2018/16-Space-Wpns.pdf

[50] “India’s Space Security Policy: A Proposal | Manohar Parrikar Institute for Defence Studies and Analyses,” Idsa.in, 2016. https://idsa.in/policybrief/indias-space-security-policy_alele_280416 (accessed Oct. 27, 2021).

[51] “Space ISR in a Contested Environment.” Accessed: Oct. 4, 2021. [Online]. Available: https://www.afcea.org/mission/intel/documents/AFC_FallIntel_WhitePaper_R4.pdf

[52] Shounak Set, “India’s Space Power: Revisiting the Anti-Satellite Test,” Carnegie India, 2019. https://carnegieindia.org/2019/09/06/india-s-space-power-revisiting-anti-satellite-test-pub-79797 (accessed Sep. 14, 2021).

[53] Kapoor, Lt Gen Anil. “Joint C6ISR and Exploitation of Space Domain - A Roadmap to Address the Capability Gaps.” Cenjows.in, CENJOWS, Aug. 2021, cenjows.in/upload_images/pdf/Synergy_%20August%20-2021_Final.pdf. Accessed 23 Sept. 2021.

[54] “Press Release: Space Technology for National Defence | SAMDeS INDIA’S BLOG,” SAMDeS INDIA’S BLOG, Sep. 08, 2021. https://www.samdesindia.in/blog/press-release-space-technology-for-national-defence/?_ga=2.90344670.590392948.1635025414-1598202995.1635025414 (accessed Oct. 23, 2021).

[55] Chethan Kumar, “To counter China, India’s DSA begins scouting for star wars technology,” The Times of India, Feb. 23, 2021. https://timesofindia.indiatimes.com/india/india-begins-scouting-for-star-wars-technology/articleshow/81163698.cms (accessed Oct. 28, 2021).

[56] “Reportlinker’s Space-Based C4ISR Market – Growth, Trends, COVID-19 Impact, And Forecasts (2021 – 2026) – SatNews,” Satnews.com, Mar. 29, 2021. https://news.satnews.com/2021/03/29/reportlinkers-space-based-c4isr-market-growth-trends-covid-19-impact-and-forecasts-2021-2026/ (accessed Oct. 23, 2021).

[57] A. Rosner, E. Coyle, and K. Pugh, “Agile Electromagnetic Spectrum Operations,” AFCEA, Dec. 2020. https://disa.mil/-/media/Files/DISA/News/Events/2020-Virtual-Experience/AFCEA_Agile_EMSO_Rosner_Coyle_Pugh_11-3-20_Final_PAO_Approved.ashx (accessed Oct. 03, 2021).

[58] Lieutenant Colonel Vivek Gopal, “Electronic Warfare Capability: Establishment of Spectrum Warfare Wing and Roadmap for India – Centre for Land Warfare Studies (CLAWS),” Claws.in, Jun. 28, 2021. https://www.claws.in/publication/electronic-warfare-capability-establishment-of-spectrum-warfare-wing-and-roadmap-for-india/ (accessed Oct. 27, 2021).

[59] Vivek Gopal, “Joint Waveform Interoperability System - Common Tactical Data Links for the Force of 21St Century,” Centre for Joint Warfare Studies (CENJOWS), 2021, doi: 10.13140/RG.2.2.23398.55362.

[60] “Global Electromagnetic Spectrum Information System (GEMSIS).” Accessed: Oct. 24, 2021. [Online]. Available: https://www.disa.mil/~/media/Files/DISA/Services/DSO/GEMSISSpectrumCapabilities.pdf

REVOLUTIONIZING THE BATTLEFIELDS OF TODAY & TOMORROW

आज़ादी का अमृत महोत्सव

UNMATCHED FIREPOWER | DEEP PRECISION | ULTIMATE WEAPON SYSTEM

BrahMos
An India - Russia Joint Venture

BrahMos Aerospace
16, Cariappa Marg, Kirby Place, Delhi Cantt., New Delhi - 110010 INDIA
Tel.: +91-11-3312 3000 **Fax:** +91-11-2568 4827
Website: www.brahmos.com **Mail:** mail@brahmos.com