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

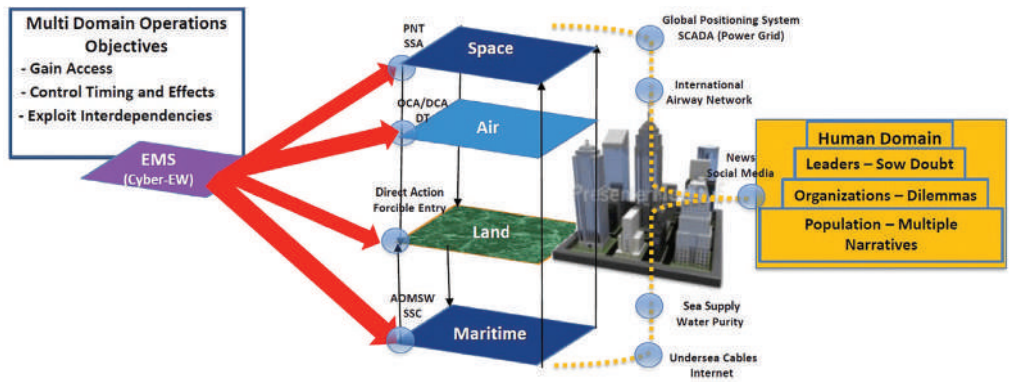
9 Ryo Nakamura and Tsukasa Hadano, "US to strengthen electronic-warfare abilities in South China Sea", Nikkei Asia, 17 July 2020; https://asia.nikkei.com/Politics/International-relations/South-China-Sea/US-to-strengthen-electronic-warfare-abilities-in-South-China-Sea; accessed 26 Dec 2021

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].



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