CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 295 June 2021

# Electronic Warfare Capability: Establishment of Spectrum Warfare Wing and Roadmap for India*

**Lieutenant Colonel Vivek Gopal**, a graduate of the National Defence Academy, was commissioned in December 2000. A MTech, paratrooper & certified Project Management Associate, the Officer is presently posted as Instructor (Class 'A') at a premier training establishment.

## Introduction

History is replete with examples of how Electronic Warfare (EW) has undergone a transition—from the Russo-Japanese War (1904-05) to the present day evolution in terms of cognitive phenomena wherein Artificial Intelligence (AI) and Machine Learning (ML) are being extensively used to make EW more lethal and responsive. EW plays a pivotal role as part of the mosaic warfare and development is bound to happen if nation's leverage its potential within associated fields of radio frequency engineering. EW recently, apart from the domains of traditional frequency ranges— from Direct Current (DC) to Super high frequency, is also associated with incorporating 'never seen before technologies' and is extending into the realms of cyber[1] and space.[2] As far as India is concerned, we have no dedicated EW doctrine,

**Key Points**

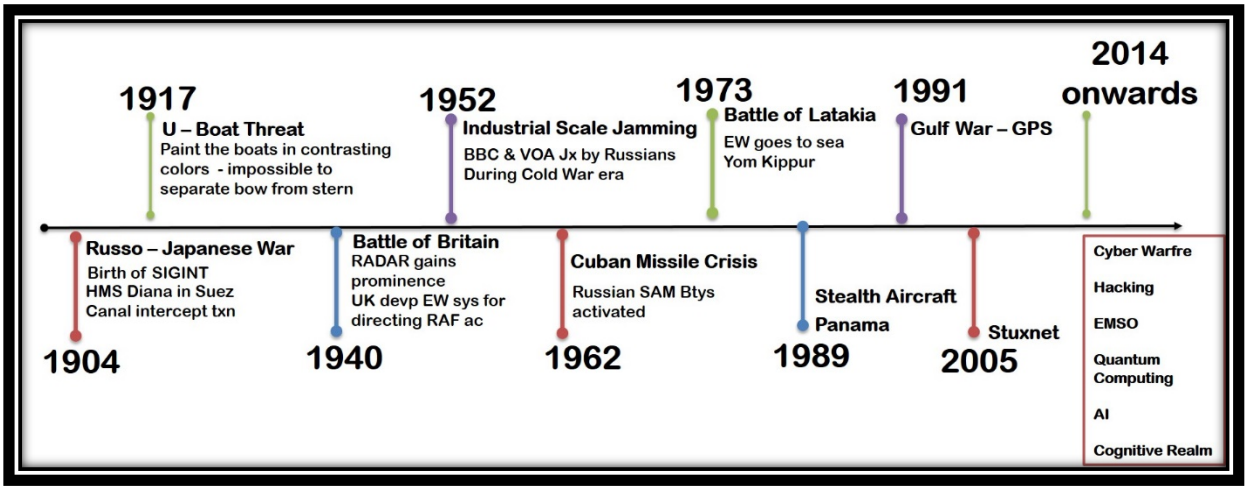
- Spectrum Warfare Wing is the need of the hour for Electronic Warfare assets management and utilisation.
- There is a need for greater in-house and indigenous research & collaborative R&D.
- In-house development of hardware and software followed by validation of technology by using of test beds, should be worked upon.
- Impetus to be laid on Cyber & Space EW convergence.
- Cross-functional teams are the need of the hour to develop better and more potent systems— learn from lessons of conflicts in the recent past.

*Adapted from the author's presentation on EW Systems at Geosmart India National Conference.

although we do have separate doctrines that mentions the EW based scenarios— there is a lack of a unifying thread which connects all these realms together.

The aim of the paper is to recommend the establishment of a 'Spectrum Warfare Wing' under the aegis of the National Security Council Secretariat (NSCS) to serve as the nodal agency to monitor, plan and manage the entire set of activities related to the electromagnetic spectrum (EMS) to include offensive and defensive operations.

**Figure 1: EW Chronology (Important Milestones)**




*Source: Author's own Representation*

**General Overview of EW Development in Some Countries**

EW development has grown steadily in countries such as US, Russia, Turkey, China and India. Some present day developments in EW domain in various countries are mentioned as under:

***India***

Indian Armed Forces have integrated EW systems into deployable entities like Samyukta[3] and Himshakti[4]. However, the gestation period for these technologies requires more resources and time. There is definitely a need to be self-reliant rather than relying on items ex-import.

***USA***

Apart from the recently launched 'Project Convergence'[5] under the US Army Futures Command, the USA is focused on developing EW capability to establish itself ahead of its earlier prime rival— Russia especially with the latter showing its prowess against the Turkish

systems during the Syrian conflict. DARPA† has made substantial effort towards developing AI and ML based EW systems such as Behavioral Learning Adapted for EW[6] (BLADE‡), Cognitive Reasoning and Representation Architecture[7] (CORA). The EW Planning and Management Tool[8] (EWPMT) is also an asset being developed for the commanders to have a real assessment of the battlefield EW scenario. The thoughts echoed by the US Airforce Chief General Charles Brown — "In some aspects, an electron is much cheaper than a very expensive missile"[9], highlights EWs importance for the forces.

***Russia***

The Concern Radio-electronic Technologies (CRET) Group § has produced variety of systems for the Russia covering all frequency bands in addition to the latest cellular technology. Russia surely utilised the Syrian conflict as a test bed for its various EW systems– the prowess to jam the position, navigation and time signals (PNT)[10] to cause a GPS blackout was felt heavily by the adversarial forces.[11] They have also developed substantial capability to thwart damage attempts by Unmanned Aerial Vehicles (UAVs)/ drones by developing systems that have the capability to target satellite communications and UAV ground station links. Estimated 40% of Russian ground forces are expected to be network enabled by 2030.[12] Similarly, there will be about 100 per cent rise in the elite units vis. Special Forces, Spetsnaz GRU, VDV** and Naval Infantry.

**Table 1: Snapshot of Russian Army and Airborne EW Systems**

| System Name | Estimate of Frequency Coverage | Probable Purpose |
|---|---|---|
| Krasukha-C4 (1RL257) | 8.5- 18 GHz | Jam airborne radars in X (8-12 GHz) and Ku (12 to 18 GHz) bands |
| Zhitel (R -330Zh) | 1-1.6 GHz | GNSS jamming |

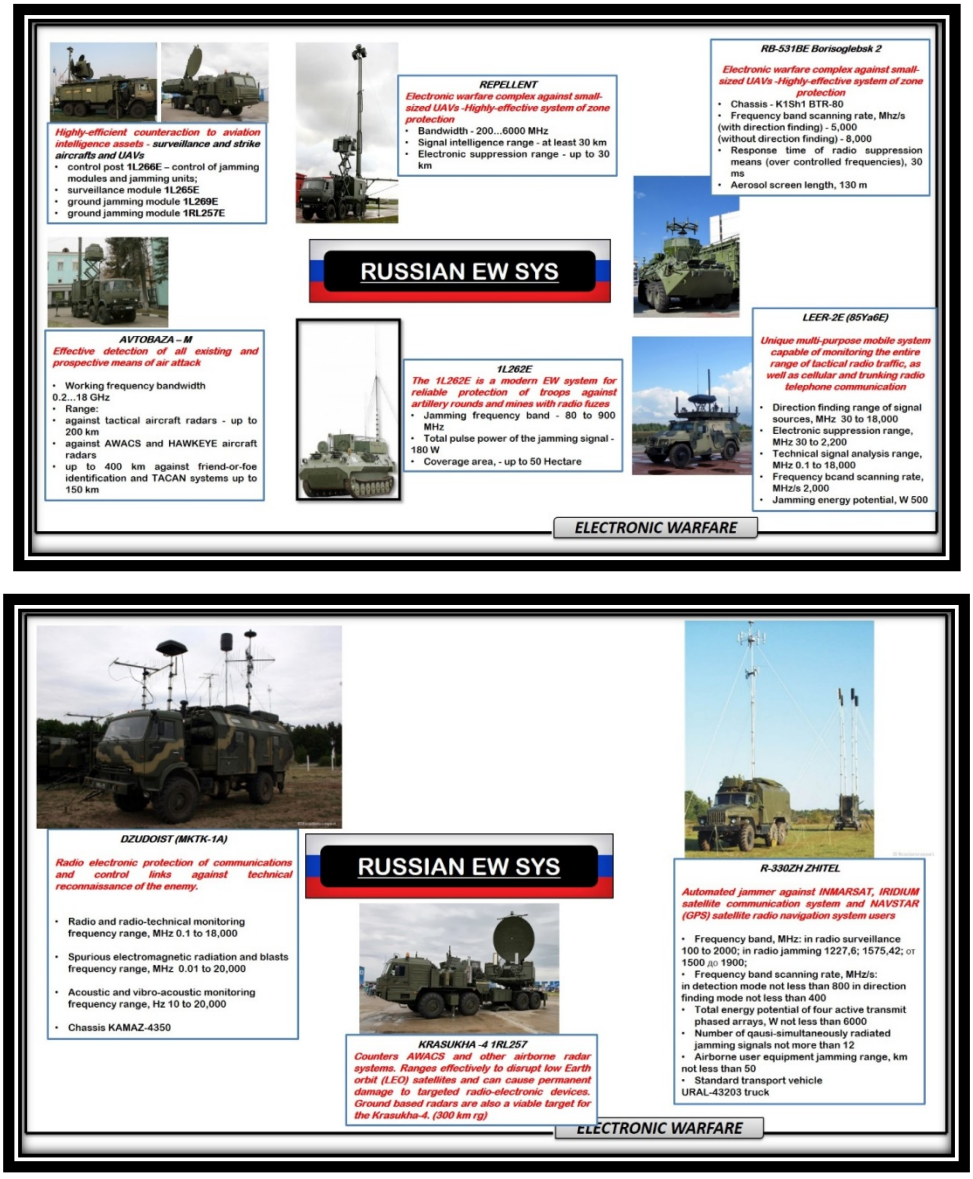
† DARPA: Defensed Advanced Researched Projects Agency (US)
‡ The Behavioral Learning for Adaptive Electronic Warfare (BLADE) program is aimed at developing the capability to counter new and dynamic wireless communication threats in tactical environments.
§ Concern Radio-Electronic Technologies (KRET) is a holding company within the Russian state-owned Rostec group that develops and manufactures military specialised radio-electronic, state identification, aviation and radio-electronic equipment, multi-purpose measuring devices, detachable electrical connectors and a variety of civil products.
** The Russian Airborne Forces or VDV (from Vozdushno-desantnye voyska Rossii)

| | | |
|---|---|---|
| Leer- 3 (RB 314V) | 0.8-2 GHz | Anti-cellular networks |
| Khibiny (L-175V/VE) | 2-18/40 GHz | Airborne ELINT installed on the Su-30 and 35 aircrafts |
| Borisoglebsk-2 (RB-301) | 30 MHz- 3 GHz | V/UHF COMINT |
| Repellent-1 | 300 MHz – 6 GHz | Anti-UAV and control links of UAVs |
| Lorandit (RP-377LA) | 3 MHz – 3 GHz | Location of H/V/UHF emitters and COMINT |

*Source: https://www.iiss.org/publications/the-military-balance/military-balance-2020-book/military-use-of-the-electromagnetic-spectrum*

Russia also possesses the A-100 “Premier” airborne early-warning and control aircraft equipped with active phased array radar (APAR) which can reportedly enable effective targeting of cruise and even hypersonic missiles. The Rtut-BM mobile EW complex, is specifically designed to protect troops and military hardware from artillery rockets and shells. Zaslon-REB (Barrier-EW) communication security system (COMSEC), is specifically designed to protect the information space and the area of operations (AOO) of the Russian Armed Forces and Tirada-2S is used for SATCOM jamming. Some details of the EW systems in use along with their capabilities in condensed form is shown pictorially in Figures 2 below. Additionally, they have also developed nuclear powered satellite based EW capability.[13]

**Figure 2: Overview of Russian EW Systems**




*Source: Author's own Representation*

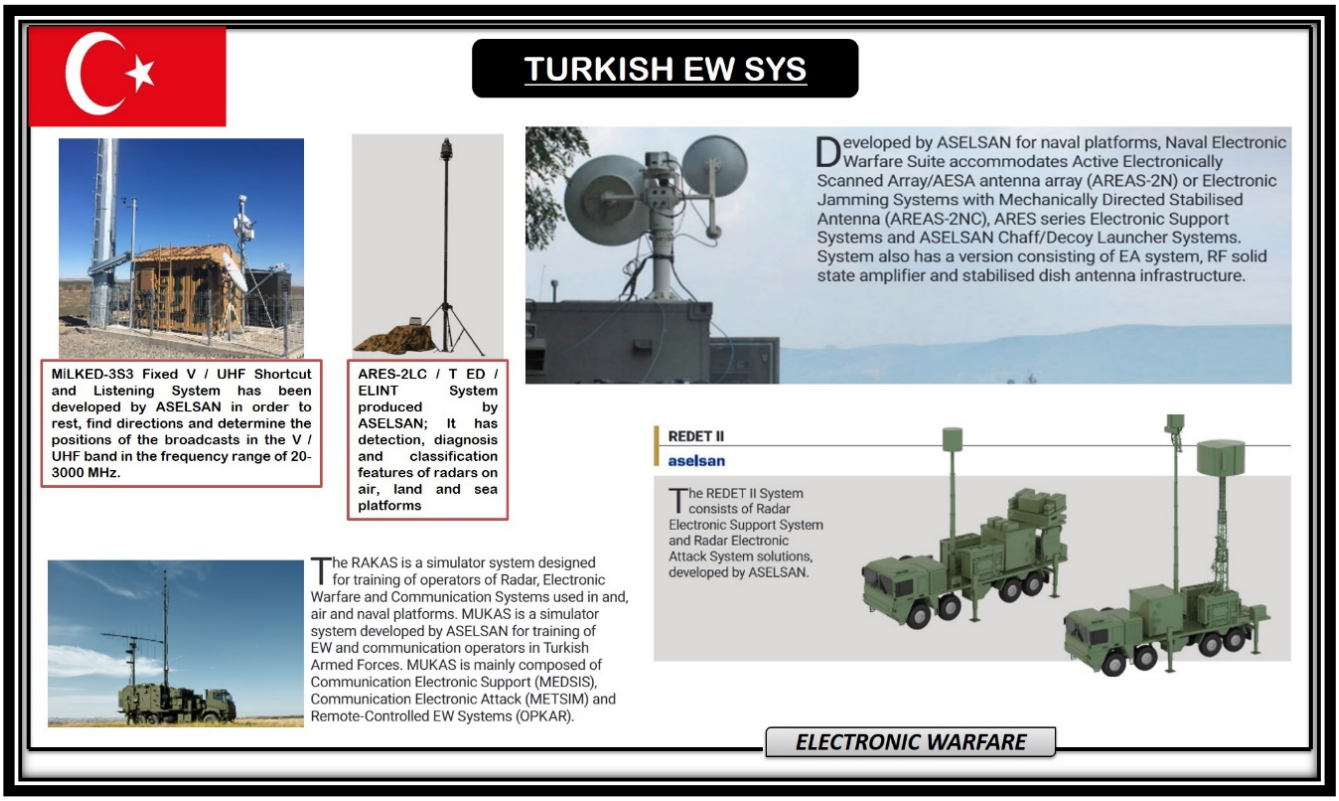
***Turkey***

The REDET II, RAKAS, MILKAR and KORAL are few of the well-developed EW suites by Aselsan†† which proved their prowess against the Syrians.[14] Turkey is also making similar

†† "***As***keri ***El***ektronik ***San***ayi, *Military Electronic Industries* . is a Turkish defence corporation headquartered in Ankara, Turkey.

progress with respect to UAV and drone warfare. A condensed snapshot of the Turkish EW systems is shown in Figure 3.

**Figure 3: Snapshot of Turkish EW Systems**




*Source: Author's Own Representation*

***China***

Apart from the expansionist tendencies exhibited by the Dragon from time to time, the focus of the PLA towards 'Intelligentisation' as a graduated upward move from 'Informatisation', as laid down in the grand vision for the country, is taking shape. The launch of various satellites to complete its constellations apart from reverse engineering systems obtained by indirect means and thereafter tailor making it to suit the requirement, is noteworthy. The restructuring of the 3rd and 4th General Staff Department (GSD) and grouping it under the PLA Strategic Support Force (PLASSF) displays the importance being given to EW as a force multiplier. The PLA's game plan, as per a study conducted by the Jamestown Foundation,[15] is divided into four principles and stages: -

- Gather one's strengths and advantages to achieve a superior starting position;

- Pursue multi-level integration;
- Employ precise release of energy; and
- Demonstrate effects in multiple areas. The fourth and final stage is the most important one in securing victory, and is the main focus for majority of EMS stratagems.

**Figure 4: Dongfeng EQ2050E 4x4s of the PLAGF seen at a parade in Beijing likely configured for EW missions**


*Source:https://mags.shephardmedia.com/Digital_Battlespace/2018/DB0118webmagwim/pubData/source/DB-01-18-webmag.pdf*

## Conflict Paradigm and Strategic Imperatives for India

The growing importance of EW needs to be viewed under the present day conflict paradigm. Pertinent points which merits mention are:

- ***Enlargement of the spatial dimension.*** This comprises of the geographical indeterminacy of theatre of operations– where and how the adversary will strike, has become even more complicated. Also, the technology to deliver chaos and destruction has made geographical boundaries irrelevant, if not redundant.
- ***Transformation of the temporal element.*** Simultaneous multiplicity of points of interaction with forces on a broad front, thereby compelling one to fritter the resources.
- ***Concurrent acceleration and deceleration of engagement.*** This results from the simultaneity of operations and feigning/ deception at the strategic level.

- ***Mutation of the belligerents' identity.*** The categorisation of participating factions as combatants or civilians has become fuzzy. The present day conflicts eradicated the 'thin boundary' between military and civil targets.
- ***Systemisation within asymmetric warfare.*** There is some amount of systemisation within asymmetric warfare and orderliness in execution is being seen within the framework of asymmetry i.e. greater synchronisation between participating elements.
- ***Militarisation of Civilian Assets.*** Civilian assets are being weaponised and 'pure military-like' assets have ceased to exist. Warfare has thus become 'all encompassing'.
- ***New Manoeuvre Space.*** Specifically, with reference to EW**,** the spectrum is treated as a manoeuvre space.
- ***Being Offensive.*** There is a need to shift more to being offensive especially in the EW domain, as staying in the defensive role will entail a lot of 'catching-up' to do which will ultimately prove unaffordable.

The above picture of warfare, as it is seen today, entails certain strategic imperatives for us. The importance of EW, as an inseparable part of future warfighting, has already been reinforced during the Syrian conflict. Apart from the conventional ascendancy over the adversary, why EW development is paramount can be listed as:

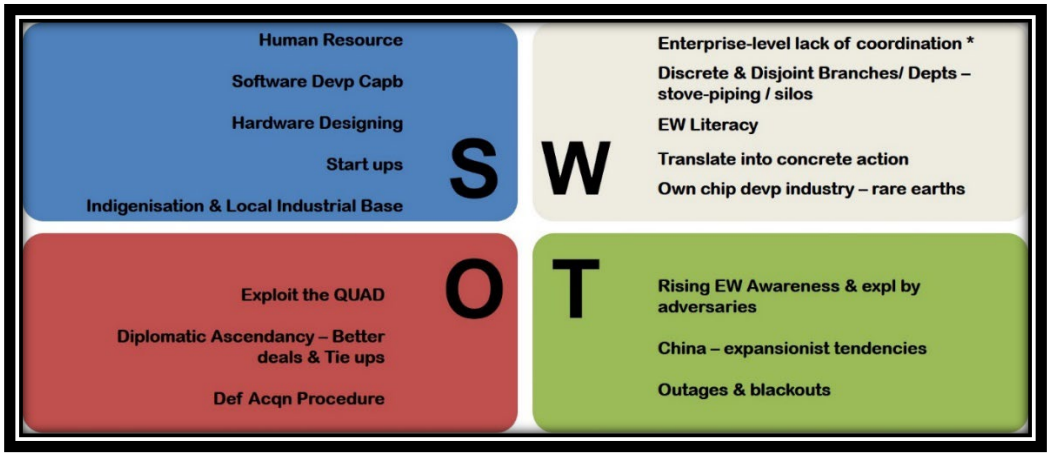
- ***Multi- Domain Operations.*** Grey Zone conflicts will be the norm and importance of Algorithm Warfare will need to be understood by all being ubiquitous.
- ***Influence Operations will gain primacy.*** In the ever evolving threat landscape, there will be a need to address this issue with greater deliberation as shaping of the battlefield will be preceded by shaping of one's opinion, which would be based on what one transmits and what one receives.
- ***Growing convergence between Cyber – EW domains.*** Both these domains cannot be considered as independent to one another. While EW will entail operations pertaining to optimum utilisation of the spectrum, cyber will augment these efforts by means of smart algorithms and machines to perform this task.
- ***Establish spectrum dominance.*** Overall adversarial destruction *a priori* main operations– moral and psychological ascendancy over the adversary, can be attained by offensive EW operations.

- ***New Threat Vectors.*** Drones and counter drone systems as primary threat vectors has emerged in the recent years. These systems can be employed for both, offensive and passive role in EW. Simultaneously, cyber-physical systems can be used to deter any large sale attack on account of this threat.
- ***Force projection.*** As was witnessed during the First Gulf War and the recent Syrian conflict (2011 onwards that lasted over a decade), EW serves as a means to project power. Strong EW systems gives a head start to the opposing force in any scenario.
- ***Attack Surface Widened.*** With greater reliance on networked elements (Network Centric Warfare) and advanced satellite communication systems, widened attack surface has emerged, therefore, command and Control (C2) has become vulnerable like never before.

**SWOT Analysis**

Before recommending policy level changes, there is a need to view the strengths and weaknesses of the present day system. It is only then, that we can afford to recommend policy changes. The SWOT analysis with respect to the converged domains of Cyber-EW-Space can be seen as the schematic given below.

**Figure 5: SWOT Analysis- EW system Development**




***Absence of a holistic, overarching EMS operational concept**

*Source: Author's own Representation*

**Policy Recommendations**

In the backdrop of a freshly emerging conflict paradigm and strategic imperatives, certain policy level changes are mandatory. The recommendations are based on providing impetus to EW and its emergence as a game changer for the future battlefield.

- ***Need for an Exclusive and All-inclusive EW Doctrine.*** While there exists a dedicated Land Warfare as well as Joint Warfare Doctrine, exclusivity is yet to be given to EW on similar lines. In the backdrop of the Cyber Command and parallel 'theaterisation process', the EW Doctrine should jointly address ELINT, COMINT (SIGINT) in addition to the space segment at not only the tri-services level, but also with other National level agencies, thereby helping achieve an actionable picture on a grand scale.

- ***Spectrum Warfare Wing.*** A Spectrum Warfare Wing should be established to look into the EMS operations at the national level. It should focus exclusively on joint concepts *ab initio*. Inputs from various intelligence and space related organisations should be fed into this group to help in developing a 'Joint Macro-level picture' (DIARA + Tri-services Intelligence agencies + DIPAC + DIA + IB + NTRO).

- ***Civil – Military Fusion.*** In order to get an accelerated progress, Public-Private Partnership (PPP) as well as civil-military fusion is compulsory. Stakeholders should include academia, research facilities/ laboratories and the private players.

- ***Establish EW Test Ranges.*** These ranges will not only help to test EW equipments, but also establish an environment to validate EW concepts. It is also mandatory for validation of concepts under EW degraded environment. All EW resources alongwith cyber and space capabalities could be grouped at the theatre level.

- ***Bilateral and Multilevel Collaboration.*** We need to hold joint training and exercises to garner new concepts and establish collaborative effort if the need arises. Leveraging the QUAD for such an aim will be profitable against expansionist tendencies of China in the South China Sea.

- ***Focus on monitoring and countering cellular bands.*** There has been an increase in the use of private LTE/ 5G networks in the military. Targeting the conventional VHF/ HF / UHF bands in the tactical battle area, will need to be changed.

- ***National Waveform Development.*** Protected Tactical Waveform will be a necessity in times to come; with its inherent advantages against eavesdropping, it will enable easier collaborative effort for the forces.
- ***Reverse Engineering.*** When compared with systems being developed concurrently by other leading nations, we are a few notches behind. Following the Chinese principle, it will be beneficial to reverse engineer products and thereafter pursue mass production. Albeit time consuming, we might end up having some technology spin-offs (by-products) which might be used in other sectors. While 'Make in India' has its advantages, reverse engineering developed technologies might in the end help save time by preventing us re-invent the wheel.
- ***Dedicated Institutions.*** We need to have dedicated organisations which can think, design, plan, progress and implement all facets of the EMS. Think tanks, research organisations such as Indian National Defence University, need to be established on a fast track basis.
- ***Validation of Concepts.*** There is an immense requirement of training our forces under an EW degraded environment. Jointly, even better. There is an ever growing need to harness the potential of AI and ML.
- ***Development of EMS Operational Assets over Land, Air and Sea.*** We should not only address the joint capabilities offered by the EMS assets on land, air and sea, but also address the cyber and space elements. The market is looking at open source/ 'modular and scalable systems' vis. Open VPX/ VPX architecture.
- ***Prototyping Timelines.*** Accelerate development and deployment of Advance Technology thereby reduce prototyping timelines.

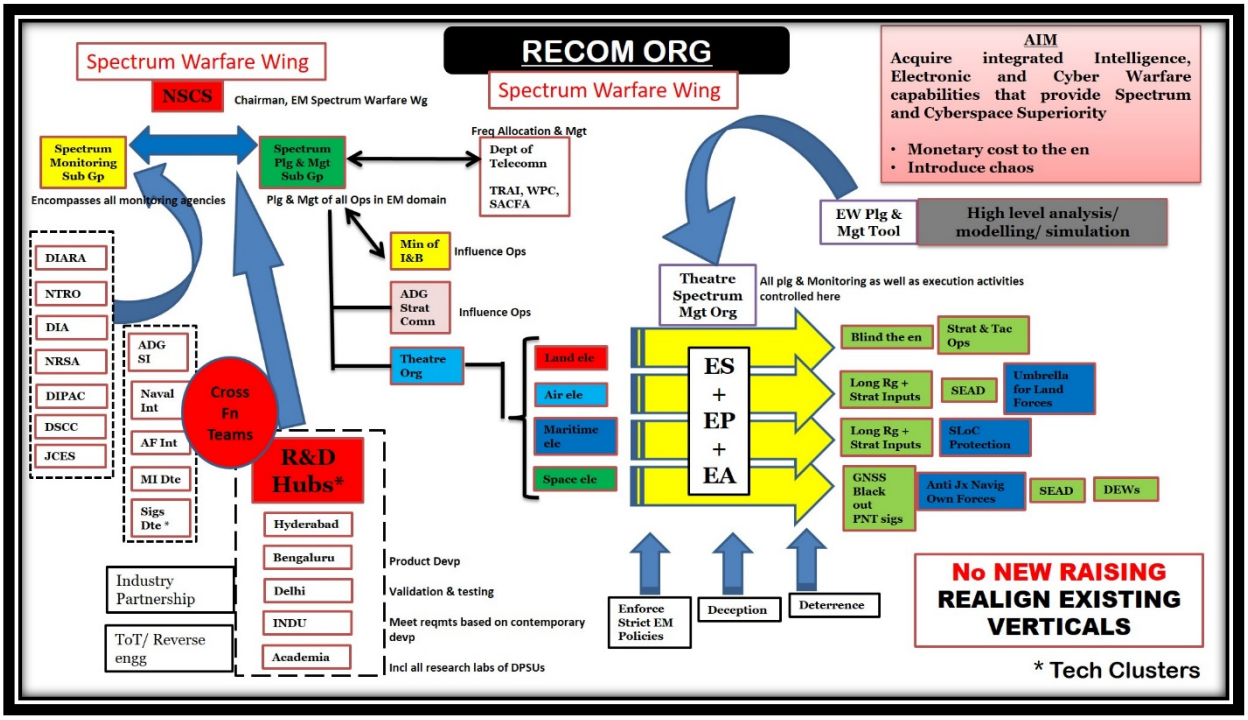
**Intra and Inter Organisational Rehash: Re-alignment of Existing Verticals**

Having seen the strategic imperatives and making a prognosis of conflict scenario, we need to realise these concepts on ground to see the actual implementation. For the singular aim of establishing a Spectrum Warfare Wing, the proposed wing will be divided into two sub agencies — Spectrum Monitoring Sub Group and Spectrum Planning & Management Sub Group.

- Spectrum Monitoring being the key aspect of EMS operations, should include developing an overall picture/ scheme based multiple input servicing agencies.
- The definition of EW will not be limited to the conventional radio spectrum i.e. VLF/HF/VHF & UHF only. Based on the inclusion of Cyber, DEWs, Radiation Weapons as well as intelligence inputs, the Monitoring Sub Group will be mandated to monitor all aspects of the spectrum.
- Inputs to the Monitoring Sub Group will be based on reports generated by the agencies as under.
    - DIARA[##] for monitoring cyber activities.
    - NTRO[§§] for data gathering and processing, cyber security, cryptology systems, strategic hardware and software development and strategic monitoring.
    - DIA, IB, RAW for helping in developing an overall threat assessment based on HUMINT in turn contributing towards the corroboration of details revealed by the spectrum analysis.
    - The Joint Communication Electronics Staff (JCES) alongside the Wireless Planning Commission (WPC) and Standing Advisory Committee on Radio Frequency Allocations (SACFA), should ensure that relevant frequencies are monitored and relevant inputs fed to the Spectrum Monitoring Sub Group.
    - NRSA, DIPAC & DSCC for corroboration of facts, filling in the details of newly perceived setups as seen through hi-resolution satellite images. This will help us allocate resources for spectrum monitoring and therefore activity detection and forecasting.
    - ADG SI and Wireless Experimental setups can help serve inputs of long range intercepts. With focus of countries reverting back to High Frequency secure communication, a need is felt to surveillance the otherwise considered 'backup' frequency band.
    - Tri-services Intelligence Directorates needs to be established with the Department of Military Affairs (DMA) as the nodal agency.

[##] Defence Information Assurance and Research Agency (DIARA).
[§§] National Technical Research Organisation (NTRO).

**Figure 6: Recommended Organisation of the Spectrum Warfare Wing**




*Source: Author's own Representation*

- The Spectrum Planning and Management Sub Group should base its actions, both offensive and defensive, on the inputs and analysis as given by the Monitoring Sub Group.
    - To shape the psychological domain of the nation, the execution of the tasks will include relevant portions of the Ministry of Information & Broadcasting, TRAI, WPC.
    - Influence operations should be taken care of by the Additional Director General (ADG) Strategic Communication by accelerated use of social media and offensively also collaborate on activities by the newly established Cyber Command.
    - The last mile delivery of defensive and offensive options should be delivered by the Theatre Spectrum Management Organisations. With 'theaterisation' in mind, theatre level organisations will entail the convergence of all theatre assets vis. land/sea /air/ space and cyber. The combined might of these resources shall be pooled in to shape the battlefield as well as extend the battlespace, thereby breaking any

typical settings and creating chaos for the adversary. Being offensive will certainly reap greater benefits.

- Suppression of enemy air defences/SEAD, Blinding the enemy, GPS blackout— are all examples of offensive defence which can play havoc for the adversary.
- An EW Planning and Management Tool will should be made available at all theatre level Commands to view, analyse and forecast the EW battlespace. This will help in judicious and optimal utilisation of the EW resources in a theatre.

- Civil-Military fusion is an important aspect for capability development of EW resources.

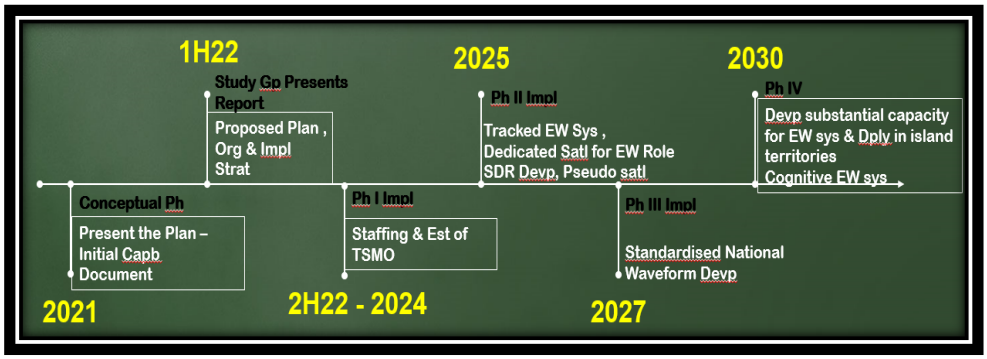
Technology clusters are being envisaged in cities such as Hyderabad, Bengaluru which are beaming with electronic and software industry. This will also include the interaction with private players, startups as well as academia. DRDO labs will also be included within its ambit. The Indian National Defence University when established will also cater to providing valuable research inputs towards technology harvesting and strategising in this field.

Being offensive and keeping pace with technology in the domain of EW is key to maintaining a strong upper hand of the adversary in addition to tacit power projection.

As no new accrual of organisation is foreseen and the plan involves a re-arrangement of verticals, the proposed organisation and plan is seen as being implemented in a time frame of 10 years as part of vision 2030 with augmented facilities and systems.

The proposed timeline is shown by the schematic (Figure 7) below.

**Figure 7: Tentative Timelines to Achieve Establishing a Spectrum Warfare Wing**




*Source: Author's own Representation*

**Table 2: Tentative milestones and Timeframe of Implementation**

| **Milestone** | **Projected Benefits/ Results** | **Timeframe and manner of Implementation** |
|---|---|---|
| Providing an Initial Capability Development Document | This document will help to streamline the mandate of the Spectrum Warfare Wing and lay down the charter of duties and mechanisms to collaborate and collate information related to the EMS. | To be implemented by December 2021 under the NSCS. |
| Proposed plan and its implementation | | First half of 2022/ June 2022. |
| Staffing of the Wing and its 'Theaterised' sub-organization. | While the Spectrum Warfare Wing will serve at the apex, its counterpart in the context of theaterisation will be the Theatre Spectrum Management Organisation (TMSO) | To be established by December 2024 |
| Development of tracked EW capability, Space based EW weapons including pseudo-satellites. | Matching mobility suited to the terrain and forces deployed on the Western & Northern front. Space based EW weapons will help is address a wide area of operations. | December 2025 |
| Proposed development of a National Waveform | Having a uniform classified/ secretive waveform will ensure interoperability within the operating elements as well as lead us to be less susceptible to interception or the adversaries cyber/ EM operations. | December 2027 |
| Development of Cognitive systems leveraging AI/ML. | Self-sufficiency in development of own EW suites. Less prone to or subject to interference by adversary. | December 2030 |

*Source: Author's own Representation*

## Conclusion

The traditional definition governing EW has metamorphosed. It now includes the domains of Direct Energy Weapons (DEW), Anti-radiation Weapons (ARW), Cognitive EW as also Spectrum Management owing to the explosive growth of civilian broadcasts and frequencies

in the environment. Use of space to develop space related EW has also seen a major boost in the recent years. Novel methods are being developed to network sensors leading into the realm of Internet of Things (IoT) which will rely extensively on radio waves for communication. Also, there is a growing convergence between the cyber and EW domains. The use of drones (including swarms─Unmanned Aerial Systems or UAS) for offensive and defensive actions are being witnessed every day. The control of this essential facet is hence, of paramount importance─ the one who can control this spectrum can control the outcome of any situation.

## End Notes

[1]Jabu Mtsweni, "Cyber Warfare 4.0 Meets Electronic Warfare: Opportunities and Implications", *CSIR (Presentation)*,6-8 November 2017. Accessible at https://cdn.ymaws.com/www.crows.org/resource/collection/523B3578-3F15-4120-AF50-6EE2426CA715/Dr_Jabu_Mtsweni_-_Cyber_Warfare_4.0_meet_Electronic_Warfare.pdf. Accessed on 10 June 2021.

[2] Massimo Annulli, "Space EW", *Emsopedia*. Accessible at https://www.emsopedia.org/entries/space-ew/. Accessed on 10 June 2021.

[3] "Programme Samyukta" , *Defence Research and Development Organisation –(DRDO), Ministry of Defence, Government of India*, 2019. Accessible at https://www.drdo.gov.in/programme-samyukta. Accessed on 10 June 2021.

[4] Bulbul Singh, "Indian Army EW Programme" *Battlespace*, 13 October 2013. Accessible at https://battleupdates.com/update/indian-army-ew-programme/ Accessed on 10 June 2021.

[5]"Project Convergence" *Army Futures Command* 19 January 2021. Accessible on https://armyfuturescommand.com/convergence/. Accessed on 12 June 2021.

[6]Behavioral Learning for Adaptive Electronic Warfare (BLADE), *DARPA*. Accessible at https://www.darpa.mil/program/behavioral-learning-for-adaptive-electronic-warfare. Accessed on 12 June 2021.

[7] Stephen Lee-Urban, Ethan Trewhitt et al., "CORA: A Flexible Hybrid Approach to Building Cognitive Systems", 2015, *Semantic Scholar*. Accessible at https://www.semanticscholar.org/paper/CORA-%3A-A-Flexible-Hybrid-Approach-to-Building-Lee-Urban-Trewhitt/313ffe6ff3a8b4d6d5b71205839134f996b8806d . Accessed on 13 June 2021.

[8] "Raven Claw Augments Battle Management for Electronic Warfare Operations". Accessible at https://www.army.mil/article/199368/raven_claw_augments_battle_management_for_electronic_warfare_operations. Accessed on 13 June 2021.

[9] Mark Pomerleau, "Air Force Chief: Electromagnetic Spectrum Could Be Cheaper Option to Defeat Enemies".*C4ISRNET*. 28 January 2021. Accessible at https://www.c4isrnet.com/electronic-warfare/2021/01/27/air-force-chief-electromagnetic-spectrum-could-be-cheaper-option-to-defeat-enemies/. Accessed on 13 June 2021.

[10] Roger McDermott, "Russia's Electronic Warfare Capabilities as a Threat to GPS". *The Jamestown Foundation*, 10 March 2021. Accessible at https://jamestown.org/program/russias-electronic-warfare-capabilities-as-a-threat-to-gps/. Accessed on 13 June 2021.

[11] Jonas Kjellén,"Russian Electronic Warfare:The role of Electronic Warfare in the Russian Armed Forces", *September 2018*. Accessible at https://www.foi.se/rest-api/report/FOI-R--4625—SE. Accessed 14 June 2021.

[12] Roger McDermott, "Tracing Russia's Path to Network-Centric Military Capability". *The Jamestown Foundation*, 04 December 2020. Accessible at https://jamestown.org/program/tracing-russias-path-to-network-centric-military-capability/. Accessed on 15 June 2021.

[13] Bart Hendrickx, "Ekipazh: Russia's Top-Secret Nuclear-Powered Satellite", *The Space Review*, 07 October 2019. Accessible at https://www.thespacereview.com/article/3809/1. Accessed on 15 June 2021.

[14] "How Turkey Won the Electronic Warfare Battle against Syria in Idlib", Defenseworld.net, 02 April 2020. Accessible at https://www.defenseworld.net/news/26643/How_Turkey_Won_the_Electronic_Warfare_Battle_Against_Syria_in_Idlib#.YK_qi6gzbVg. Accessed on 15 June 2021.

[15] Zi Yang, "PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of 'the Winning Mechanisms of Electronic Countermeasures", *The Jamestown Foundation*, 01 February 2019. Accessible at https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/. Accessed on 15 June 2021.



**CENTRE FOR LAND WARFARE STUDIES (CLAWS)**
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com
Website: www.claws.in