CLAWS

ISSN 23939729

NO. 110

2025

MANEKSHAW PAPER

PLA Electronic Warfare Capabilities, Its Growing Relevance and Implications on India

Abhishek Acharya

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Photographs courtesy: The Manekshaw family/FORCE

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 110, 2025

PLA Electronic Warfare Capabilities, Its Growing Relevance and Implications on India

Abhishek Acharya

Centre for Land Warfare Studies
New Delhi

KW Publishers Pvt Ltd
New Delhi

Editorial Team : CLAWS

ISSN 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91-11-25691308 Fax: +91-11-25692347
email: landwarfare@gmail.com; website: www.claws.co.in
CLAWS Army No. 33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore, may not be quoted or cited as representing the views or policy of the Government of India, or the Ministry of Defence (MoD) (Army), or the Centre for Land Warfare Studies.

www.kwpub.in

Published in India by

Kalpana Shukla
KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: +91 11 43528107 email: kw@kwpub.in • www.kwpub.in

Contents

PLA Electronic Warfare Capabilities, Its Growing Relevance and Implications on India

Executive Summary

- The paper attempts to analyse all the information available on China's Electronic Warfare (EW) capability in the open domain, some printed publications and discussions with important stake holders in the field. It attempts to analyse how EW is merged with the much more recognised Cyber Warfare. A bit on rationale for China to invest heavily in this domain like the Russians to counter the US Military by hitting at its vulnerabilities. The paper brings out the structure of EW organisation within the Cyber Space Force (CSF) from highest level to the lowest, and how the reforms of 2015 and 2024 have aligned it to be more integrated with the theatre commands and all service HQs. The paper illustrates an analogy to give a fair idea of the role of Information Support Force (ISF) by comparing its functioning with similar Indian military organisation at the apex level. It brings out the concept of operations of the EW assets at the theatre level emphasising on the Western Theatre Command (WTC) involving inter-say relationship between Technical Reconnaissance Bureau (TRB) and the tactical EW formations orbated to the theatre, Corps and Brigades (Bde).
- The paper highlights China's capabilities in EW in the most contested South China Sea to monitor and influence the Electro-Magnetic (EM) spectrum of its neighbours. Most importantly, how the EW is playing a key role in redefining the character of military conflict sighting lessons from the current Russia-Ukraine War and its implications on our Northern Borders.
- It highlights on China's capability to apply EW drones to blind our Air Defence radars at Vulnerable Points and Areas (VA & VP) and thus enabling effective Suppression of Enemy Air Defence (SEAD) Operations for successful Counter-Surface operation by PLAAF. Therefore, there is a requirement to increase scale of own Drone Jammers, Spoofers and Anti-Drone rifles. It highlights vulnerability of own Army tactical

communication infrastructure in forward areas of Northern Borders to the combined effect of PLARF, Artillery and EW, there by denying any means of rearward and lateral communication for Battalion (Bn) and downward. Therefore, there is a requirement to conduct training in a realistic EW environment and employ frequency hopping sets with higher hopping rates than Chinese Jammers. Also induct light vehicle-based Jammers to give matching mobility to own forces in high altitude terrain.

Key Findings

- The ISF can be compared to the Corps of Signals less the EW Bdes and Bns in IA parlance. ISF is responsible for providing secure and reliable communication to all HQs of PLA from CMC to the last of PLA Bns deployed in forward areas. It is responsible for integrated data flow among all the four services and four arms of the PLA. Unlike own Corps of Signals, the Head of ISF now comes directly under the Central Military Commission (CMC). This highlights the level of priority the CMC gives to scrutiny, monitoring and protection of information. The digitisation, automation and integration of data allows direct scrutiny by CMC and anti-graft departments on all confidential information available with the military formations. This will enable better control by Chinese Communist Party, which is known to post political commissars at all important levels.
- To assist the PLA theatre Commands in their campaign planning and operations, they have been provided with TRBs and EW/Electronic Counter Measures (ECM) Bdes. The role of TRBs is in the intelligence domain and of ECM bdes is in the operational domain. While the TRBs are the central repository of all the electronic information on enemy radios, radars, and drone frequencies and its terrain specific application in the theatre of operation on ground, air and in sea domain. The ECM bdes are expected to utilise this repository for carrying out tactical operations of Jamming and deception based on the direction of joint operational department on the enemy.
- The Western Theatre Command (WTC) is controlling the four Army TRBs, which were earlier under the Military Regions (MR) of Chengdu and Lanzhou. There are five known Army subsidiary offices of TRBs operating closer to its border. The PLAAF and PLAN respective TRBs are also expected to operate with the respective theatres where they are co-located. The 2nd PLAAF TRB was located at Chengdu and is expected to continue with its operations along with its 13 known sub offices in WTC. Each Combined Corps (CC) and the Combined Arms Bde (CAB)

has been provided with a dedicated EW coy like in the Russian Army. In addition, there is an EW Bn in every Air Def Bde of the CC envisaged for counter drone operations.

- The economics of warfare has led to "Drone Warfare" as the most cost-effective means to carry out precession strike against enemy. EW has emerged as the most effective means to counter drone due to its dependence on the EM spectrum. The successful invasion of Crimea in 2014 is attributed to skilful integration of drones and EW by Russian military. This was possible because Russia had invested heavily in EW post the Gulf War as an Asymmetric means to counter US superiority in Network Centric and precession warfare. The Chinese seems to have developed similar capabilities to counter US forces as can be seen by the similarities of the EW assets available to both countries at theatre and bde level.
- PLA's expertise in manufacturing drones in large scale at affordable cost gives it a huge scope to apply EW drones in mass scale for Suppression of Enemy Air Defence (SEAD) operation for prolonged periods. Thus, enabling favourable conditions for fighter bomber aircrafts to carry out degradation on own Vulnerable Areas and Points (VA) and (VP) to include Air field and Naval Ships
- PLA has developed enormous EW assets at the seven Islands of the SCS to dominate the EM spectrum, thereby denying same to the contending countries. Chinese media have been boasting openly of EW success achieved by PLAN over superior US capabilities in SCS by quoting two incidences in past one year.
- The Army OFC based communications in mountains at the forward areas is vulnerable to PLARF and Artillery degradation as a result of terrain constrains. The alternative available mobile communications and secondary means as Radio Relay (RR) are prone to Kinetic degradation. Secure satellite communication is also prone to PLA space-based jamming or kinetic means. This brings the last secured means of communication i.e. the Radio in the ambit of PLA EW. PLA has dedicated EW coys at bde level in addition to dedicated coys at Combined Corps as reserves. Therefore, it is imperative that own forces will face electronic degradation through jamming and deception operations during the escalatory matrix and conflict. This will deny our ground forces bde and downwards any reliable means of rearwards or lateral communication. Therefore, PLA has the capability to impart Electronic Isolation to our forces by jamming at key battle areas via its large EW assets available to it at the theatre, Corps and Bde level.

Introduction

The PLA in their endeavour to find an asymmetric edge over US in Non-Contact warfare has been building capabilities in Electronic Warfare (EW) domain since early 2000. The effort now seems to pay dividends when during the recent EW confrontation between the two forces put the US forces on the receiving side. Chinese media highlighted two successful PLA EW operations over US forces during a period of seven months. The first one was in SCS in Dec 2023[1], where a US commander of the EW Attack Squadron from an Aircraft Career fleet was removed from comd[2] and the second one was the withdrawal of US fleet from the northern Philippines water under intense EW Jamming by Chinese Navy for 12 hrs degrading its ship communication and navigation means in July 2024.[3] A report published by the US-China Economic and Security Review Commission (USCC) of 2024 has mentioned that the PLA has developed 'substantial' Electronic Warfare (EW) to 'detect, target, and disrupt' the US militaries command and control communication links in the Indo-Pacific during the possible Taiwan Strait conflict. Beijing expected Washington to field unmanned submarines, surface ships, aerial drones, and precision-guided munitions to target PLA forces as per its 'Hellscape' strategy.[4]

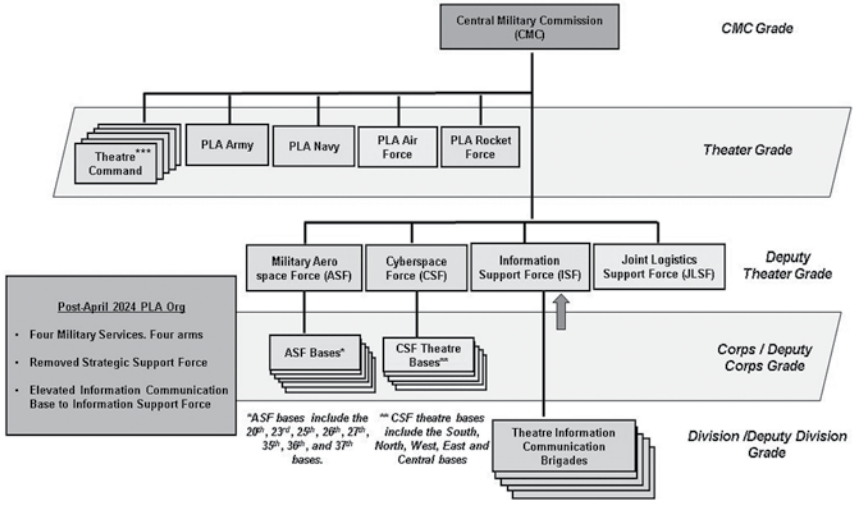
PLA EW strategy is deeply integrated into its joint operations, providing support across all military domains.[5] It had adopted a formal IW strategy in early 2000[6] called the 'Integrated Network Electronic Warfare (INEW) that consolidates the offensive and defensive missions for both Computer Network Attacks (CNA) and Electronic Warfare and considers both under the Cyber domain. CNA or network warfare includes those activities that target enemy computer information systems, software, hardware, and their associated networks. Network attack differs from electromagnetic attack in that it is conducted digitally and through networks, rather than through the electromagnetic spectrum. EW highlights suppressing enemy's radio or radar communication by employing high energy electro-magnetic waves, there by damaging his capability to carry effective command and control, coordinating its operations and affecting its ISR and precession strikes by radar, drones and GPS guided systems. The present research paper brings out PLA's EW capabilities.

Background to Electronic Warfare in the PLA. Before the 2015 reforms leading to the formation of erstwhile PLA Strategic Support Force (PLASSF), the EW, Cyber Network Exploitation (CNE) and Radar assets were divided among the 3rd PLA and 4th PLA department under the erstwhile General Staff Department (GSD) of CMC. The Cyber and EW in defensive and intelligence collection role or also termed as Signal Intelligence (SI)

was under the 3rd PLA department and the Electronic Offensive assets and the Radar department were with the 4th PLA department.[7] During the 2015 reforms both offensive and defensive assets were brought together and referred as the Network System Department (NSD) under the erstwhile PLASSF. The NSD and the Space System Department (SSD) along with the Information communication base constituted the erstwhile PLASSF.[8]

Reforms on PLASSF in April 2024. The reforms removed the overarching authority of PLASSF and made the three subordinate organisations independent and directly under the Central Military Commission (CMC). These three independent organisations are now renamed as the Cyber Space Force (CSF), Aerospace force (ASF) and the Information Support Force (ISF). They along with Joint Logistic Support force work as the four arms of the PLA. These four arms along with the four services i.e. Army, Navy, Airforce and Rocket force constitute the PLA as shown in Figure 1 below.[9]

Figure 1: Post-April 2024 PLA Organisation



*** Theatre Information Communication Bdes, CSF theatre bases and elements of PLAA, PLAN and PLAAF have dual Command of theatre commanders and respective Service and Arms heads.

The PLASSF commander was equivalent to the theatre/services commanders. These, now independent commanders of the three forces are one rank below theatre/service level.

Information Security Force (ISF). To understand their functioning, the role of ISF can be compared to the Corps of Signals less the EW brigades (bdes) and batallion (bns) in the Indian Army parlance as it is responsible for safe and secure transmission of information in PLA. The Corps of Signals is responsible to provide secure and reliable communications (voice & data) among all the HQs of Indian Army, right from the IHQ MoD (Army) to every Bn spread in the country. With the present reforms, the head of the ISF can be compared to the DG of Corps of Signals in IA parlance, accept that he is directly under the Joint staff department of the CMC equivalent to the MoD in India. This highlights the level of priority the CMC gives to scrutiny and protection of information. The digital automation and integration of data allows direct scrutiny by CMC and anti-graft departments on all confidential information available with the military formations. We are aware that the Communist Party of China ensures a tighter control on PLA by posting political commissars at all important levels, this centralized scrutiny will further enhance their control. The EW Bdes and Bns allotted to IA Commands can be compared to the respective ECM bdes, which are operationally under the PLA theatre commands as field forces, but also under the CSF control.

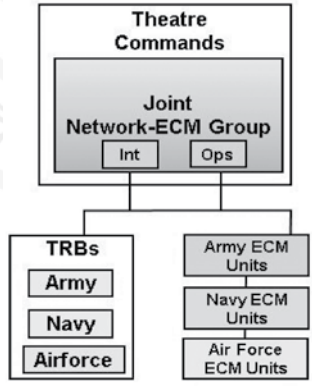
Cyber Space Force (CSF). The role of CSF may be compared to the joint role of Signal Intelligence (SI) department and Cyber Agency department of the Armed Forces of any country. These are joint service organizations, where SI units are deployed all over the border areas for electronic surveillance. China's CSF has a major composition of Cyber Network Exploitation (CNE) units, i.e. the twelve operational bureaus, the Beijing North Computing Centre (BNCC), most of these bureaus are located in Beijing itself. Further CSF possesses the science and technology equipment Bureau controlling Research institutes responsible for computing, sensor technology and cryptography located in Shanghai, Beijing and Tianjin and three more research institutes comprising the 56th, 57th and 58th operating the three respective domains as above.[10] These units were erstwhile under the 3rd PLA department under GSD. The 2nd and 6th operational bureau under CSF are known to carry out Computer Network Exploitation (CNE) against English speaking and South-SE Asian Countries respectively. Therefore, India falls in the ambit both the bureaus. The pre 2000 yrs saw the 3rd PLA department, mainly constituted the SI units like own SI, as the era of internet had not been prevalent. Post the internet revolution, the CNE became a dominant means to collect intelligence over the adversaries. The CSF in addition has been allotted with **one Air Def ECM brigade and one ECM Bde** ex 4th PLA department, envisaged as central reserve collocated at Beijing.[11]

Justification of removal of PLASSF HQ. The reason to remove PLASSF commander, who was at power with the other theatre/service commanders seems to give a hint for a requirement of better assimilation the CSF, ISF and the Aero Space Force (ASF) as their commanders are one rank below theatre commander. This will assist in better integration with services and theatres by eliminating the perceived self-centered bureaucracy with in the HQs of PLASSF. Further, there is a requirement of the ISF to infuse better interoperability among the four services and the five theatres in terms of integration of their communication and computer networks. Also this gives a higher degree of freedom to the three arms to compete for resources for further development among other services and arms from the CMC.

Theatre Command, Combined Corps/Group Army & Combines Arms Bde level

Before the PLA reforms, every army centric Military Region (MR) and the PLAAF and the PLAN had minimum one Technical Reconnaissance Bureau (TRB) and one ECM Bde/Regiment each responsible for carrying out Cyber and electronic operations.[12, 13, 14] The Central and Southern Asia (India) Centric erstwhile Chengdu and Lanzhou MR had two TRBs each. These two MRs have merged to establish the WTC, so it is envisaged that all four PLAA TRBs are under the CSF of WTC. PLAAF is allotted one TRB each at Beijing, Nanjing and Chengdu. PLAAN is allotted one TRB each at Beijing and Xianmen. These are explained at **Appendix A**. Post reforms, the disposition and role of these organaisations are assessed below.

Figure 2



Concept of Operations as Envisaged. EW assets available to the Theatre Command is given at **Figure 2**.[15] The EW during operations

involves control of the electromagnetic spectrum for enabling its effective employment for own military purpose and denying the same to enemy. To enable this, there is a requirement of continuous electronic reconnaissance of the enemy deployment during peace time across the border. **This task is envisaged to be carried out by the theatre-based Army/Airforce/ Navy TRBs, which are assumed to be the central repository of all the electronic information on enemy radio, radar, and drone frequencies and its terrain-based application in the specific theatre of operation in ground, air and in sea domain**. To achieve this, the TRBs are also expected to carry out Cyber Network Exploitation (CNE) on the neighborhood country like the Operational TRBs under the CMC in order to gain maximum info on Cyber vulnerabilities which can be exploited in the escalatory matrix to conflict. **The Army/Airforce/Navy ECM bdes are expected to utilise these repositories of information from TRBs and carry out Jamming and Deception operation to degrade own use of electromagnetic spectrum for effective functioning of own radio communications, radar, drone and satellite operations based on the operation planned by joint operational department.** The elements of ECM Bdes may also be employed to generate electronic int at tactical level, however to maintain confidentiality of these offensive assets, their tasks may be limited in peace times.

Command and Control. The erstwhile, Chief of Staff (COS) of the HQ MR's/PLAAF/PLAN were controlling the respective TRBs and the erstwhile 3rd department under CMC were issuing them policy guidance and general int collection and report tasking.[16] Therefore, in the present reforms, they are envisaged to be dual controlled, i.e. under CSF for policy guidelines and general reporting however operationally under the Theatre command.[17] Therefore, the CSF will exercise the technical control and the theatre command exercises the operational control. This fact was further substantiated during the PLA 90th Anniversary parade in 2017, where there was display of elements of an ECM formations from Army Air Defence Bde and an Army Division ECM dets, which were from the PLA units for display[18] and these were other than the regular and more talked about PLASSF vehicles displayed in the parade. **Further, in consonance with their role, the TRBs are envisaged to be under the intelligence department and the tactical ECM formations under the operational department of the Theatre Command**.

Implication of the Concept at Western Theatre Command. As brought out above, the Western Theatre Command (WTC) has four Army TRBs and two ECM regiments based on the erstwhile Chengdu and Lanzhou

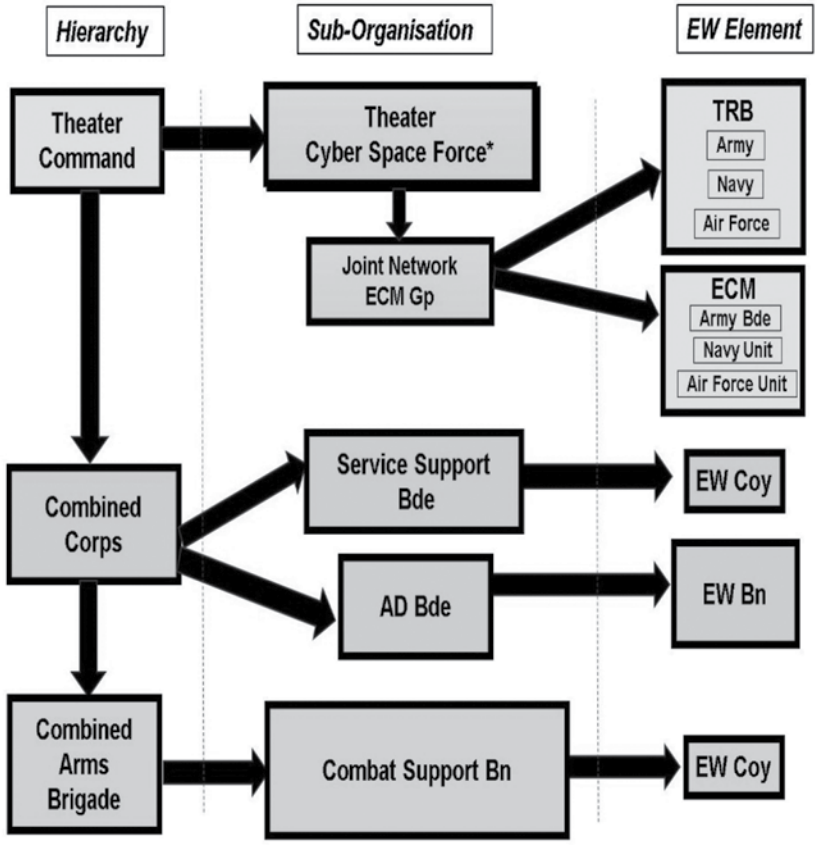
MRs. These TRBs were located at Chengdu, Kunming, Lanzhou and Urumqi with some of their known subsidiary offices located closer to border[19] as shown at **Appendix A**. The units are expected to continue operating post the reforms. Every theatre command is grouped with minimum one Army ECM Bde[20], the WTC is envisaged to have three army ECM bdes. This is assessed on the bases of merger of two MRs and WTC holding the largest geographical frontages as compared to other theatre commands. One ECM bde each is appreciated to be allotted to XMD & TMD[21] in addition to its inherent ECM bde at WTC HQ. The PLAAF TRBs are located at Beijing, Chengdu and Nanjing. The Chengdu TRB is appreciated to operate under WTC. It monitors the Air activity and Air Def Communication along China's southwestern, western and northwestern borders. There are no inputs of Naval TRB located in WTC**. It is appreciated that TRBs are passive defensive means to collect Cyber (network and electronic) intelligence and therefore under the intelligence department at theatre level. The ECM assets are trained and exercised for EW offensive as per the operational plan envisaged and hence they are envisaged under the operational department.** The Joint Network ECM group as a coordinating agency at CSF theatre level coordinates between the TRBs and ECM assets. The EW assets below theatre level at Combined Corps (CC) and Combined Arm Bde is given in subsequent paras.

Service Support Brigade at CC Level. Each Combined Corps (CC) is having six supporting Bdes, i.e. Artillery, Air Defense Aviation, SOF, Engineer and the Service Support Bde. The Service Support Bde for each CC serves the purpose of providing logistics, communication, medical, Repair, Unmanned Aerial systems (UAS) and EW support and have respective Units earmarked for the same purpose[22, 23] as explained in diagram-I at **Appendix B**. The EW Coy is appreciated to have elements as explained at diagram-II at **Appendix B.**

Combat Support Bn at CAB Level. Every **Combined Armed Brigade (CAB)** is appreciated to have four to six combined arm battalions (bn) along with five support bns to include Recce bn, Arty bn, Air Def bn, Combat Support Bn and Service support bn.[24] The combat support bn possesses the Engineer and EW component. Each Combat support bn is grouped with an engineer company (coy), command and communication coy, chemical defence coy, defense and security coy and electronic warfare coy as shown in the diagram-3 at **Appendix B**.

EW Organisation in PLA at Theatre and below Elements in each of the hierarchy from Theatre to CAB is given at **Figure 3**.

Figure 3: EW Organisation in PLA at Theatre and below



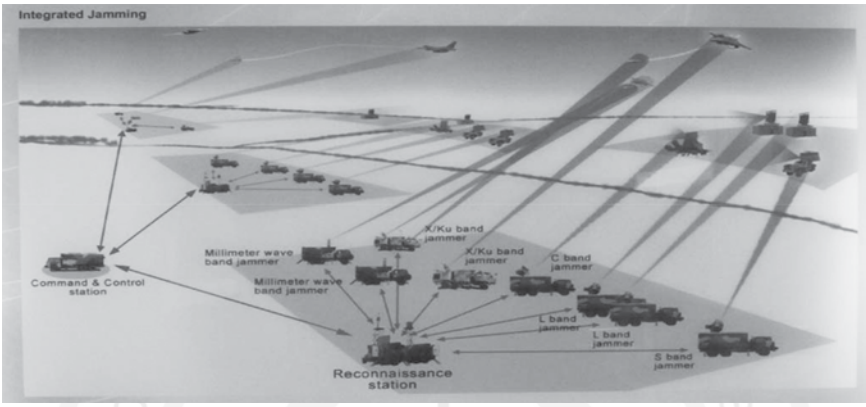
Predominance of EW in Counter Drone Operations. Having discussed the EW inventory available to PLA and its conventional role, it is important to bring out EW's predominance in countering the most emerging military technology i.e. the 'Unmanned Aerial Systems' (UAS). The emergence of drone warfare is a defining factor in the current Russian-Ukraine war. The successful invasion of Crimea in 2014 is attributed to skillful integration of drones and EW by Russian military. However, as the war of 2022 commenced, Ukraine was able to learn lessons and by end of 2023, had contracted 300,000 drones and had projected a requirement to produce 1 million drones for 2024.[25] Its developing its own drone warfare and EW capability rapidly to counter the Russian Military.[26] The drones have demonstrated precession, attrition and lethality at much lower cost to exchequer. An average drone

cost about 400-500 compared to an unguided arty shell whose cost had increased to 8000$ from 2000$ due to increase in demand during the War to Ukraine.[27] Considering large scale employment of drones in war as it's the most viable and cost-effective means for precession strike, It is appreciated that it will be employed in masses scale in a war scenario on this sub-continent. The relevance of EW against drone warfare lies in the limited means available in the conventional inventory of Air Defence forces to counter drones. As observed in Op-Zafran, post Balakot airstrike, the conventional AD was not completely effective nor was an economically viable option to counter drones. The Chinese personal from the 77th Combined Corps accepted the difficulty of shooting down drone swarms as the shells achieved 40 per cent attrition in August 2024.[28] Drone Spoofers and Jammers in the EW domain have proved effective in counter drone operations, further EW rifles which are much lighter with limited range of 3- 5 Kms have also become popular with Ukraine in the war. Ukraine increased its drone rifles from mere dozen in the beginning of war to qty 100 in the first year and further to 1000 in the second year ensuring minimum two rifles in every Inf bn. The importance of EW to counter drones can be envisaged from the knowing the fact that every PLA Air Defence Bde is allotted an EW Bn.[29] **Appendix C** illustrates the methodology of intercepting a UAS by Drone Jammers.

Development of EW as Asymmetric Capability by Russia and China. Chinese importance to EW can be envisaged from the Russian EW capability. Russia in order to counter the US's integrated communications, precision strike capability and target a perceived NATO's general dependency upon GPS and satellite technologies have invested heavily in EW.[30] In practice, the Russian ground forces, and to a lesser extent airborne and Naval Infantry have dedicated EW companies, Bns, and Bdes. While the EW Bdes are capable of fulfilling operational and strategic objectives, each Russian maneuver brigade has a dedicated EW company with tactical capabilities as illustrated at **Appendix D**.[31] **It can be inferred that each Bde of Russia has a dedicated EW asset against aircrafts, drones, IED, enemy radios, radars, mobile and satellite communication**.[32] Comparatively little is known about PLA EW equipment, especially its 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'.[33] The state-owned China Electronics Technology Group Corporation (CETC) displayed a graphic at a recent arms exhibition showing the notional composition of ground based EW. While this graphic is generic as shown at **Figure 4** below, depicts an EW command and control vehicle communicating with EW reconnaissance

stations that feeds information to individual specialised jammers, each covering a different part of the electromagnetic spectrum. Individual jammers are shown creating interference in the millimeter wave band, X/Ku band, C band, L band, and S band in support of an air defense mission.

Figure 4



PLA Ground and Air EW Capability in SCS. An assessment of PLA EW assets deployed on the seven islands in the South Chian Sea (SCS) as on 2020 itself gives an understanding on the emphasis on EW by PLA to deny the EM spectrum to any of the claiming countries and controlling it for its own benefit. These capabilities include a diverse array of specialised mobile ground based vehicles as explained above, deployed on the island. Fixed signals intelligence facilities include sites that may be used to monitor, locate, or jam foreign satellite signals and an High Frequency Direction Finding (HFDF) site that enhances the PLA's regional HF triangulation capabilities. The EW coverage by ground based elements in SCS is given at **Appendix E**.[34] This coverage is **vastly enhanced** by employing EW on air platforms like the Y-9JB, Y-8G and follow up Y-9LG transport aircrafts as given in **Appendix E.** The fighter aircrafts deployed to the island reef airfields may also carry KG600 or KG800 jamming pods for electronic attack/standoff jamming missions. Chinese Unmanned Aerial Vehicles (UAVs) like the Wing Loong are also capable of carrying jamming pods or signals intelligence packages. China has swiftly improved its EW systems after failing to track US military aircrafts during US American politician Nancy Pelosi to visit Taiwan. The reverses experienced by US by Chinese EW offensive in SCS this year as brought out earlier seems to be by product of lessons learnt during her visit, where PLA has invested heavily on airborne standoff ISR and Airborne Early Warning and Control Systems (AEW&CS).

Implications For India

Implications on Northern Borders. One of the aims of EW ops is to deny effective use of electromagnetic spectrum by enemy. Own Indian Army tactical communication from Corps HQ to Bn HQ is based on Optical Fiber Cable (OFC). In comparison to planes of western or southern theatre where the cables are optimally underground, the OFC/copper cable deployed in forward bn HQs and bns are over ground at many places due to terrain constraints. There is also a higher degree of coordination required between Border Road Organisation (BRO) and formation signals, when constructing/ repairing a road. Considering, the overwhelming fire power available to PLA in terms of PLARF and Artillery, these cables are highly susceptible to destruction. The specialised lineman capable to repair in time are limited. The satellite communication can be hampered by PLA space jamming capability. Further the Radio Relay (RR) meant for bde HQ and 'upwards' communication is co-located with HQ location and is vulnerable to damage as the HQs is expected to be targeted in the initial phase of attack. Therefore, the tactical communication will be likely to be opened up on radio. The radio will be vulnerable to interception and jamming by the overwhelming EW capability available to PLA as discussed above. This will invariably lead to electronic isolation of own forces at Coy/Bn or even at Bde level at critical periods for extended duration. Considering China's expertise in EW drone, he shall have the capability to negate the screening effect in electronic offensive operations in mountains. Therefore, it is recommended that dedicated funds be allotted for ensuring complete undergrounding of OFC, allocate blasting resources from engineers to limit the vulnerability to electronic attack and ensuring a higher degree of coordination between the BRO and formation signals during road construction/repair.

Implications in Air and Naval Domain. Air and Sea based communications are purely on radio and hence has much higher vulnerability to EW systems. China's capability to detect, decode and suppress enemy signals has been enhanced by incorporating AI and that has challenged the US hegemony in EW for decades and has been demonstrated in SCS. Thus, their capability to degrade own electromagnetic depended radars, UAS and missile makes us vulnerable to Suppression of Enemy Air Defence (SEAD) operations. The affordability of massed scale employment of drones can effectively prolong the SEAD period, enabling free movement of fighter bombers to carry out degradation task and also freeing their commitments from EW task. A prototype of CH-7 Unmanned Combat Aerial Vehicle (UCAV) was displayed in China Airshow exhibition in Zuhai, Guangdong Province in November 2018 will be able to carry out Jamming payload across

the border to carry out SEAD.[35] Similarly, advancement in their defensive EW capabilities in terms of AI enabled Air Defence radars will make own SEAD operations much difficult.

Conclusion

EW has emerged as a critical domain in the modern warfare. PLA has invested heavily in this field to asymmetrically challenge the US domination in military operation by developing capabilities to hit its vulnerabilities that is US network centric communications, ISR and GPS enabled precession strike operations. Towards this the employment of these non-contact warfare force multipliers with arty/PLARF degradation can effectively electronically isolate own forces at Bde and downward level thereby denying any backward or lateral communications in the Northern Borders. Further effective SEAD operations by employing EW drones can enable smooth degradation by PLAAF. Therefore, it is imperative to induct SDRs with higher hopping rates to minimize effect of jamming and carry out training of troops in realistic EW environment during every operational alert exercise. Increase scale of drone jammers and spoofers to minimum one each per brigade with dedicated manpower for carrying out effective anti-drone operations.

Notes

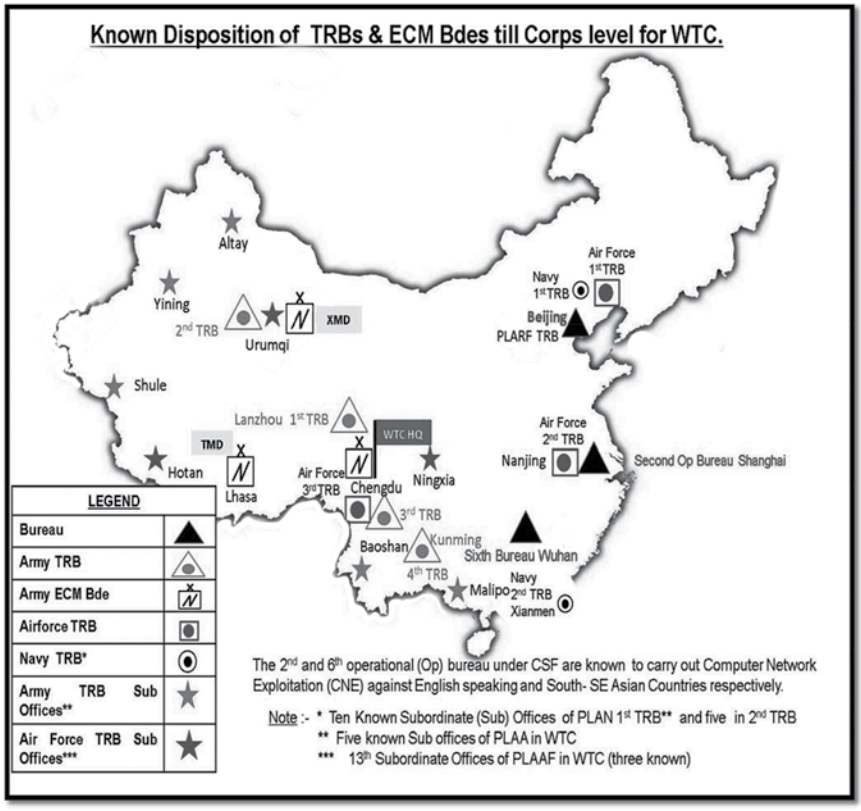
1. The Chinese had claimed that their type 055 destroyers equipped with sophisticated advance AI enabled radar jamming system was able to out manoeuvre the capabilities US advanced EW fighter the EA-18G (F-18) Growler operating from USS Carl Vinsom Aircraft Career. This is a pivotal component of the US Air Sea Battle strategy.
2. China's electronic warfare surge shocks US in South China Sea by Gabriel Honrada Asia Times, 18 July 2024, https://asiatimes.com/2024/07/chinas-electronic-warfare-surge-shocks-us-in-south-china-sea/7dec2024.
3. Chinese and U.S. Navies Engaging in Intense EW Battles Near Philippines. Military watch 22 July 2024, https://militarywatchmagazine.com/article/navies-electronic-warfare-battles-philippines 7 December 2024.
4. US report warns PLA EW could pose 'significant challenge' in Taiwan Strait, SCMP, 20 November 2024, https://www.scmp.com/news/china/military/article/3287227/us-report-warns-pla-electronic-warfare-could-pose-significant-challenge-taiwan-strait. Accessed on 7 December 2024.
5. China's electronic war plane made to dominate South China sea, 2 September 2024, *Asia Times*, https://asiatimes.com/2024/09/chinas-electronic-war-plane-made-to-dominate-south-china-sea/. Accessed on 7 December 2024.
6. Integrated Network Network Electronic warfare, Chinas new concept of Information warfare, Vol. 4, No. 2, April 2010, Journal of Defence studies IDSA.
7. China's strategic support forces: A force of new era, Centre for study of Chinese Military affairs. Institute of National strategic studies National Defence University. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf /. Accessed on 7 December 2024.

8. James down foundation on ISF China Brief, Volume 24, Issue 9, April 26, 2024. https://jamestown.org/wp-content/uploads/2024/04/CB-V-24-Issue-9-April-26.pdf
9. Ibid.
10. Maj Gen PK Mallic, Chapter IV, Organisations dealing with Cyber domain, China in the Cyber domain, Print Publication Pvt Ltd.
11. Figure 5, The Strategic Support Force and future Chines Information Operations, Elsa B. Kania and Jhon K. Costello chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf
12. n. 10.
13. Chapter 10, Pg 357, The Biggest Loser in Chinese Military Reforms , The PLA Army by Dennis J Blasko https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748401/the-biggest-loser-in-chinese-military-reforms-the-pla-army/
14. The Strategic Support Force and future Chines Information Operations, Elsa B. Kania and Jhon K. Costello.
15. Figure 5, China Strategic Support Force: A Force of New Era by John Costello and Joe McReynolds, Accessed on 5 February 2019.
16. Chapter IV, Organisations dealing with Cyber domain, China in the Cyber domain by Maj Gen PK Mallick.
17. 2.11, PLA Chain of Command Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC, 9 August 2021, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf. Accessed on 31 August 2024.
18. The Strategic Support Force anf future Chines Information Operations, Elsa B. Kania and Jhon K. Costello, Page 115 , Spring 2018.
19. Chapter V, Signal Intelligence, Computer Network Defence and Electronic Counter Measure Organisation, China in the Cyber domain by Maj Gen PK Mallick.
20. 2.10 Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC. Accessed on 9 August 2021.
21. A Baseline Assessment of the PLA Army's Border Reinforcement Operations in the Aksai Chin in 2020 and 2021 by Dennice Blasko, 9 April 2024, https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Display/Article/3735300/a-baseline-assessment-of-the-pla-armys-border-reinforcement-operations-in-the-a/. Accessed on 7 December 2024.
22. 2.10 Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC. Accessed on 9 August 2021.
24. "More Than 10 Units Combine into a Brigade, Harmoniously" [10多个单位合编成一个旅, 和谐相处有妙招], *PLA Daily* [解放军报], June 3, 2017, available at <www.81.cn/jwgz/2017-06/03/content_7626985.htm>
24. 2.38. Operational Support battalion Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC, 9 August 2021.
25. Ukraine to produce thousands of long-range drones in 2024, minister says 12 February 2024, https://www.reuters.com/business/aerospace-defense/ukraine-produce-thousands-long-range-drones-2024-minister-says-2024-02-12/
26. Ukraine is now dominating the Drone and EW domain, 21 August 2024, https://www.forbes.com/sites/vikrammittal/2024/08/21/ukraine-is-now-dominating-the-drone-and-electronic-warfare-domains/. Accessed on 7 December 2024.
27. Inside Ukraine's Killer-Drone Startup Industry, 2 May 2024, https://www.wired.com/story/ukraine-drone-startups-russia/
28. China's PLA found 'shooting at drone swarms challenging' in recent air defence drills SCMP 2 September 2024, https://www.scmp.com/news/china/military/article/3276769/chinas-pla-found-shooting-drone-swarms-challenging-recent-air-defence-drills

29. 2.26. Operational Support battalion Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC. Accessed on 9 August 2021.
30. Recommendation for Intelligence staffs concerning Russian new generation warfare Oct 2017, https://www.researchgate.net/publication/329934258_Recommendations_for_Intelligence_Staffs_Concerning_Russian_New_Generation_Warfare 07 dec 24
31. Return of Ground-Based Electronic Warfare Platforms and Force Structure July-Aug 2019 Miliatry Review. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/#:~:text=There%20is%20some%20movement%20on,%2Dmounted%2C%20and%20UAS%2Dmounted. Accessed on 7 December 2024.
32. Recommendation for Intelligence staffs concerning Russian new generation warfare October 2017.
33. Mei Changwei, Fan Yongqiang, Chen Yu, Mei Shixiong, Wang Yushan, Li Bingfeng, Wang Jingguo, Chen Yu, Wang Xiang, and Zhang Wei, "9个作战群, 空地一体受阅" [9 Operations Groups, SurfacetoAir Missiles All Receive Inspection], 新华每日电讯 5 版 [Xinhua Daily Telegraph 5th Edition], July 31 2017, http://www.xinhuanet.com//mrdx/201707/31/c_136487232.htm
34. Figure 6 &17 South china sea military capability series. Electronic Warfare and Signal Intelligence.chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jhuapl.edu/sites/default/files/2022-12/EWandSIGINT.pdf. Accessed on 7 December 2024.
35. Asian Military Review, Chaina redies updated stealth UCAV, 2 February 2024, https://www.asianmilitaryreview.com/2024/02/china-readies-updated-stealth-ucav/. Accessed on 7 December 2024.

Appendix A

DISPOSITION OF TRBS AND ECM BRIGADES TILL CORPS LEVEL: WTC

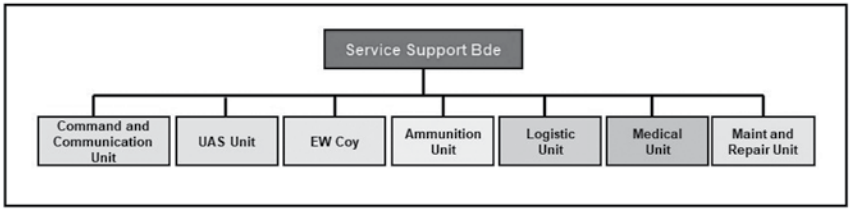


Source Chapter V, Signal Intelligence, Computer Network Defence and Electronic Counter Measure Organisation, from the book 'China in the Cyber domain' by Maj Gen PK Mallick, Print Publication Pvt Ltd

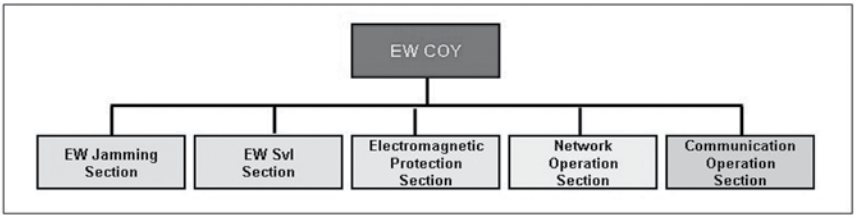
Appendix B

COMBINED CORPS (CC)/GROUP ARMY (GA) LEVEL SERVICE SUPPORT BRIGADE ORGANISATION

DIAGRAM 1

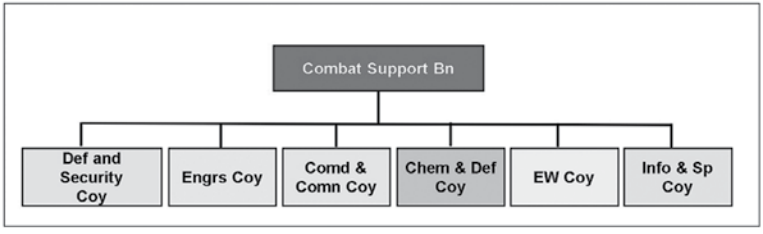


EW COY ORGANISATION
DIAGRAM 2



COMBINED ARM BRIGADE (CAB) LEVEL

COMBAT SUPPORT BATTALION
DIAGRAM 3

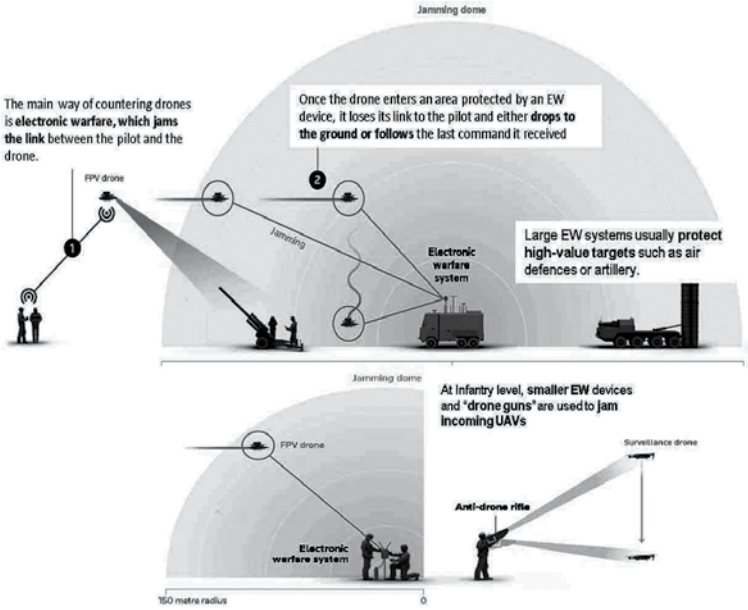


Source PLA Chain of Command Chinese Tactics, Army Techniques Publication No 7-100.3 Headquarters Department of the Army Washington, DC, 09 August

Appendix C

ELECTRONIC WARFARE AGAINST DRONES

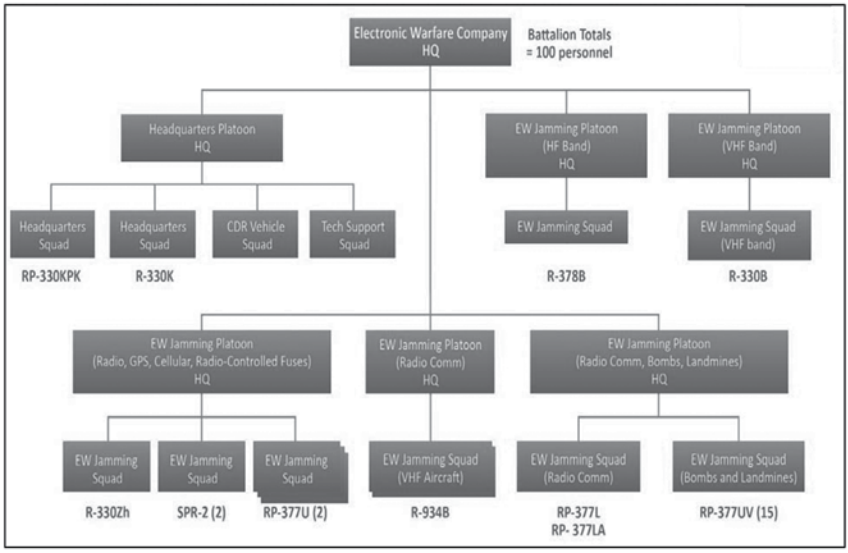
Electronic warfare (EW) systems have proved to be the most effective way of stopping drones. Both sides use EW systems to jam radio frequencies in certain areas. When a drone's signal is jammed, the pilot loses the ability to control the craft or can no longer see the video signal, depending on which frequency has been disrupted.



Source - How drone combat in Ukraine is changing warfare, Reuters 26 Mar 24

Appendix D

ORGANISATION OF EW COY GROUPED TO RUSSIAN MANOEVURE BDE

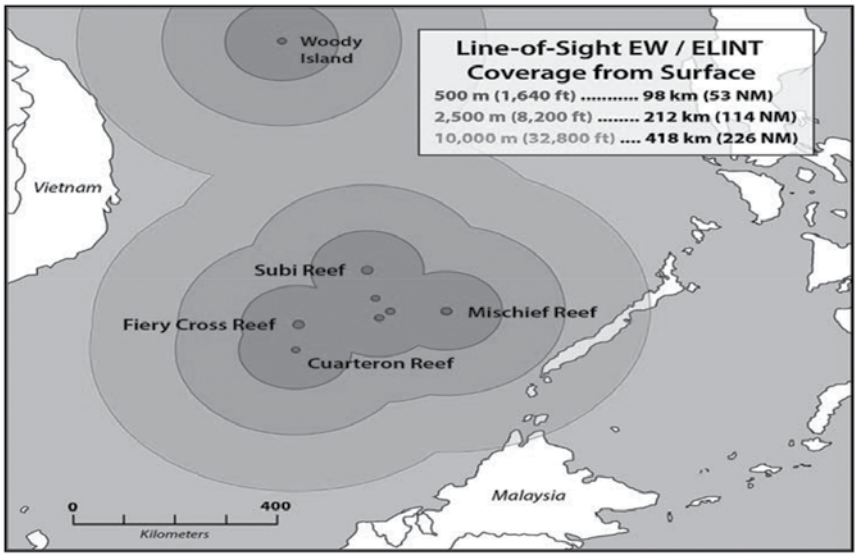


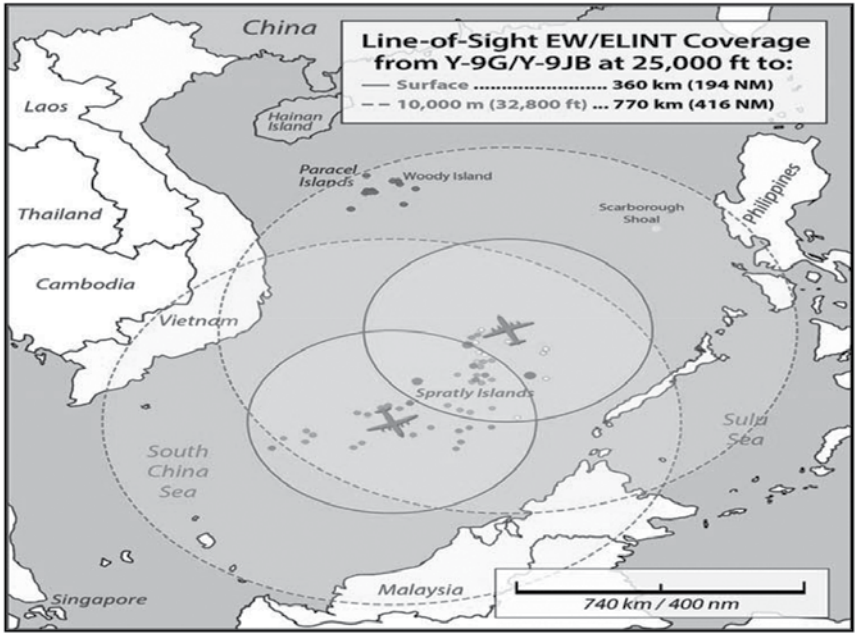
- **SPR-2: VHF/ UHF Radio Jammer**
- **RP-377U: Portable Radio Jammer VHF**
- **RP-377L, RP-377LA: Veh Mtd IED Jammer**
- **RP-377UV: Portable Jammer (against IEDs)**

- **RP-330KPK: VHF Command Post**
- **RP-330K: Control Station**
- **R-378B: HF Jamming Station**
- **R330B: VHF Frequency Jammer**

- **R-330Zh: Jammer against INMARSAT, IRIDIUM, GPS satellite systems and mobile Communications**
- **RP-934B: VHF Jamming Station tactical air communication and guidance systems**

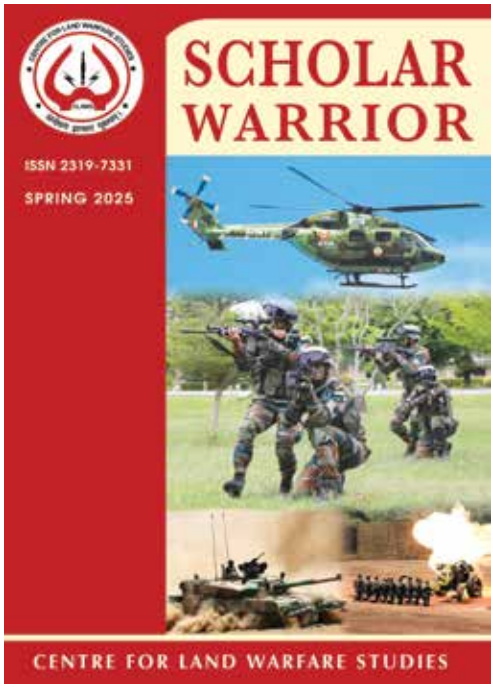
Source Return of Ground-Based Electronic Warfare Platforms and Force Structure July-Aug 2019 Miliatry Review





Source. Figure 6 &17, John Hopkins Applied Physics and Laboratory. South China sea military capability series. Electronic Warfare and Signal Intelligence

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA
☐ Rs. 500 /- per copy

SAARC COUNTRIES
☐ US $ 15 per copy

OTHER COUNTRIES
☐ US $ 20 per copy

☐ Rs. 1000 /- Annual Subscription (2 issues)

TO SUBSCRIBE SEND YOUR REQUEST TO

Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi
Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

The paper attempts to analyse all the information available on China's Electronic Warfare (EW) capability in the open domain, some printed publications and discussions with important stake holders in the field. It attempts to analyse how EW is merged with the much more recognised Cyber Warfare. A bit on rationale for China to invest heavily in this domain like the Russians to counter the US Military by hitting at its vulnerabilities. The paper brings out the structure of EW organisation within the Cyber Space Force (CSF) from highest level to the lowest, and how the reforms of 2015 and 2024 have aligned it to be more integrated with the theatre commands and all service HQs. The paper illustrates an analogy to give a fair idea of the role of Information Support Force (ISF) by comparing its functioning with similar Indian military organisation at the apex level. It brings out the concept of operations of the EW assets at the theatre level emphasising on the Western Theatre Command (WTC) involving inter-say relationship between Technical Reconnaissance Bureau (TRB) and the tactical EW formations orbated to the theatre, Corps and Brigades (Bde). The paper highlights China's capabilities in EW in the most contested South China Sea to monitor and influence the Electro-Magnetic (EM) spectrum of its neighbours. Most importantly, how the EW is playing a key role in redefining the character of military conflict sighting lessons from the current Russia-Ukraine War and its implications on our Northern Borders.

• • •

Lieutenant Colonel **Abhishek Acharya** was commissioned into the Corps of Signals in 2004. He holds a BE in Electronics and Telecommunication from National Institute of Technology (NIT) Raipur and MSc in Defence and Strategic Studies from DSSC Wellington. He has served in four Division Signal Regiments including an Armoured division, two in Hight Altitude Areas near LAC and LOC and one in Assam. He has been OC Communication in a Corps, tenanted an appointment of GSO1 (China) and served in Army Centre of Electromagnetics (ACE), Mhow. He has commanded an Electronic Warfare Unit in North East and a Signal Unit in an Independent Armoured Brigade on the Western Borders.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in Contact us: landwarfare@gmail.com

Rs 100.00 US $ 5.00

KW PUBLISHERS PVT LTD
www.kwpub.in