ORF OCCASIONAL PAPER
203
JULY 2019

Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army

Kartik Bommakanti

ORF OBSERVER RESEARCH FOUNDATION

Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army

Kartik Bommakanti

ORF OBSERVER RESEARCH FOUNDATION

ABOUT THE AUTHOR

Kartik Bommakanti is an Associate Fellow with ORF's Strategic Studies Programme. He specialises in space military issues, and more specifically, the relationship between the space medium and terrestrial warfare. Kartik also works on nuclear, conventional and sub-conventional coercion, particularly in the context of India and the role of the global powers in the subcontinent's strategic dynamics. His research has been published in various peer-reviewed journals.

ISBN: 978-93-89094-49-7

Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army

ABSTRACT

Cyber Warfare (CW) and Electronic Warfare (EW) are crucial to combat in modern warfare. Both are products of Signals Intelligence and constitute one part of Information Warfare (IW) and what is known as Network Centric Warfare (NCW). This paper explores how the People's Liberation Army (PLA) of China and the Indian Army (IA) have approached CW and EW. Both the PLA and the IA acknowledge NCW as doctrinally important. Organisationally and in Command and Control (C2), the PLA has undergone significant reforms; the same is not true for the IA. As opposed to the PLA, the IA is yet to fully acknowledge and recognise the complementarities between EW and CW.

(This paper is part of ORF's series, 'National Security'. Find other research in the series here: https://www.orfonline.org/series/national-security/)

Attribution: Kartik Bommakanti, "Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army", *ORF Occasional Paper No. 203*, July 2019, Observer Research Foundation.

INTRODUCTION

Few have addressed the question of how Cyber Warfare (CW) and Electronic Warfare (EW) capabilities intersect in the conduct of land operations by the Indian Army (IA) and China's People's Liberation Army (PLA). This paper explores the effects of cyber and electronic warfare on land operations. It examines the complementarities, similarities and differences between cyber warfare and electronic warfare, and how their relationship has long been recognised by strategic studies experts.

Cyberspace operations and EW occur across the electromagnetic spectrum. This paper demonstrates their importance in ground combat missions by undertaking a comparative analysis of the performance of the PLA and the IA in terms of capabilities, doctrine, and command organisation. The analysis is less concerned with Psychological Operations (PSYOPs) and Military Deception (MILDEC), which are integral to IW operations; the focus is on establishing technical links between CW and EW, Command and Control (C2), and doctrine. EW and CW are integral to Network Centric Warfare (NCW). NCW is geared to generating combat power by effectively networking all the elements of warfighting. It involves connecting geographically dispersed forces to enhance battlespace awareness, which include troops, platforms, weapons, sensors and decision mechanisms for sustained dynamically synchronised operations. NCW is not exclusively about technology, but as much about synchronising command and operational or tactical doctrine for the effective execution of military operations and missions according to the commander's intent.[1]

China recognises the linkages between CW and EW and has an established C2 structure that integrates the two components into a single information warfare force. The PLA, however, has yet to release

an official doctrine on offensive and defensive operations in the cyber domain, and more generally, in the area of IW; this, despite PLA experts since the 1990s having already articulated the importance of Information Operations (IO) in Joint Warfare.[2]

A note on sources: Most of the extant work on China used in this paper are either English translations of Chinese analyses, or Western sources on PLA's capabilities in the domains of CW and EW and the growing linkages between the two. Meanwhile, India's views are gleaned from existing doctrines of the IA and the tri-service. India is yet to formulate a coherent view on the challenges and opportunities about CW and EW to the same extent as China.

This analysis focuses on the military-operational domain of not simply CW, but the complementarities between CW and EW on the battlefield. What is the scope of integration between Indian and Chinese armies? Relative to the PLA, how much more integrated are the Indian Army's EW and CW capabilities at different echelons? China is known to adopt an integrated approach to the cyber and electronic domains; India is not. Beyond purely capabilities and the functional fusion between CW and EW, India needs a command structure that can cope effectively with the combined activities and demands of CW and EW across the electromagnetic spectrum.

This paper makes the case that integration and not just coordination is fundamental to the effective and synchronised use of cyber warfare and electronic warfare capabilities. China has moved carefully and methodically to create an integrated CW and EW as part of its Information Warfare (IW) strategy. The cyber-electronic integration is vital, which are both a part of the Electromagnetic Spectrum (EMS) or at least rely on the EMS for transmission.

The succeeding analysis will first define what "cyber warfare" and "electronic warfare" mean. It then defines "cyber weapons" and "electronic weapons" and how the cyber and electronic domains are linked. The third part evaluates the presence and integration of CW and EW capabilities by the People's Liberation Army (PLA); the analysis is done for the Indian Army in the subsequent section. The paper closes with an evaluation of where the Indian Army stands relative to the PLA in the integrated use of CW and EW capabilities for military operations.

I. CYBER WARFARE AND ELECTRONIC WARFARE: DEFINITIONS IN THE CONTEXT OF LAND WARFARE

1.1 Cyber warfare

In May 2008 former United States (US) Deputy Secretary of Defence Gordon England defined cyberspace thus: "A global domain within the information environment consisting of the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[3] Cyber Operations (CO) may be defined, meanwhile, as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in and through cyberspace."[4]

There are various risks involved in utilising cyberspace for specific objectives. This paper focuses on two specific types of risk: the first is operational, and the second, technical. *Operational* risks centre on how threats can compromise mission effectiveness; the effectiveness of cyber-attacks (or lack of it) in turn generates operational consequences.[5] Intrusion in cyberspace can undermine data and systems, and technical networks producing outcomes such as personnel deaths, damage or loss of equipment and property, capability degradation, mission degradation or even the overall failure of the mission.[6] The adversary

could potentially extract data from the Army's networks, depriving the army of the element of surprise and the ability to undertake an ambush. Adversarial forces may execute attacks through cyberspace and EMS against friendly forces, capabilities and networks, consequently compromising future cyber-attacks and missions geared to exploit cyberspace.[7] In addition, cyber-attacks are directed at generating an advantage within the cyber domain and supporting friendly forces. They contain specific actions that involve denial, disruption, degradation, destruction and manipulation.

The technical risks, meanwhile, are associated with vulnerabilities that are exploitable in the Army's systems and networks. Technical systems are generally networked across armies, generating shared vulnerabilities.[8] Potential vulnerabilities of shared networks and parts could undermine the projection of military power and support for the mission. Risks can be subject to mitigation through Defensive Cyber Operations (DCO) and cyber security measures to defend against attacks that exploit technical weaknesses.[9] A range of measures are necessary, including strong systems engineering capabilities, security, intelligence, counterintelligence, software and hardware integrity, supply chain risk management, and security engineering of information systems—these will enable the army to manage risks and maintain integrity and trust.[10] Before embarking on cyber-attacks, the army will have to examine the technical risks involved to avoid rendering its own networks vulnerable to counter-attacks.[11] In these circumstances, a defence-in-depth approach will be necessary to fend of attacks through anti-virus and anti-malware software programmes, strong sensors networks, prevention of intrusion, and other physical barriers to reduce technical risks.[12]

"Cyber warfare" is then defined as "attacks by a nation or quasi-national organisation on the software and data (as opposed to the people) of an information system."[13]

1.2 Electronic warfare

Electronic Warfare takes place within the Electromagnetic Spectrum (EMS). The EMS itself can be defined as the "…range of frequencies of electromagnetic radiation from zero to infinity".[14] The wavelengths and frequencies range from radio frequencies to gamma rays (See Annex Figure 1). EW is crucial in military operations. The integration and conduct of EW to support military missions occurs across all services; in this paper, the analysis is confined to the respective armies of China and India.

There are three elements in EW:[15]

Electronic Support (ES). ES focuses on interception. ES provides surveillance and warning data extracted from intercepted EM environmental emissions.

Electronic Protection (EP). EP focuses on encryption. EP provides self-protection to the host platforms against an electronically controlled threat.

Electronic Attack (EA). EA focuses on jamming. EA covers both ES and EP to defend a battle force consisting of several platforms or combat units.[16] Just as is the case with cyberspace, EA covers both defensive and offensive forms of warfare. Defensive EA protects friendly forces and host platforms, whereas offensive EA involves denial, disruption or destruction of adversary capabilities and forces.[17] Electronic warfare encompasses three core areas along the EMS: communications, navigation and radar functions, and the use by the adversary of these functions.[18]

1.3 CW and EW in land warfare

In the context of land warfare, CW and EW operations are undertaken to support Army operations and missions. Most immediately relevant to land operations are ground-based EW systems and aerial EW systems.

Ground-based EW capabilities. Ground-based EW equipment and operations support commanders in manoeuvre. For example, a dismounted soldier or platforms that are highly mobile can be used for ground-based EW capabilities.[19] Inherent in ground-based EW is the short-range characteristics of tactical signals direction finding. EA capabilities or equipment is normally deployed in forward areas with or in close proximity to forward units.[20]

There are various advantages to ground-based EW systems. For one, they provide direct support to army units on the battlefield during combat manoeuvres through counter radio-controlled improvised devices and communications or sensor jamming. EW ground capabilities are geared for supporting sustained land operations and enabling a speedy response to the commander's directives. Land-based EW units are most effective when they grasp the EMS signature and direct their effort to protect their respective EW equipment from adversary ground and aerial threats. Survivability and mobility are crucial for EW equipment for effective mission support. Only ground commanders can establish their respective EW needs and manoeuvre units have to logistically support EW assets.

To be sure, ground-based EW assets have limitations. They are vulnerable to adversary geolocation, electromagnetic deception, EP measures, and physical attacks, and are susceptible to terrain masking.[21] They are also constrained by distance and propagation limitations against adversary electronic warfare systems.

Airborne electronic warfare systems. Airborne EW systems, both manned and unmanned, perform almost identical functions in support of ground operations. However, aerial electronic warfare is more time-critical. AEW is normally undertaken at higher tempo and shorter in duration. It places a high premium on detailed planning. Successful

airborne EW in support of ground operations must include a clear understanding of the commander's objectives, detailed planning and integration, ground support infrastructure, interaction between aircrew providing EW support for ground forces, and defence against adversarial aircraft and air defence units.[22]

The advantages of AEW assets range from provision of tactical support for action beyond ground forces such as electronic suppression of enemy air defences, use of anti-radiation missiles, and destruction enemy air defences. Airborne EW capabilities provide greater mobility and flexibility. Unlike ground-based EW, they provide support over extended ranges and provide better line of sight and direction finding capacities.[23] However, airborne EW too has weaknesses such as limited time on station and as with ground-based EW; airborne electronic assets are vulnerable against EP. In addition, AEW assets are exposed to electromagnetic deception and adversary geolocation, and may need the support of supplementary assets.[24]

Any army will generally have a combination of ground-based and airborne electronic assets. The challenge lies in leveraging both subsets in a synchronised manner. Beyond EW assets, the challenge is either to conduct operations independently or in concert with CW assets based on the commander's directives and the mission.

II. CW AND EW: DIFFERENCES, COMMONALITIES AND THEIR ROLES IN THE ELECTROMAGNETIC SPECTRUM

A study by RAND Corporation found that cyber operations fuse with 60 percent of EW and roughly 80 percent of Signals Intelligence (SIGINT).[25] However, the relationship between SIGINT and EW and CW is a complex one. Indeed, there is a view that EW and CW are more complementary than combined.[26] This paper shares this view.

The primary functions of EW are in two areas: directed energy and brute force (barrage) jamming.[27] Directed Energy encompasses a set of technologies that generate a beam of concentrated electromagnetic energy or atomic or sub-atomic particles.[28]

In the case of SIGINT, it is eavesdropping. Electronic Intelligence (ELINT) is a component of SIGINT and technical and foreign geolocation intelligence extracted from non-communications electromagnetic radiations. Non-communication radiations include radars, Surface to Air Missile Systems (SAMs), and aircraft.[29] Along with ELINT, SIGINT consists of several other forms of intelligence such Communications Intelligence (COMMINT) and Foreign Instrumentation Intelligence (FISINT). Finally, in the case of CW, a range of operational and attack options exist such as web and email spam, denial-of-service attacks, malware and viruses.

The commonality between CW and EW is both a matter of perspective and misunderstanding. As a rule, any network is vulnerable to penetration and corruption whether it is air-gapped (connected to the internet) or not. In the case of air-gapped networks, penetration and corruption or manipulation of networks could come through physical intrusion in the form of virus or malware containing external devices such as flash drives. Even an electronic network is susceptible to corruption because it might not be "cyber-secured".[30] To that extent, both cyber and electronic networks share this common vulnerability. Vulnerabilities could affect military platforms. Take for instance, UAV systems, which are also cyber-physical systems in that they depend on an interaction between physical and computational features of the UAV system.[31] UAVs are particularly vulnerable because their communications are relayed via satellite, ground stations and other UAVs within the network.[32] Nevertheless, as electronic and cyber warfare platforms they are critical assets in land warfare.

Modern armies, including the PLA and the IA depend on UAVs. Cyber-attacks could be launched against UAVs sensor nodes by manipulating their sensor input and functions and trigger existing malware to disable them by generating denial of service attacks or mislead the processes on which the UAV network's sensors are dependent and generate a failure in the fail-safe mechanisms of the UAV network.[33] Like in the case of satellite systems, spoofing and jamming which fall within the domain of electronic warfare would be the most natural and effective methods for crashing and capturing UAVs. Satellite signals are highly vulnerable to spoofing attacks as are UAVs. Jamming involves deliberate transmission of radio frequency signals to disrupt the transmission of other radio signals. Spoofing, on the other hand, despatches intentionally misleading signals to a receiver of an antenna by making it accept false information.[34]

Table 1 in Annex provides a concise explanation of the relationship between the EW domain and the cyber domain. Their missions tend to be similar, albeit conducted in separate domains. The similarities between the two relate to access and denial operations against specific threats. Their differences lie in means, mechanisms and paths.[35] As General John Hyten, currently commander of the US Strategic Command (USAC), observed: "In cyberspace, we provide pathways for information, we deny adversaries information. It's the same [EW] mission that…we do in different domains."[36]

Beyond these shared features, information warfare actions cover both cyber and EW operations in the arena of military deception. The commonly used form of EW by tactical aircraft is "synchronised false jamming".[37] Technically, it creates deceptive targets that appear realistic and sows confusion by creating a match between the jamming to the target radars electronic signatures through an injection into the back and side lobes of the adversary's air defence network.[38] This form of

jamming can transmit through automated electronic countermeasures or filters and generates 'realistic'-looking targets that are not authentic information.[39] In the case of CW, "software decoys" may be developed as a technique for generating false defensive tactics. These decoys comprise software modules that act like normal software but can identify attacking behaviour of the adversary and generate a deceptive response (See Table 2 in Annex). The greatest possibility lies in coordinating actions between the cyberspace domain and electromagnetic spectrum. The data stream can be fed into the target antenna and consequently the network itself can be penetrated and exploited for manipulation.

III. CHINA'S VIEW OF CW AND EW CAPABILITIES: CONVERGENCE OF DOMAINS?

3.1 Cyber Warfare and Electronic Warfare: PLA's View

Under China's conception of cyber warfare, an entire range of capabilities and technologies characterise computerised warfare. In Chinese parlance, CW is described as Computer Network Operations (CNO) that involve digitisation and computer systems that are completely networked and provide clarity and data in real time to military commanders on the field.[40] CNO can assume the form of hacking and cyber-attacks. Further, through simulated false commands, the adversary can be deceived.[41]

From a Chinese standpoint, warfare across the electromagnetic spectrum requires initiative and offensive action. The purpose, according to the PLA, is to dominate the electronic spectrum and effectively deny the enemy the use of its electronic equipment. Offensive operations across the electronic medium would employ electronic jamming, electronic deception, directed energy weapons and electromagnetic pulse radiation. The defence (as opposed to offence) would require hardened facilities, dispersion, countermeasures, and

physical retaliation. Consequently, microelectronics has been a key area of investment for the PLA.

3.2 The Overlap of CW and EW

In 1999, PLA Major General Dai Qingmin was the key advocate behind the adoption of China's integrated view of CW and EW operations as part of the PLA's Information Warfare (IW) strategy. Dai secured a promotion to head the erstwhile 4th Department of the Chinese General Armaments Department (GAD). He made the case for fusing EW with Computer Network Operations (CNO). He defined Information Operations (IO) as a series of operations with information systems as the direct operational target, and with electronic warfare and a computer network war as the principal form."[42]

According to the PLA, EW and CW are not mutually exclusive; it is necessary to recognise their convergence and integration to dominate information operations during wartime. Dai Qingmin called it Integrated Network Electronic Warfare (INEW) composed of the "…organic combination of electronic warfare and computer network warfare." As the American scholar James Mulvenon put it, this was "revolutionary", because even experts and information warriors in the United States were yet to be convinced about the connectedness between the two forms of warfare; they deemed electronic warfare to be completely outside the realm of computer attack networks.[43] For Dai and others within the Chinese strategic and military establishment, a blended view of CW and EW was the 'essence' of "integrated combat operations" to fight "enemy information systems" with the aim of "seizing battlefield superiority".[44] Although China has not established a formal information warfare doctrine, it has gone ahead of the curve in grasping the importance of the opportunities in combining cyber and electronic warfare, or at least seeing the complementarities between them.

There is evidence to suggest that PLA intends to confront the adversary pre-emptively through cyberspace alone, which is not necessarily linked to dominating the electromagnetic spectrum. This effort would require computer network operations that infect the enemy's weapons systems with malware while they are still inactive, but the malicious code only activates at predetermined time with the aim of destroying the adversary's Command and Control system, such as "…circuits that control railroads, military air traffic and divert trains to wrong routes to cause traffic jams".[45] The PLA, therefore, also views cyber operations as an independent means to subdue the adversary and sees computer network operations as having disruptive effects on them.

Is there an "organic" link in the form of INEW for the PLA between the cyber and electronic domains for battlefield operations, which the PLA has tested? In 2011 and prior to the introduction of the 2015 military reforms, the PLA conducted a series of exercises involving for instance, in the Chengdu Military Region (MR) an unnamed artillery regiment's employment of INEW as a "soft kill" approach which included electromagnetic jamming and computer network attacks against the adversary's command and reconnaissance systems.[46] Consequently, instruments appear to be integrated into the artillery unit's fire support mission that are independent of Electronic Counter Measures (ECM), implying that other non-ECM combat elements also include "electronic warfare and computer network attack as an organic capability" with the PLA divesting reliance "…solely on dedicated external INEW units for support".[47]

One other notable exercise conducted in 2009 as part of a large-scale multi-MR exercise employing a "blue force jamming and information offense-defense units" were effective in suppressing red force armour

and motorised infantry and its command and control through a combination of network and jamming attacks.[48] Thus, the Chinese approach to CW and EW in the guise of INEW underlines the significance of a connection or complementarity, if not a complete overlap, between the two areas of the cyberspace domain and the Electro-Magnetic Spectrum (EMS). These exercises also demonstrate the extent to which PLA has pursued the integration of CW and EW capabilities as part of a networked fighting force and subjected them to intensive tests to measure their effectiveness as well as training combat personnel.

To improve the effectiveness and speed of decision-making and sustain secure and reliable communications, the PLA as of today fields an automated command system known as the Integrated Command Platform with mobile and static units.[49] This enables the PLA to execute joint operations more effectively at close and far combat zones with advanced weapons systems. Lower echelon units field the Integrated Command System facilitates communications across all the service arms of the Chinese military.[50] The Chinese military's C2 structure is similar to Western C2 systems to the extent that operational commanders determine the force structure drawn from units trained and equipped by the each of the Chinese services. The joint C2 structure encompasses mostly People's Liberation Army Air Force (PLAAF), People's Liberation Army Navy (PLAN) and the Strategic Support Force (SSF). This emphasis enables more jointmanship.[51]

While China does not have a formal doctrine enunciating the link between CW and EW, the Chinese approach to CW and EW is compatible with this paper's conception of cyber-electronic operations to the extent that it recognises they are crucial nodes on the electromagnetic spectrum.

3.3 The SSF Integration and Command and Control Advantage? China's Computer Network Operations (CNO) and EW

China has undertaken a reorganisation of the command structure of its capabilities in cyberspace, electronic warfare and space, placing them under the authority of the Strategic Support Force (SSF).

The "cyberspace force", China calls it, is part of SSF's Network Systems Department (NSD). The 3rd General Staff Department (GSD) of the PLA was the precursor to the NSD. The NSD is similar to the command structure of the People's Liberation Army Navy (PLAN) to the extent that it has an operational commander as well as political commissar. Two inferences can be drawn from this. The centralisation of command under the Central Military Commission (CMC) of China's information warfare arms is possibly due to Xi Jinping's taking on greater control over these critical domains (cyber, electronic and space-based).[52] For instance, the first military commander of the NSD was Lieutenant General Zheng Jungie and the NSD political commissar was Lieutenant General Chai Shaoliang.[53] It can also be inferred that the CMC intends to see the SSF do what it desires: execute the intent of the CMC in wartime. At the inception of the reforms in 2015 CMC guidance noted that, "the CMC commands; the services equip; and theatre commands fight".[54] This allows the CMC the PLASSF to direct intelligence for all battlefield operations.

The military reforms introduced in 2015 were far-reaching to the extent that they have expanded the CMC's direct control over military operations and operational forces and all the technical functions were consolidated under the PLASSF.[55] The PLASFF's establishment reflects a shift in priorities, and intelligence is more focused on supporting military operations. The NSD is believed to be a reorganised, renamed

and upgraded entity,[56] and it is encompassing most of the institutional functions performed by the erstwhile GSD undergird.[57]

Chinese cyber forces have been centralised under the NSD, which is a significant move as it demonstrates a seriousness to overcome the coordination problems that plagued the erstwhile 3rd GSD. This shift in the structure of command will enable the NSD to coordinate and conduct operations with greater effectiveness. Integration brings considerable benefits to the PLA:

- Integration enables better cyber reconnaissance, allowing the PLA to gather information about technical and operational matters for intelligence, which thereafter will be employed for operational planning for the execution of cyberattacks.[58] The latter are enabled by the reconnaissance mission, which provides access, tactics and techniques for the conduct of offensive cyber operations.[59] Chinese strategic thinkers generally emphasise the significance of surprise in the context of cyber warfare, and that revealing too much about their capacities risks compromising their network defence, and thereby deterrence. This is not unusual from a doctrinal and operational standpoint because cyber warfare itself is still evolving and the possibilities of integration of CW and EW continue to mature.

- The PLA's rationale for assuming a complementary view of CW and EW is also borne out of its quest to establish information dominance in the initial stages of a conflict by disrupting the adversary's Command and Control (C2), C4ISR, logistical network, communications and commerce. Finally, cyber warfare capabilities for the PLA will and is considered to serve as a force multiplier in conventional military operations during conflict.[60] Unlike the space and cyber missions, the Chinese military's electronic warfare

mission has been nowhere nearly as divided.[61] All the PLA's electronic warfare missions have been comprehensively clustered into the former 4th department of the GSD. The former 4PLA oversaw radar and computer network attacks, which has now undergone a division along administrative and operational lines with several functions and roles either eliminated, reorganised or moved to the Joint Staff Department (JSD) and the SSF.[62] At the apex level the 4 Department has been reconstituted as the new joint force called the Network Electronic Bureau (NEB) or JSD-NEB. Most likely, in its re-invented *avatar,* it is responsible for the management and execution of cyber and EW missions across the SSF, the theatre commands and services.[63] Indeed, the PLASSF has integrated the whole of the erstwhile 3PLA, 4PLA, satellites and UAVs comprehensively into a single information service and is a vital organisation indicating how effectively it can generate a shared intelligence picture in the battlefield for its warfighting units.[64]

One of the distinctive features of the SSF is the integration of Chinese cyber militias. The cyber militias existed long before the establishment of the SSF. Being hackers, these militias are known to mobilise and launch attacks quickly following the onset of a crisis.[65] The integration of cyber militias into the SSF is intended as much to discipline them and direct their energy and utility towards specific missions and objectives. They serve as a vital force multiplier, saturating an adversary's cyber network defences through coordinated attacks in the early stages of a war to gain information superiority. For an adversary such as India, this presents profound consequences for Command and Control (C2), because it could potentially experience simultaneous attacks against several layers of the network's defence-in-depth assets generating considerable devastation.[66] In addition, PLA land forces also deploy a variety of Unmanned Aerial Vehicles (UAVs) for

a range of ground operations and missions. These UAVs are controlled by operators and technical personnel across various units of the PLA. UAVs will be used for reconnaissance missions extending to the brigade level. Even at the battalion level and smaller units known as "teams" UAVs will provide tactical support in the form of information denial, target acquisition, imagery data, radar jamming, electronic counter-measures, position and targeting information for precision artillery fire. They are also geared to disrupting enemy C2 structures by undermining the enemy's use of the electromagnetic spectrum. The PLA's miniature UAVs such as the ASN-207 have a range of 600 km. ASN-20 7 and other UAVs are vehicle mounted. Chinese armoured brigades and special forces are equipped with hand-held UAVs for localised reconnaissance.[67]

Another distinctive feature behind the integration of EW and CW capabilities under the SSF is the role Civil-Military Integration (CMI) has played in China's information warfare capabilities. CMI has been critical to President Xi Jinping's military reforms introduced in December 2015 and vision to leverage the scientific and technological strengths of the civilian industry and academic institutions to aid technological strengths of the military.[68] The PLA's EW and CW capabilities are beneficiaries of the CMI effort. Thus, if China is to maintain both a competitive edge and dominant position against it peers in the military domain, then it needed a deep techno-scientific synergy between civilian and military domains. As Xi put it in his report to the 19th Party Congress of the Communist Party of China (CPC), "We must keep it firm in our minds that technology is the core combat capability, encourage innovations in major technologies, and conduct innovations independently. We will strengthen the system for training military personnel, and make our peoples forces innovative."[69] The CMI has its origins in the 1990s, undergoing progressive institutionalisation

and transitioned to deeper engagement between civilian and military domains. The fusion between civilian techno-scientific and defence sectors that CMI embodies is intended to bring efficiency and improved resource allocation "...whereby spending and investment are mutually beneficial to the military and the local economies".[70]

Integrating cyber operations with EW has been a longstanding PLA theoretical requirement and the basis of China's current information warfare operations. CMI has played, and will continue to play a key contributory role in the PLA INEW operations. It requires the close coordination and synchronisation between cyber and electronic warfare employment in all domains including land warfare.

IV. THE INDIAN VIEW OF CW AND EW

4.1 Lack of doctrinal clarity

India's approach towards electronic warfare and cyber warfare is nowhere as evolved as that of China's. Most of the extant work on India's cyber initiatives centre on threats to critical national infrastructure, government agencies and financial institutions like banks and insurance companies, as well as corporate entities.[71] There are exceptions in this regard about how cyber capabilities ought to be optimally used. For instance, a study did consider and recommend the importance of creating "training and assimilating a cyber-force for offensive and defensive operations."[72] Even when they do address the imperative and importance of CW capabilities, the engagement is limited. Therefore, the focus, at least in these analyses of the cyber domain, while important, is more on intelligence missions for the protection and security of critical national infrastructure reliant on information systems rather than the role of CW and EW activities for military-operational missions on land, sea and air.

To be sure, there are some exceptions within the Indian discourse, which do recognise China's INEW strategy and the PLA's quest to synchronise CW and EW operations and what India's response should be.[73] However, they do not engage with both the gaps in India's capabilities and whether India could learn something from the Chinese experience, its vulnerabilities and establish the extent of a link between synchronised EW and CW operations in the context of land operations.[74]

Drawing on existing official documents from the Indian Army and the Integrated Defence Staff (IDS) Headquarters and some extant work on cyber, EW and electromagnetic spectrum operations, there is a challenge in the way the IA views CW and EW in ground operations. This is most pronounced in the IA's doctrine.

In some respects the Indian Army's (IA) conception of IW is similar to the PLA's approach to IW to the extent that both armies view the complete attainment of "…full spectrum information dominance over the adversary."[75] However, they are also dissimilar in that the IA does not visualise a merger a between CW and EW along the electromagnetic spectrum. Indeed, the Indian Army's Land Warfare Doctrine released in 2018 treats CW and EW as distinct realms. The army defines CW thus: "Cyberspace will be the new dimension of warfare and will be a key battle winning factor in future conflicts. While developing Cyber Warfare capabilities, all elements/ forces must retain the capability to fight through a disruptive Cyber Warfare domain/environment. The Indian Army will upgrade existing Cyber Warfare capabilities with the objective to develop cyber deterrence and defence capabilities, while simultaneously devising means of eliminating such threats."[76] Meanwhile, it defines electronic warfare distinctly in this manner: "We shall continue to develop a span of Electronic Warfare eco-systems to upgrade operational focus, equipping and skilling. Our Electronic Warfare capabilities shall evolve into full spectrum, electro-optical dominance to

include capabilities in Communication Intelligence (COMINT), Electronic Intelligence (ELINT), interception, jamming, spoofing and deception. To contain proxy war, endeavours will continue to degrade the communication capabilities of terrorists/ insurgents and enhance our technical prowess to combat the impact of radicalisation/ alienation."[77]

Both these definitions under the IA's land warfare doctrine treat "disruptive" as part of CW and "deception" as EW. However, the doctrine's framers do not view deception to be as much a part of CW. As earlier mentioned, CW plays as much of a role in deception as does EW. More critically, the IA has yet to develop anything remotely resembling the Chinese INEW approach encompassing EW and CW.

A likely reason for this is that there is inadequate interaction between the Indian Army Training Command (ARTRAC), which is responsible for formulating and updating service doctrine, and all the technical entities, such as the Defence Intelligence Agency (DIA), the Corps of Signals, the Defence Information Assurance and Research Agency (DIARA), and the National Technical Reconnaissance Organisation (NTRO). This is a requirement to the extent it gives a sense of direction to army commanders and how cyber and electronic warfare capabilities for ground warfare ought to be used to attain objectives. The PLA might not be the best example for comparison simply because it lacks a formal and publicly available information warfare doctrine or a doctrine that incorporates the CW and EW components in land warfare.

It is the US Army's efforts that could provide some direction for how the IA could proceed. Generally, as one Indian army officer put it, "India's [IW] doctrine and methods differ only slightly from those used by many Western nations".[78] Information Operations (IO) is the only distinctive feature in India's IW doctrine. Among the few former Indian

Army officers, recognising this importance updating is Lt. Gen. R.S. Panwar and a former Corps of Signals officer who observed: "There is a need to substantially update existing IW doctrines at the Joint Services as well as individual Service levels. In view of the ambiguity in the definition of IW terminologies world- wide, these doctrines must make a deliberate effort to rigorously define terms as applicable in the Indian context."[79]

4.2 Inter-service integration

Beyond the absence of doctrinal clarity, there is a lack of theaterisation, which will enable greater synergy and efficiency as the Corps of Signals trained manpower can be used particularly in the domain of communications.[80] Network-enabled platforms and force, are crucial for a communications intensive fighting force. To be sure, NCW goes beyond simply communications, even if it is a significant contributor to network-centricity. Network-enabled platforms would be effective only if India were to *actually* create integrated theatre commands. As of today, with the exception of the theatre-based Andaman and Nicobar Command (ANC), which is a tri-service command under a single operational commander, India lacks the kind of five integrated theatre commands that China has established.[81] Nevertheless, what is to be made of intra-service efforts or considerations to create network-enabled platforms such as the IA? One of the few who have addressed this question is Lt. General V.K. Kapoor formerly Commandant of the Army War College Mhow who observes "cost" and "complexity" mean that only a few formations geared for offensive operations can be network enabled.[82]

For instance, a motorised infantry division with C2 and Combat elements of vehicles can be 100-percent network-enabled, whereas its support elements such as troop ferrying vehicles, repair and recovery

and logistics vehicles can only be networked selectively.[83] Indian technologists from the Bharat Electronics Limited (BEL) recently reinforced the view that the cost of ownership is likely to increase due to complexities and challenges involved in "...integration and interoperability in the existing architecture" of combat and combat support vehicles, which "...result in higher total cost of ownership."[84] Using vetronics technology, also known as "vehicle electronics standards", they propose certain improvements which can be made to the performance of intra-vehicle and inter-vehicle platforms. Due to the increasing complexities in integrating technologies, vetronics will facilitate the seamless integration of sensors and weapons and enable communications within and between wheeled and tracked platforms such as Infantry Fighting Vehicles (IFVs) and tanks.[85]

However, within IA doctrine there is little discussion of how EW and CW merge and whether a consolidated approach should be undertaken for combined cyber and electronic warfare operations. For China, employing the instruments of INEW will be particularly applicable in the early stages of a conflict[86] with India.

From an organisational and integrative perspective, as noted earlier, there is support for combining EW and ELINT under a single commander or formation, but there is little discussion at least at the Indian end about CW and EW under a single combatant command. Critically, DCA itself, which appears to be a centralised entity, might not be the answer as it also undercuts support to conventional military operations for specific missions and military objectives, particularly against a potential adversary such as China. As Panwar observed long before the establishment of the DCA: "Presently, all indications are that the DCA would be located and deployed centrally, under the presumption that it is not advisable to deploy offensive cyber capabilities in a decentralized manner. If a full-scale multi-domain war is

to be fought by us, especially with an adversary like China, such an organizational architecture may not be suitable to meet operational requirements for carrying out integrated multi-domain operations at all levels of warfare, i.e., strategic/ operational/ tactical. This issue needs to be deliberated upon in all seriousness."[87]

The recent announcement by the government of India establishing a Defence Cyber Agency (DCA) is only the first step, but it does appear to be exactly what Panwar declared it would be – a centralised command entity overseeing all cyber operations rendering it inadequate in a land war, let alone a comprehensive multi-domain conflict against China.[88] That apart, it would grate also against at least the intent behind tri-service doctrine's "centralised intent, decentralised execution". As the IA's Eastern Army Commander Lt. Gen. Naravane put it in January this year, "It will be an inter-services agency, not purely Army, functioning under the IDS and they will be looking after all the threats in the cyber domain."[89] It will be headquartered in New Delhi with "…units or cells or dedicated officers at every [Corps] Headquarters across the country."[90] However, the DCA will likely be subject to the same civilian bureaucratic controls, as its Chief will not have much authority. Since the DCA will be placed under the "headless" IDS as, Lt. Gen. S.K. Sinha once described the IDS, with a non-specialist bureaucracy wielding authority without responsibility and accountability.[91] Without a Chief of Defence Staff (CDS) and the Service Headquarters (SHQs) integrated into the Ministry of Defence (MoD), which has been consistently derailed owing to concerns ranging from inter-service rivalry to the loss of civilian control over the armed services,[92] the establishment of the DCA will not be very effective.

In addition, it is as much about whether as a potential Indian DCA like its American counterpart and to a degree, the Chinese one, the SSF can sustain offensive operations through the cyber medium as an

independent undertaking,[93] and not just in support of land operations. Offensive Cyber Operations (OCO) can be a force multiplier for conventional military operations as well.[94] Specifically, undertaking land-based operations with the help of the cyber medium by pursuing a C2 model the Indian armed services tri-service or joint doctrine describes as "Our C2 is underpinned by a philosophy of centralised intent and decentralised execution – this enables freedom of action and initiative."[95] However, the IA's land warfare doctrine specifically, does not articulate similar conception or philosophy of C2,[96] reinforcing the misgivings of Panwar of a DCA, which is excessively centralised in its organisational and operational structure. To be sure, the Army's land warfare doctrine implores the reader to peruse its own doctrine "in conjunction" with the tri-service doctrine. Even so, the tri-service doctrine is likely to be effective only if there are established theatre commands with organic EW and CW and ELINT capabilities. Unless this fundamental inadequacy is overcome, both the establishment of the DCA and the tri-service doctrine stated intent to sustaining networked operations through potentially Integrated Theatre Commands (ITCs) that China has instituted would remain unfulfilled.

Reliance on a centralised cyber network undermines timeliness and potentially undercuts the commander's time-critical missions and operational objectives. An architecture that is centralised in intent, but decentralised in command—allowing EW and CW to be under a single operational or theatre commander—enables the military unit to stay on mission and follow the commander's directives.

The foregoing discussion has focused on cyber elements in the information domain and little on its connection between electronic medium with the cyber domain underlining the weaknesses inherent in the doctrine of the Indian army. Even as CW and EW are possibly complementary, IA's current land warfare doctrine does not reflect this

change or visualise it as a possibility. Nor is there evidence to suggest a shift in its command structure to manage CW and EW operations in the context of land warfare, which has been the case with China (at least organisationally, if not doctrinally), and increasingly other armies worldwide. As noted earlier, in addition to the Indian army's land warfare doctrine, the Integrated Defence Staff Headquarters (IDSHQ) too has published a tri-service or joint doctrine. The joint doctrine traverses a somewhat greater distance in seeing the importance of cyber capabilities at the "operational" and "tactical" level. It does not see any complementarities or synergies between CW and EW in military operations at the tactical and operational levels.[97] However, it recognises the importance of cyber power in Network Centric Wars (NCW). It seeks to exploit "information technology and Integrated Reconnaissance, Surveillance and Command, Control, Communications, Computers, Information and Intelligence systems, [which] will win battles."[98] However, the pursuit of NCW by exploiting the complementarities between CW and EW can only be effective if India's C2 structure is reformed.

4.3 Command, Control, and Capability Disadvantage: India's Limited View of Combined CNO and EW

Unlike China's Strategic Support Force (SSF), India lacks a dedicated information warfare service that could be deployed in service-specific missions and military goals. New Delhi's information warfare capacities are fragmented and lack a clear command structure. India's EW capabilities have not matured in the form of miniaturisation to the extent of China's own.

Before the analysis proceeds further, there is a need to assess how SIGINT has evolved in India and what role it has played in India's wars.

While India has fought conventional wars, its experience in these campaigns has not been sufficient to bring about a shift in the nature of its C2 architecture.

Historically, the integration between intelligence and field formations and divisional commanders in India has been uneven. This has been as true for SIGINT as it has been for other forms of intelligence. In the post-independence period, we can draw from India's experience with SIGINT and from the wars India has fought. In India from 1947 to 1962, signals intelligence languished. Indeed, a large portion of the Signal Directorate, suffered a major of loss of personnel just prior to independence who transferred to Pakistan.[99] The contraction was so enormous that it led to a downgrading of the Signal of Officer in Command (SO-in-C) to Brigadier rank.[100] Post-independence and Partition, Indian intelligence experienced sharp reductions and there were very few operational Field Security Service (FSS) units.[101] Significantly, the FSS operated separately and its headquarters was based next to the Intelligence School (India) and Training Center.

All personnel requirements of the FSS were managed by this entity. In addition to making key staff appointments in Army intelligence, the duties of intelligence personnel involved specialised assignments linked to interrogation, signals intercepts, prisoners of war camps and other intelligence assignments.[102] Further, prior to the Sino-Indian boundary conflict, Over-aged, superseded officers generally staffed the Intelligence Corps of the Indian Army or personnel rejected by their principal arms or services.[103] Specifically in relation to signal intelligence, following Partition, dedicated SIGINT did not exist in the army and instead virtually all the units that specialised in SIGINT were dissolved. Whatever remained, merged with the Military Operations and Intelligence Directorate (MO&ID).[104] Signals notably did play a role

between early to middle October of 1962 before the outbreak of full-scale war completing a communications grid by establishing telephone lines connecting Tsangdhar with the IA's 7 Brigade deployment along most of the Namka Chu River.[105] This example is only one among the few publicly available pieces of evidence of the uses of Signals in the 1962 war.

Following India's defeat by China in 1962, the Henderson Brooks Enquiry Committee developed a list of recommendations, including the implementation of an "integrated concept" of Intelligence.[106] The concept required that every single formation commander had to possess his own intelligence resources to neutralise threats, sustain counter intelligence missions and complete intelligence acquisition tasks.[107] Thus, a single intelligence unit was required to perform these tasks, and an organisation of intelligence and Field Security Company (FSC) was created to execute closer coordination. Specifically, the Signals Corps came into existence and underwent expansion.[108] The increase in the size of the Corps of Signals was driven by native demands that never existed under the British; new entities were established to meet India's intelligence needs and cater to its geographic conditions such as the mountain divisional signal regiment, the special signal regiment and radio monitoring companies.[109]

The gargantuan Eastern Command was divided into separate commands – Eastern and Central. The Corps of Signals came into existence as a tri-service organisation drawing personnel from all three services namely the navy, air force and army. The latter, however, served as the prime source of recruitment. By the late 1960s, the elevation of the commander of the SO-in-C to lieutenant general officer rank[110] or major general meant that the SO-in-C is now a general officer.

Given this background, a brief explanation is due on the wars India has fought after 1962. Three years after the 1962 war, the second India-

Pakistan war broke out in 1965 with the Pakistani attack in Kashmir. Signals communications was unsatisfactory in the initial stages of the war—it was under-resourced and poorly organised—[111] eventually improving as fighting progressed. Signal communication through radio relay, which ironically, was opposed by Brigade commanders during training prior to the war for the reason that it prevented concealment and gave up their presence to the adversary due to electronic detection, were enthusiastic about not only of radio relay terminals accompanying them, but also being set-up well in advance of their deployment.[112] Overall, the Signals Corps gained experience operating in desert terrain.

In the run-up to the 1971 war, India's signal preparations went into overdrive and the Signals Corps capacities were stretched to extreme lengths. Generally, Signals support is extended following operational and tactical planning, which was not the case in 1971, because the operational plan was in a constant state of change.[113]

Despite all these important shifts and improvements, the IA's attitude towards Signals Intelligence was inadequate. As Major General Yashwant Deva put it, "…the concept of tactical signal intelligence was only accepted in 1986."[114] Indeed, in 1983 as Chief Signal Officer of the 16 Signals Corps he was the first to write about the significance of tactical signals intelligence. Before Operation Pawan in Sri Lanka, most SIGINT was limited to strategic and national intelligence. Based on the analysis of Deva, there was extensive signal reconnaissance testing undertaken along the entire breadth of the India-Pakistan border to ascertain its effectiveness.

In 1986 under the leadership of General Sundarji on the recommendation of the 18 Corps were "dedicated signal intelligence" units established to be part of the IA's "holding corps".[115] The "holding

corps" are "static" defensive formations consisting mostly of infantry divisions and forward deployed against Pakistan.[116] Tactical Signal Intelligence supports the tactical commander. The tactical commander has to be authorised to acquire it and following its acquisition only, the commander is competent to assess the authentication, validation and evaluation. "This cannot", as Deva put it, "be done at the higher echelons of hierarchy. Research and Analysis Wing and Signal Intelligence Directorate (SID) should concentrate on strategic signal intelligence and leave tactical signal intelligence to commanders in the field."[117] The SID is a tri-service organisation. At best even if apex-level commanders did involve themselves in the mission or operation at hand, it could at best be to corroborate information and support the operational or tactical commander's execution of a mission or operation. Among Indian Defence technologists at least dating back to the 1990s, there has been recognition of the importance of networked computer and digital communications in support of military operations and the significance of a C2 architecture that is well adapted to exploiting the emerging communications and sensor technologies. [118]

The IA maintains a range of SIGINT and EW capabilities,[119] although the extent of their strength at the strategic, operational and tactical levels is variable. In terms of organisation, the IA's SIGINT units operate as part of a two-level structure. The IA has six geographical commands, which include Northern, Eastern, Southern, Central and South Central and the Army Training Command known as ARTRAC.[120] To be sure, India does have an Andaman and Nicobar Command (A&NC), which is a tri-services command, which potentially could serve as test bed synchronising CW and EW for joint operations. However, for the purpose of this analysis our focus will only be on each of the Army's five Commands. The Eastern and Northern Command are the most crucial for IA's defence against China.

While the Directorate General of Military Intelligence (DGMI) and also known as the Military Intelligence Directorate (MID) plays a role in collecting tactical intelligence particularly on Pakistan, but its role is minor relative to the Signals Corps.[121] The latter role focused on gathering ELINT and strategic intelligence. The DGMI is not independent, collecting and disseminating intelligence mostly from other agencies, and liaising between Naval and Air Intelligence Directorates, Research and Analysis Wing (R&AW) and the Intelligence Bureau (IB). The Corps of Signals is a tri-service organisation based in New Delhi. In the 1990s, it is estimated the Corps of Signals handled roughly 40 percent of India's SIGINT activities and functions.[122] Today most of the tasks and functions of the MI have been transferred to the National Technical Reconnaissance Organisation (NTRO) and the Research and Analysis Wing (R&AW). The former is responsible tracking and monitoring all cellular and Radio Frequency (RF) communications.

The Indian Air Force (IAF) and the Indian Navy (IN) have their own SIGINT capabilities. However, the MID under its Central Monitoring Organisation (CMO) is the largest repository overseeing Electronic Intelligence (ELINT) and Communications Intelligence (COMINT).[123] In recent decades the weaknesses of IA's SIGINT were seen in counterinsurgency operations: India's involvement in Sri Lanka and, subsequently, in Kashmir. Reliance on HUMINT is considerable even today as opposed to SIGINT in Counterinsurgency (CI) and Counter-terrorist (CT) and true for the experience of states across the world.[124]

Today UAVs can perform to a limited extent some of the tasks, which ground-based stations cannot in mountain terrain such as Kashmir. Their capacity to loiter at high altitudes makes them a good platform for transmitting surveillance data, ELINT information and relaying communications between two stations beyond the line of sight as

between the radar stations and AWACs and Command and Control Center (C&CC).[125] There are considerable restrictions on ground-based radars in mountain terrain as mountain folds or valleys and mountain shadows render radar coverage limited.[126] Even airborne AWACs on their own will find it difficult to detect hostile aircraft, which was visibly demonstrated in the February 2019 air battle between the Indian Air Force and the Pakistan Air Force (PAF).[127] The IAF's MiG-21s went undetected by the PAFs AWACs as the MiGs emerged from the shadows of the Pir Panjal mountain ranges.[128] Therefore, UAVs when paired with AWACs and Airborne Early Warning (AEW) platforms will help redress the radar detection challenges.[129] Even ground-based EW capabilities are and will be at a disadvantage, because they are likely to be "masked by terrain".[130] These capability requirements are as applicable along the mountainous Sino-Indian border as they are in Kashmir against Pakistan. To produce a synergistic effect between EW and CW an air-gapped network could be subjected to intrusion through the EMS, before malware is injected into the network.[131]

Beyond the absence of an integrated conception of CW and EW, there is a deficit in the command structure of the IA. The command over Signals in Operation Pawan in Sri Lanka in the 1980s again revealed the importance of unified command. Initially, the IA did assign the mission to a single operational commander. However, this effort became too centralised for execution, if not in intent. If the IA were to move towards integrating CW with EW, it would also need a single operational commander to oversee all combined CW-EW activities and personnel within the domain of conventional military operations. As one former IA officer put it, "In order to keep pace with evolutionary changes in tactical doctrine, improvements in army command and control (C2) are required. The rapidly changing combat environment will impose severe time pressures on the staff and the commander."[132]

As of today, the Indian government has organisationally placed information related operations primarily under the rubric of intelligence and staff commands of each of the service manage their respective CW and EW. It also reflects an acute dilemma in regards to the linkage between CW and EW and where they stand in relation to each other. The challenge that the IA and the MoD face lies in the future. All prospective information based operations will need integration with traditional land warfare military operations; absent a single operational or joint force commander to execute integration, this will be a difficult aim. Generally, electronics, cyber, information and electromagnetic spectrum based operations are consequential to the communications, intelligence and the operational segments of the defence and national security establishments. The IA's Corps of Signals is a vital source of expertise in both the cyber as well as the electronic warfare domains. It will be the source of supply personnel to both the recently established DCA and an Army-centred cyber corps.[133]

However, if the MoD and the larger national security establishment see CW in particular, if not EW functionally as an exclusively intelligence-related activity and view the EW domain and cyber domains as discrete, then they risk overlooking the complementarities between cyber and EW and the opportunities to leverage and synchronise them for kinetic land operations. They also risk undercutting the role of the army commander in integrating cyber and electronic warfare capabilities across multiple lines of operation. The commander's role has to be defined clearly, if the IA is to exploit the EW and CW capacities in support of its missions. In the event India establishes more integrated commands like the A&NC, the inter-services theatre commander will need greater authority to integrate EW and CW for greater network-centricity. Authority has to percolate to division and brigade level. At these echelons, organic EW and CW capabilities will be necessary.

Indeed, China has the organic capabilities in this regard, whereas India's EW capabilities are still very weak.

At one level, it makes sense for the MoD, IA Service Headquarters and the intelligence establishment to view and treat cyber specifically as a competency of the intelligence community, which is entrusted to protect critical national infrastructure reliant on information systems, government agencies such as ministries, and the national internet and cyberspace. For the IA, cyber's role in support of land operations and IA's other missions is crucial.

As of today, the IA's EW capacities are still limited and consist of EW groups/units.[134] Some of them are available at the corps level.[135] Consequently, these EW units, which are scarce, are placed directly under Command Headquarters of the IA for efficiency. The EW groups are deployed primarily for electronic attack (EA) and "exploit" functions. As is evident, CW and EW perform separate operational roles. As opposed to the IA, the Indian Air Force (IAF) and the Indian Navy (IN) focus almost all their EW effort on integrating and employing platform-based non-communication (anti-radar) capability.[136] The IA has to consider undertaking platform-based employment of EW. In the realm of electronic warfare capabilities, India does possess ground-based vehicle mounted EW systems. The Indian Army fields electronic warfare platforms Samyukta[137] and the Himshakti electronic warfare system. In 2016, the latter was under advanced stages of trialling, designed for use in mountain terrain,[138] and possibly now deployed. Yet beyond these specialized mobile EW units of this kind, which are logistically cumbersome, the IA will need to continue adapting tanks and even motorized vehicles and unmanned aerial systems for electronic and cyber warfare.

There are weaknesses confronting the IA in EW. The IA's Signals Intelligence Directorate in 2017 did draw the government's attention to

the need for Man portable Radio Frequency Relay communications equipment for High Altitude operations.[139] In mountain terrain as opposed to desert terrain, line of sight communications is crucial.[140] As of today, the IA fields logistically burdensome equipment and EW detachments. Miniaturisation is the way forward for radio communications in mountain terrain as the IA's Directorate General of Signals observed, "Thus to reduce the logistics effort and improve availability, there is an emergent need to reduce the size of Radio Relay Frequency Equipment to make it more man portable".[141] Serving IA officers have reinforced the importance of miniaturisation in sensors, weapons and platforms for the detection, interception and more broadly the conduct of operations across the electromagnetic and information domains.[142] Public sector monopolies such as the Bharat Electronics Limited (BEL), if not out rightly ill equipped to meet the demands of miniaturisation and the effective integration electronics with platforms such as tanks, remain a challenge and shortcoming. A further weakness the IA faces relative to the PLA is in the area of encryption.

Encryption is crucial for the preservation of secrecy in communications. In order to break every conceivable encryption; quantum computing is the solution or at least the way forward. Unlike current computers based on classical physics within the IA Signals Corps inventory, quantum computers can break encryption techniques that are derived from mathematical algorithms.[143] Classical computers are built on algorithms developed by humans, whereas quantum computing whose properties consist of qubits or quantum bits are a derivative of quantum mechanics, which is intrinsic to nature. The value of qubits integral to quantum computing lies in processing information more rapidly and accurately.[144]

In addition, cyber attacks can be launched through sound waves. For instance, wireless network entry points are increasingly at risk of being

bypassed and penetrated. One way this penetration becomes increasingly feasible is through "side channel" attacks. The target device's characteristics can be identified such as the amount of power it consumes, duration it takes to perform a set of functions, the intensity of light it emits or other electromagnetic emissions it radiates.[145] Due to the miniaturisation of computers within electronic devices, the challenge has become more acute if they are connected to the internet or some non-internet based communications network. Sound could be used to interfere with accelerometers, which measure acceleration.[146] Navigation systems could be affected by it as well, which measure distance and movement, which are vital to military operations. Other examples include a swarm of drones that emit high-powered soundwaves. As shown earlier, China does possess a range of drone and UAV-related capabilities, which will play a key role in support of a potential Chinese land campaign against India. Low-cost UAVs are part of the PLA's swarm drone strategy. Significant tactical and operational advantages will accrue from the employment of miniaturised drones and UAVs, if they are well coordinated for executing missions.[147] These sound waves could potentially interfere with equipment containing accelerometers generating mass denial of service attack thereby compromising military operations involving high-powered electromagnetic radio waves.[148] These changes have in part been brought about by miniaturisation, which is a key developmental innovation propelled by advances in nanotechnology and microelectronics.[149] The Size, Weight and Power (SWaP) requirements, which are at the heart of miniaturisation, presents enormous challenges for the defence microelectronics industry.[150] Guidance and navigation of Precision Guided Munitions (PGMs) can be disrupted or disabled using advances in EA techniques. Only advances in microelectronics that are rugged, but also "purpose-built" for specific missions and meet the space constraints of PGMs can make the guidance and navigation safe from EA.[151]

Miniaturisation is vital for platforms in mountain warfare, which is precisely the deficiency India faces against China.

V. CONCLUSION

While China's People's Liberation Army (PLA) has not articulated a formal doctrine on cyber and electronic warfare, it has engineered, through the establishment of the Strategic Support Force (SSF) a shift in its command structure. The establishment of the SSF would be meaningless, however, without a commensurate shift in China's C2 architecture. The establishment of theatre commands is tailored to exploit the creation of a unified information warfare service in the form of the SSF. To be sure, this paper has only assessed the link between EW and CW (or what China calls INEW) and its relationship to ground warfare. China is ahead in recognising both conceptually and technologically, the importance of the linkages between EW and CW.

The IA and India, on the other hand, have yet to fully acknowledge the convergence between cyber warfare and electronic warfare, whether doctrinally, operationally or organisationally. The Indian Army's thinking about the relationship between CW and EW and how both can play out through the electromagnetic spectrum is, at best, evolving. More thought will have to be given to whether the PLA's INEW approach is suitable and most effective to meet the needs of the IA's ground warfare operations. More importantly, does it need a unified information warfare service like the PLASSF?

Consequently, some clear recommendations are in order. First, injecting greater doctrinal clarity on CW and EW will help the IA meet its requirements, train, and equip its ground warfare units. The Corps of Signals will and should be the principal source of expertise for training for CW and EW.

Second, based on the foregoing analysis, developing organic CW and EW capabilities is vital for the Indian Army at different echelons from the corps to brigade level. At the tactical level, more SIGINT personnel will need to be trained in the cyber and electronic domains. Electronic warfare and cyber warfare officers should be embedded in the lower echelons of the chain of command.

Third, the MoD and the IA will need to involve India's civilian Information Technology (IT) industry and, more broadly, the private sector and top technical education institutions in how the technical capacities in the civilian economy could be applied to solving some of the technical challenges in EW and CW. More clarity is needed about the role and functions of the incipient Defence Cyber Agency (DCA), particularly what role it will have in support of the IA's missions and operations. Finally, it is critical for India to establish theatre commands if the country is to effectively employ its emerging CW and EW capabilities as part of its ground warfare strategy against China. ORF

ANNEX

Table 1. Electronic and Cyber Warfare Capabilities

Capability	*Methods*	*Indicators*	*First-order effects*
Denial of Service Attack	Overwhelming a web service, server, or other network node with traffic to consume resources preventing legitimate traffic	Abnormal network performance, inability to navigate web and access sites, uncontrolled spam, and system reboots	Degraded network capabilities ranging from limited operational planning to total denial of use
Network Penetration	Man-in-the-middle attacks, phishing, poisoning, stolen certificates, and exploiting unencrypted messages and homepages with poor security features	Unfamiliar e-mails, official looking addresses requiring urgent reply, internet protocol packets replaced, non-legitimate pages with the look of legitimate sites, directed moves from site to site, requests to upgrade and validate information, and unknown links	Uncontrolled access to networks, manipulation of networks leading to degraded or compromised capabilities that deny situational awareness or theft of data
Emplaced Malware (virus, worms, spyware and rootkits)	Phishing, spearphishing, pharming, insider threat introduction, opensource automation services, victim activated through drive-by downloads and victim	Pop-ups, erroneous error reports, planted removable storage media, unknown email attachments, changed passwords without user knowledge,	Spyware and malware on affected systems allow electronic reconnaissance, manipulation, and degrading system performance

	emplaced data storage devices	automatic downloads, unknown apps, and degraded network	
Disrupt or deny information system in the EMS	Prevent friendly antennas from receiving data transmitted in the EMS by using military or commercially available highpowered lasers, high powered microwaves, and repurposed or reengineered communications systems	Symptoms may not be evident if passive; may manifest as transmission interference, software or hardware malfunctions, or the inability to transmit data	Degraded or complete denial of service in ability to control the EMS denying situational awareness and degrading operational planning

Source: U.S. Army Field Manual for Cyber and Electronic Warfare Operations, 2017

Table 2. Analogies between EW and Cybersecurity Domains

EW Domain	Cyber Domain
Radar Warning Receiver	Intrusion Detection System
Track Quality	Integrity of Data Processes
Detection and Identification	Access to operating systems, or hardware
False Targets, False position/ velocity data	Data Corruption, Hacking, loss of system control
Threat Activity	Threat Activity

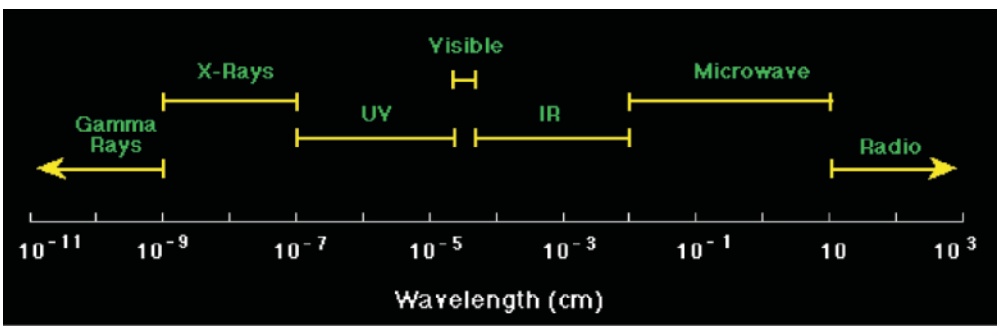
Source: R. Gutierrez del Arroyo, "The Merge of Electronic Warfare and Cybersecurity", NATO-STO.

Table 3. Key activities of Cyber Attacks and Cyber Defence

Attack Sequence	**Discover**	**Implement**	**Exploit**
	Gather Information on System Hardware, software, users and operations to identify how best to attack the system.	Execute the attack to gain initial access or expand existing access.	Use access to attack the confidentiality, integrity, or availability of the system.
Defence Sequence	**Protect**	**Detect**	**Respond/Recover**
	Put in place controls and processes to prevent unauthorised access.	Take steps to identify suspicious cyber activity.	Take steps to mitigate damage, end attack, and restore the system to full operation.

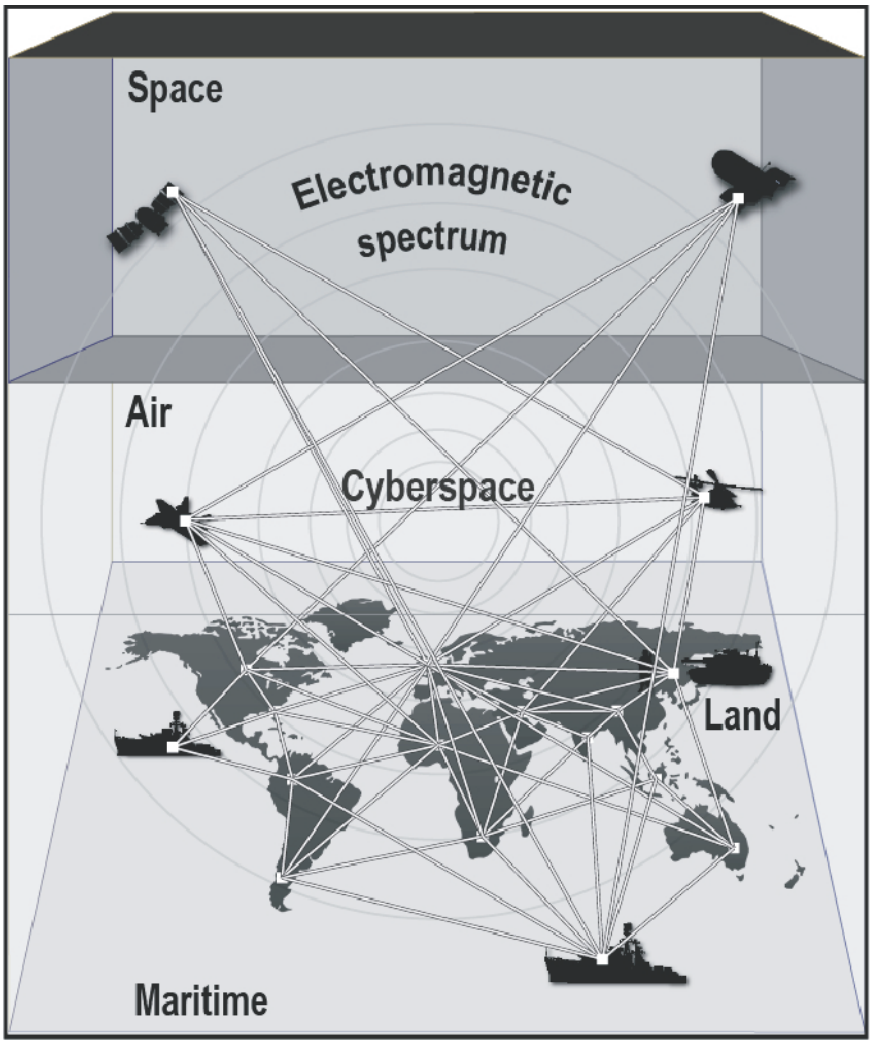
Source: Government Accountability Office Analysis of Defence Information, Washington D.C.

Figure 1. The electromagnetic spectrum



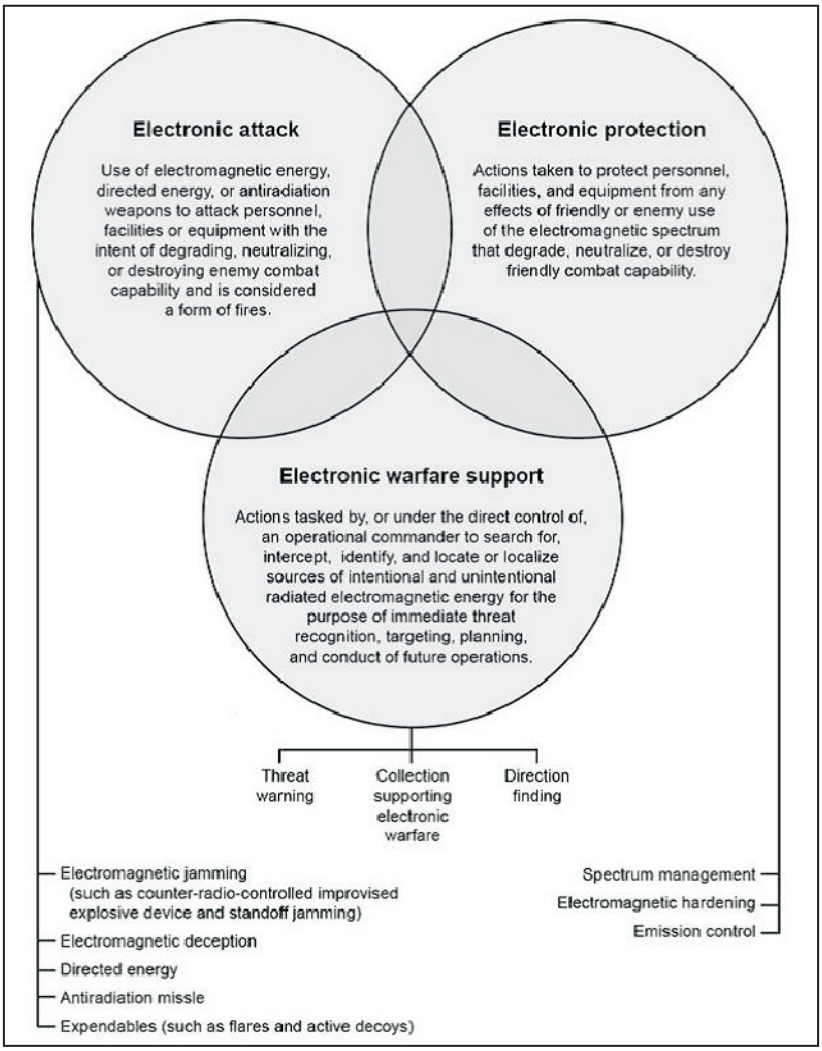
Source: University of Rochester

Figure 2a . Relationships among the five domains and the electromagnetic spectrum



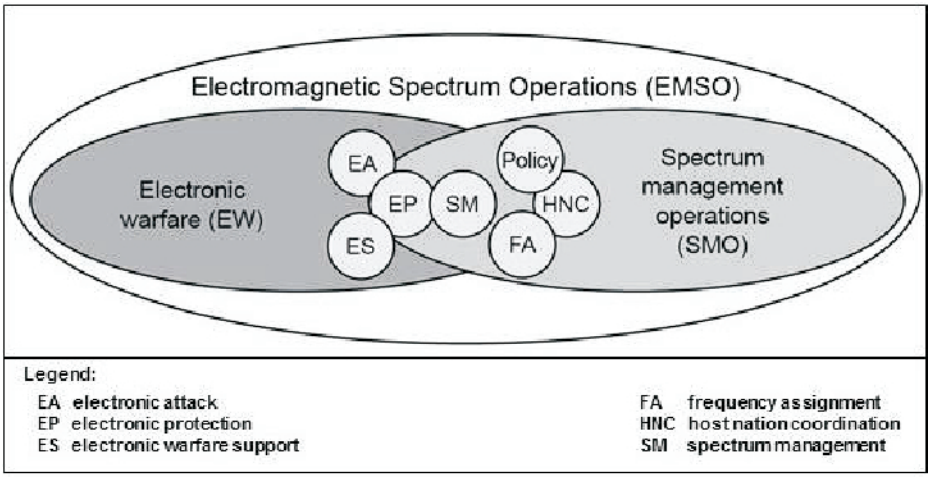
Source: US Army Field Manual 3038, Cyber Electromagnetic Activities, 2014

Figure 2b. Relationships among the five domains and the electromagnetic spectrum



Source: Cyberspace and Electronic warfare operations, U.S. Army Field Manual, 2017

Figure 3. Electromagnetic Spectrum Operations



Source: Cyberspace and Electronic Warfare Operations, U.S. Army Field Manual, 2017

ENDNOTES

1. David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd edition, (Washington D.C.: CCRP, 2000), pp. 10-15
2. See James Mulvenon, "The PLA and Information Warfare", (Santa Monica: RAND Corporation, 1999), pp. 175-186 https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/CF145.chap9.pdf.
3. Cited in Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min and Bruce J. Held, *Redefining Information Warfare Boundaries For an Army In a Wireless World,* (Santa Monica: CA, RAND Arroyo Center, 2013), p. 6
4. *Department of Defense (US) Dictionary of Military and Associated Terms*, Washington D.C. January 2019, p. 59.
5. *Cyberspace and Electronic Warfare Operations,* Field Manual No. 3-12, Headquarters Department of the Army, Washington D.C., April, 2017, pp. 19-20
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Neil C. Rowe and Hy S. Rothstein, "Two Taxonomies of Deception for Attacks on Information Systems", *Journal of Information Warfare,* 3 (2), July 2004, pp. 27-39.
14. *Cyberspace and Electronic Warfare Operations*, p. 74
15. R.A. Poisel, *Introduction to Communication Electronic Warfare Systems,* (Boston: MA, Artech House, 2002), See also M.J. Ryan and M.R. Frater, *Tactical Communications for the Digitised Battlefield,* (Boston: MA, Atech House, 2002).
16. Anthony E. Spezio, "Electronic Warfare Systems", *IEEE Transactions on*

Microwave Theory and Techniques, Vol. 50, No. 3, March 2002, p. 633

17. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations,* (Washington DC, Headquarters, Department of the Army, April 2017), p. 32
18. Spezio, "Electronic Warfare Systems", p. 633.
19. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations,* pp. 31-32
20. Ibid.
21. Ibid.
22. Ibid.
23. Ibid.
24. Ibid
25. Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min and Bruce J. Held, *Redefining Information Warfare Boundaries For an Army In a Wireless World,* p. 52
26. J.R. Wilson, "Electronic warfare technology heading-up the battlefield", *Military&Aerospace,* 1 August 2018 https://www.militaryaerospace.com/articles/print/volume-29/issue-8/special-report/electronic-warfare-technology-heading-up-the-battlefield.html
27. Ibid.
28. *Department of Defense (US) Dictionary of Military and Associated Terms,* p. 69.
29. *Cyberspace and Electronic Warfare Operations FM 3-12,* (Washington DC: Headquarters: Department of the Army, 2017), p. 30
30. Lt. Col. Jose R. Gutierrez del Arroyo, "The Merge of Electronic Warfare and Cybersecurity Test", Science and Technology Organisation, North Atlantic Treaty Organisation, p. 6 (accessed 5 April, 2019).
31. Vahid Behzadan, "Cyber-Physical Attacks on UAS Networks-Challenges and Open Research Problems", Department of Computer Science, University of Nevada, 4 February, 2017, pp. 2-4, https://arxiv.org/pdf/1702.01251.pdf, See also
32. Ibid, p. 5
33. Ibid.
34. J.W. Rooker, "Satellite Vulnerabilities", United State Marine Corps, Command and Staff College, Marine Corps Combat Development, Marine

Corps University, Virginia, p. 5 https://apps.dtic.mil/dtic/tr/fulltext/u2/a507952.pdf

35. Vahid Behzadan, "Cyber-Physical Attacks on UAS Networks-Challenges and Open Research Problems", p. 6
36. Cited in Arroyo, "The Merge of Electronic Warfare and Cybersecurity Test".
37. L. Col. John T. Arnold, USAF, "The Shoreline: Where Cyber and Electronic Warfare Operations Coexist", Air War College, Air University, Maxwell AFB, Alabama, 2009, p. 7.
38. Ibid.
39. Ibid.
40. Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace Or Emerging Threat?* Strategic Studies Institute, (Carlisle: PA, United Stated Army War College, 2001), p. 17
41. Ibid.
42. Lt. Colonel Timothy L. Thomas (Retd. US Army), "China's Electronic Strategies", *Military Review,* March-April, 2001, p. 50
43. James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organisations and Capability", in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Mission Other Than Taiwan,* Carlisle PA: Strategic Studies Institute, April 2009, pp. 259-261.
44. Lt. Colonel Timothy L. Thomas (Retd. US Army), "China's Electronic Strategies", p. 50-55.
45. Bryan Krekel, Patton Adams and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", U.S.-China Economic and Security Review Commission by Northrop Grumman, Northrop Grumman, 7 March, 2012, p. 25.
46. Ibid, p. 23.
47. Ibid, p. 23.
48. Ibid, p. 24.
49. *China Military Power: Modernizing a Force to Fight and Win,* (Defense Intelligence Agency, Washington D.C., 2019), pp. 27-28
50. Ibid.

51. Ibid.
52. Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military", *The Diplomat,* 1 April, 2017, https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/
53. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", Center for the Study of Chinese Military Affairs", Institute for National Strategic Studies, China Strategic Perspectives, No. 13, Washington D.C.: National Defense University, October 2018, pp. 23-33
54. Cited in "China reorients strategic military intelligence", *IHS Markit: Janes Intelligence Review,* 2017, p. 4, https://www.janes.com/images/assets/484/68484/China_reorients_strategic_military_intelligence_edit.pdf
55. Ibid, p. 1
56. Ibid.
57. Ibid.
58. *China Military Power: Modernizing a Force to Fight and Win,* Defense Intelligence Agency, Washington D.C., 2019, pp. 45-46
59. Ibid.
60. Ibid.
61. John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", p. 25.
62. Ibid. See also "China Reorients Strategic Military Intelligence".
63. Ibid.
64. "China orients strategic military intelligence", p. 3
65. Scott D. Applegate, "Cyber and Political Hackers – Use of irregular Forces in Cyberwarfare", *IEEE Security and Privacy Magazine,* 9 (5) September, 2011, p. 19, See also Nicholas Lyall, "China's Cyber Militias", *The Diplomat,* 1 March, 2018, https://thediplomat.com/2018/03/chinas-cyber-militias/
66. See for example why a cyber C2 which must balance offence and defence and be "dynamic" and "anticipatory", Norman R. Howes, Michael Mezzino and John Sarkesian, "On Cyber Warfare Command and Control Systems", Department of Defense, Washington D.C. 2004, p. 5 http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/118.pdf

67. Elsa Kania, "The PLA's Unmanned Aerial Systems: New Capabilities for a "New Era" of Chinese Military Power", (Washington D.C: Chinese Aerospace Studies Institute, 2018), pp. 10-13

68. "Xi Stresses military-civilian integration in new era", *Xinhuanet,* 3 March, 2018, http://www.xinhuanet.com/english/2018-03/02/c_137011871.htm

69. See Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era", *Delivered at the 19th National Congress of the Communist Party of China, October 18, 2017,* p. 48, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf

70. Brian Lafferty, "Civil-Military Integration and PLA Reforms", in *Chairman Xi Remakes the Military* in Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow (eds.), (Washington D.C: National Defence University Press, 2019), p. 633

71. A sample of some of the literature include Cherian Samuel and Munish Sharma, *India's Strategic Options in a Changing Cyberspace,* Institute for Defence Studies and Analyses, (New Delhi: Pentagon Press 2019) <https://idsa.in/system/files/book/book_indias-strategic-options-in-cyberspace.pdf>,

72. Arun Mohan Sukumar and Col. R.K. Sharma, "The Cyber Command: Upgrading India's National Security Architecture", Special Report, Observer Research Foundation, New Delhi, 2016, p. 7

73. Deepak Sharma, "China's Warfare Capabilities and India's Concerns", *Journal of Defence Studies,* vol. 5, No. 2, April 2011, pp. 62-76.

74. Ibid.

75. *Indian Army Land Warfare Doctrine,* Army Headquarters, New Delhi 2018, p. 10

76. Ibid.

77. Ibid.

78. Brigadier Sapan Kumar Chatterji, "An Overview of Information Operations in the Indian Army", (Alabama: Air University, 2008), p. 13.

79. Lt. Gen. R.S. Panwar, "Towards and Effective and Viable Information Warfare Structure for the Indian Armed Forces", 16th Major General Samir Sinha Lecture, 2018, United Services Institution, New Delhi, 2018.

80. Lt. Gen. Vinod Bhatia (Retd.), "21st Colonel Pyara Lal Memorial Lecture, 2017: Transforming the Indian Armed Forces for Meeting Future Security Challenges" *The United Service Institution of India*, 20 September, 2017, New Delhi.

81. On China see Shannon Tiezzi, "It's Official: China's Military Has 5 New Theater Commands", *The Diplomat,* 2 February, 2016, <https://thediplomat.com/2016/02/its-official-chinas-military-has-5-new-theater-commands/>, On India and the ANC see Rahul Singh, "Andaman defence commander gets power over all three services", *Hindustan Times,* 12 May, 2018, <https://www.hindustantimes.com/india-news/andaman-defence-commander-gets-power-over-all-three-services/story-LLhvEAs1CSF9nO2sVrTmBK.html>

82. Lt. Gen. V.K. Kapoor(Retd), "An Operational Perspective of Network Centric Warfare in the Indian Context", *The United Services Institution Journal,* vol. CXXXVI, January-March 2006, p. 7

83. Ibid.

84. Nimesh S. Raijada and Shrinivas V. Mugali, "Vetronics Architecture with in-vehicle Networking", *Defence Science Journal,* Vol. 69, No.3, May 2019, p. 237.

85. Ibid, pp. 237-238.

86. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation", *The US-China Economic and Security Review Commission,* (Washington, DC: Northrop Grumman, 2009), p. 10.

87. Lt. Gen. R.S. Panwar, "Strategic Thinking for Security: Defending the National Cyberspace – Part II", Data Security Council of India, 24 January, 2018, <https://blogs.dsci.in/strategic-thinking-for-cyberspace-security-part-ii/>

88. "India set to have Defence Cyber Agency in May; Rear Admiral Mohit to be its first chief", *ANI News,* 30 April, 2019 https://www.aninews.in/news/national/general-news/india-set-to-have-defence-cyber-agency-in-may-rear-admiral-mohit-to-be-its-first-chief20190430102739/

89. "India in Final Stages of Setting Up Defence Cyber Agency", *Economic Times,* 15 January, 2019 https://economictimes.indiatimes.com/news/defence/india-in-final-stages-of-setting-up-defence-cyber-agency/articleshow/67540186.cms?from=mdr

90. Ibid.
91. S.K. Sinha, "The Chief of Defence Staff", *Journal of Defence Studies,* Vol. 1, No. 1, August 2007, p. 135
92. Ibid.
93. Andrew Schoka, "Cyber Command, The NSA, and Operating in Cyberspace: Time To End The Dual Hat", *The War on the Rocks,* 3 April 2019. See also Elsa Kania, "PLA Strategic Support Force: The "Information Umbrella' for China's Military", *The Diplomat,* 1 April, 2017, https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/
94. Max Smeets, "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly,* Fall 2018, p. 92
95. *Joint Doctrine: Indian Armed Forces,* Headquarters, Integrated Defence Staff, Ministry of p. 36
96. *Land Warfare Doctrine – 2018,*
97. *Joint Doctrine: Indian Armed Forces,* Headquarters, Integrated Defence Staff, New Delhi, 2017, p. 48
98. Ibid, p. 49
99. Col. V.A. Subrahmanyam, *The Signals: A History of the Corps of Signals.* (New Delhi: Macmillan India Ltd., 1986), p. 99
100. Ibid.
101. Major General R.S. Chowdhary, *A Short History of the Intelligence Corps,* (Pune: Military Intelligence Training School Press, 1985), pp. 50-53
102. Ibid.
103. Ibid.
104. Subrahmanyam, *The Signals: A History of the Corps of Signals,* p. 101.
105. Major K.C. Praval, *Indian Army After Independence,* (New Delhi: Lancer International, 1987), p. 275
106. Ibid.
107. Ibid
108. Subrahmanyam, *The Signals: A History of the Corps of Signals,* pp. 100-101
109. Ibid, p.101

110. Ibid, p. 100.
111. Ibid, p. 158.
112. Ibid, p. 167.
113. Ibid, pp. 170-171.
114. Yashwant Deva, *Sky is the Limit: Signals in Operation Pawan,* (New Delhi: Pentagon Press, 2007), p. 184
115. Ibid.
116. For an incisive analysis of the Cold Start Doctrine, see Walter C. Ladwig III, "A Cold Start to Hot Wars? The Indian Army's New Limited War Doctrine", *International Security,* Vol. 32, No. 3, Winter 2007, pp. 159-160.
117. Deva, *Sky is the Limit: Signals in Operation Pawan,* p. 195
118. See for instance M.S. Viswanathan, "Tactical Military Communications Networks of the Future", *Defence Science Journal,* Vol. 43, No.1, January 1993, pp. 71-78.
119. Desmond Ball, "Signals Intelligence (SIGINT) in South Asia: India, Pakistan and Sri Lanka" Canberra Papers on Defence and Strategy, No. 117, (Canberra: Australian National University (ANU), 1996), p. 25.
120. "Commands", Indian Army Official Website, https://indianarmy.nic.in/Site/FormTemplete/frmTempMainPage.aspx?MnId=OTCZ/jAKb8UK0pwltsuqtw==&ParentID=9f5OQU0aRQp3hneDBh9T+w==&flag=9TshhKm6Ruy3n5n8XbW/eQ==
121. Manoj Joshi, "Signals Wars: Indian Capability in Perspective", *Frontline,* September 10, 1993, p. 76, See also *From Surprise to Reckoning: The Kargil Review Committee Report,* (New Delhi: Sage Publications India Pvt. Ltd, 2000), p. 115
122. Ibid.
123. Ibid.
124. See for example the American experience in Col. David J. Clark, "The Vital Role of Intelligence in Counterinsurgency Operations", Dissertation, US Army War College, Carlisle, PA, 2006, p. 2.
125. Lt. Colonel Piyush Kumar Sanwal, "UAVs – The Silent Force Multipliers in Future Air Defence Operations", *Journal of the United Service Institution,* Vol. CXLVIII, No. 614, October-December 2018, p. 578.

126. Ibid.
127. Shekhar Gupta, "What the IAF-PAF dogfight reveals", *Hindustantimes,* 27 March, 2019 https://www.hindustantimes.com/columns/opinion-what-the-iaf-paf-dogfight-reveals/story-dDa4H38Xtq7LPnj6DtkZRN.html
128. Ibid.
129. Lt. Colonel Piyush Kumar Sanwal, "UAVs – The Silent Force Multipliers in Future Air Defence Operations", p. 578.
130. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations,* p. 32
131. Lt. Gen. R.S. Panwar, "Towards An Effective and Viable Information Warfare (IW) Structure For The Indian Armed Forces", Unpublished paper, p. 9.
132. P.K. Mallick, "Staff System in the Indian Army: Time for Change", Manekshaw Paper, No. 31, 2011, Centre for Land Warfare Studies (CLAWs), New Delhi, p. 22
133. Interview with retired officer.
134. Lt. Gen. R.S. Panwar (Retd), "Towards and Effective and Viable Information Warfare Structure for the Indian Armed Forces".
135. Ajai Shukla, "Ministry of Defence strikes blow for private sector for defence", 20 January, 2013, https://www.business-standard.com/article/economy-policy/ministry-of-defence-strikes-blow-for-private-sector-in-defence-111070800032_1.html
136. Ibid.
137. "Samyukta" presented to the Army", *The Hindu,* 20 January, 2004, https://www.thehindu.com/2004/01/20/stories/2004012001721300.htm
138. *Annual Report: 2015-16,* Ministry of Defence, New Delhi, p. 87.
139. *Army Design Bureau: Compendium of Problem Statements,* Confederation of Indian Industry (CII), Volume 2, New Delhi, 2017, p. 48
140. Ibid.
141. Ibid.
142. Brigadier Vivek Verma, "Non Contact Warfare (NCW) – Managing Conflict in 21st Century", *Journal of the United Service Institution,* Vol. CXLIX, No. 615, January-March, 2019,, See also for the importance of miniaturization

Lt. Col. Piyush Kumar Sanwal, "UAVs – The Silent Force Multipliers in Future Air Defence Operations, p. 581.

143. *Army Design Bureau: Compendium Problem Definition Statements,* Confederation of Indian Industry (CII), Volume 4, New Delhi, 2019, p. 9
144. David McMahon, *Quantum Computing Explained,* (Hokboken, NJ: John Wiley&Sons, 2007), pp. 11-13
145. Bill Buchanan, "The next cyberattack could come from sound waves", *The Conversation,* 28 March, 2017, https://theconversation.com/the-next-cyberattack-could-come-from-sound-waves-74716
146. Ibid.
147. Scott N. Romaniuk and Tobias Burgers, "China's Swarms of Smart Drones Have Enormous Military Potential", *The Diplomat*, 3 February 2018, https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential/
148. Ibid
149. Ahmad Lotfi, "Miniaturisation will lead to 'smart spaces' and blur the line between on and offline", *The Conversation,* 27 June, 2015, https://theconversation.com/miniaturisation-will-lead-to-smart-spaces-and-blur-the-line-between-on-and-offline-40428
150. Charlie Hudnall and Philip Fulmer, "Miniaturisation electronic warfare microelectronics to advance precision-guided weapon technologies", *Military Embedded Systems,* http://mil-embedded.com/articles/miniaturizing-precision-guided-weapon-technologies/
151. Ibid.

Observer Research Foundation (ORF) is a public policy think tank that aims to influence the formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, including academic and business leaders.

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000 Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org