CHINA'S ELECTROMAGNETIC SPECTRUM DOMINANCE CAPABILITIES AND CHALLENGES FOR INDIA

Brig (Dr) R K Bhutani (Retd)*

Abstract

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

Introduction

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

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its use of information technology was well behind the curve; and its nominal space capabilities were based on outdated technologies for the day.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

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

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

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

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

3 Ibid.

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

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

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

CHINA'S ELECTROMAGNETIC SPECTRUM DOMINANCE STRATEGY AND OPERATIONAL CONCEPTS

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

4 Ibid.

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

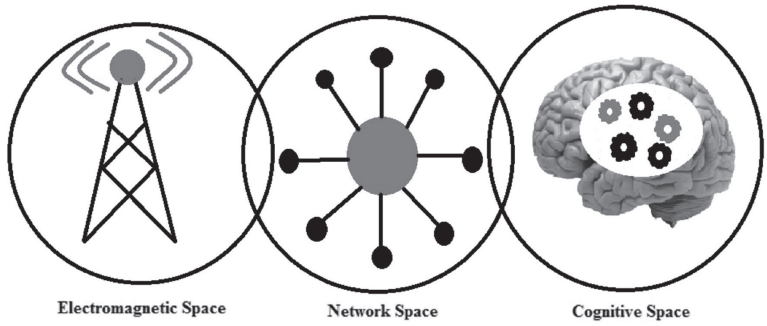


Figure 1: Network Electromagnetic Space

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

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

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

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

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

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

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

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

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

Operational Concepts

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

10 Ibid.

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

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

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

ORGANISATION, FORCE STRUCTURE AND CAPABILITIES

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

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

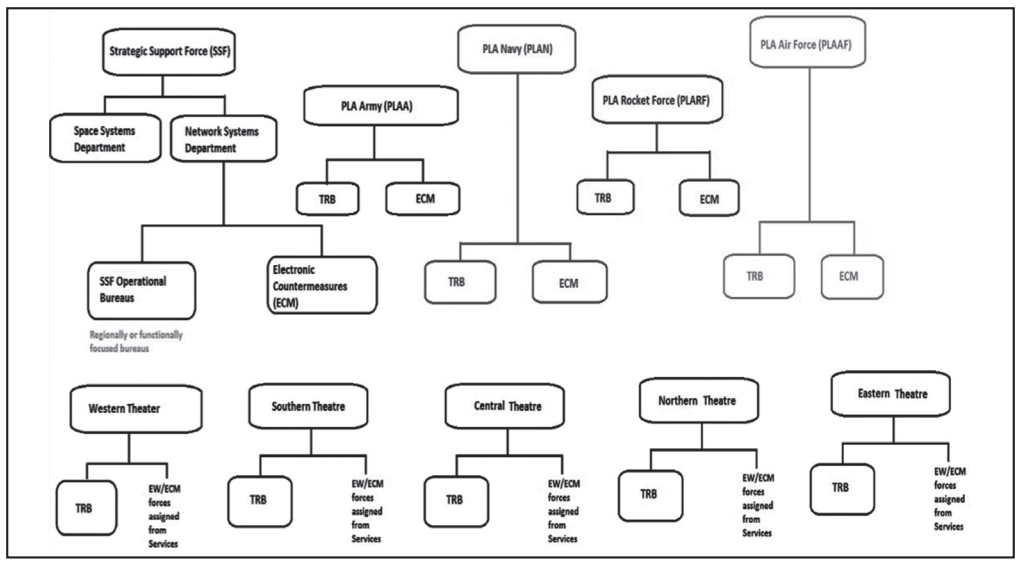
Electronic Countermeasures Units to conduct EW operations;[12] and

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

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

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

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



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

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

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

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

Capabilities

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

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

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

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

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

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

(a) Use of systems like multispectral decoys;

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

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

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

(e) Hardening against HPM effects.[18]

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

Priorities for Future Developments

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

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

18 Ibid.

19 Ibid,. p.23.

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

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

CHALLENGES FOR INDIA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  - PLA adopts frequency diversity that allows it access to the

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

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