Issue Brief

June 2024
No : 399

Entropy Warfare and PLA

Brigadier G Praveen, SM

CENTRE FOR LAND WARFARE STUDIES
CLAWS
VICTORY THROUGH VISION

Entropy Warfare and PLA

Abstract

Chinese President Xi Jinping announced a series of restructuring initiatives in 2015 to align China's military prowess with its regional and global interests and develop PLA as a world class force by 2049 (centennial year of PLA). Some of the major changes included the revamping of Central Military Commission (CMC), creation of PLA Strategic Support Force (PLA SSF, now PLA Information Support Force) and Theatre Commands, force reduction, and impetus for increased Integrated Joint Operations embracing disruptive technologies. China's Multi Domain Precision Warfare focuses on degrading enemy's will to resist by introducing absolute entropy through enmeshed pillars of national power augmented with civil military fusion. This essay examines the manifestation of Entropy Warfare in multiple domains.

Keywords: Entropy Warfare, Cognitive Warfare, PLA, PLA Information Support Force, PLA SSF, Multi Domain Precision Warfare, Psychological Warfare

We must come to terms with the fact that following yesterday's rules of war will not lead to today's (or tomorrow's) successes.

—General Stanley McCrystal

Introduction

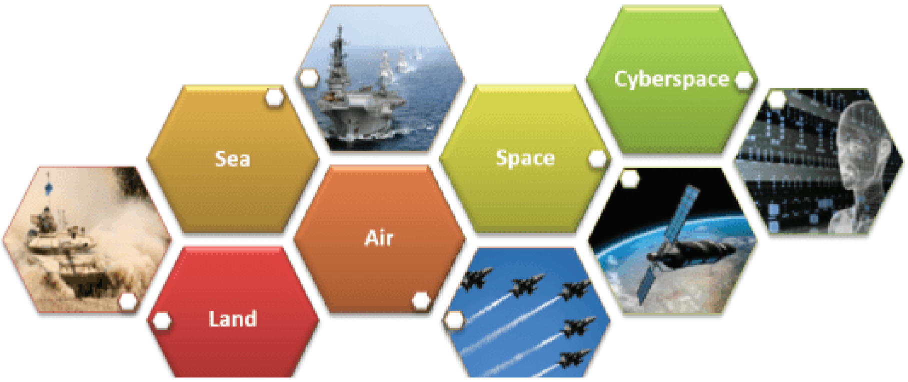
The advent of disruptive technology has seen introduction of phrases like Informatisation and later Intelligentization by the People's Liberation Army (PLA) which, in simple terms, is Artificial Intelligence (AI) enablement of PLA's systems, weapons, and platforms (Narang, 2019). The ongoing Russia - Ukraine war and Israel – Hamas conflict have seen strategists revisiting traditional literature on war and warfare - its nature and character (Esper, 2019). Irrespective of the names that are coined for emerging and predicted forms of warfare, an 'effects based perspective' would focus on the target(s) and unravel the physical manifestation of such lethal and non-lethal actions on the components of national will and combat capability. Entropy that is the measure of disorder or randomness of a system, would give an idea of the impact of such warfare at the target end. The aim of this paper is to explore the relevance of Entropy Warfare in the backdrop of Chinese Grey Zone warfare.

As autonomous weapons and systems creep into erstwhile human domains, discussions related to 'human in and out of the loop' and morality & legality of their employment will increase. Will there be a steep rise in localized wars with machines taking on most of the battle even as social media is modulated to influence and thereon defeat the enemy populace without physical capture of territory? Will "war as a means of policy by other means" be considered a cheaper and optimal option with the advent of smart technology and Chinese concepts *like san zhong zhanfa* or the Three Warfares? Will the templates of past, including Westphalian concept of Nation State and Clausewitzian constructs of largescale attrition hold true when state and non-state actors, empowered by emerging disruptive technology, wage warfare in the cognitive domain and expand the Grey Zone envelope?

What's in a Name? Relevance of Cognitive Domain

As strategists and war analysts categorize future engagements under Multi Domain Operations (MDO), Information Warfare, Grey Zone warfare, Cognitive Domain operations etc. the primary essence is that the cognitive component will play a more major role in deciding the outcome of conflict. Increased relevance of cyber, Electronic Warfare (EW) and cognitive spaces have seen some recommendations to replace Cyberspace with 'Infospace' (comprising Cyber, Electromagnetic and Cognitive dimensions) or to have two additional Electromagnetic and Cognitive domains (Panwar, 2021).

Figure 1: Present Domains of Multi Domain Operations



Source: https://futurewars.rspanwar.net/grey-zone-operations-in-the-infospace-dimension-imperatives-for-india/

Increased dependence on technology and systems, while improving the effectiveness of human- machine and human system teams, also offer a set of vulnerabilities which can be targeted by an adversary, thus exploiting the capabilities offered by the same niche technology. Though cognitive component has always been targeted as part of warfare, increased permeation of technology and capabilities of AI enabled systems will make it even easier to target and influence this component. While physical attrition, in terms of damage and destruction, would still add on to quantifying a war outcome, the achievements made by an adversary in the cognitive and relatively lesser quantifiable aspects of morale and cohesion is likely to have more impact.

Cognitive Domain operations (China, in this case) aims for 'mind superiority' through psychological warfare and seeks to use information to influence an adversary's cognitive functions, spanning from peacetime public opinion to wartime decision-making (Mustafaga,2019). Six technologies, divided across two categories, will be key in leveraging the cognitive domain for political and economic gains. The first category 'cognition' includes technologies that affect someone's ability to think and function while the second category 'subliminal cognition' covers technologies that target a person's underlying emotions, knowledge, willpower, and beliefs. These six technologies can be enumerated as :-

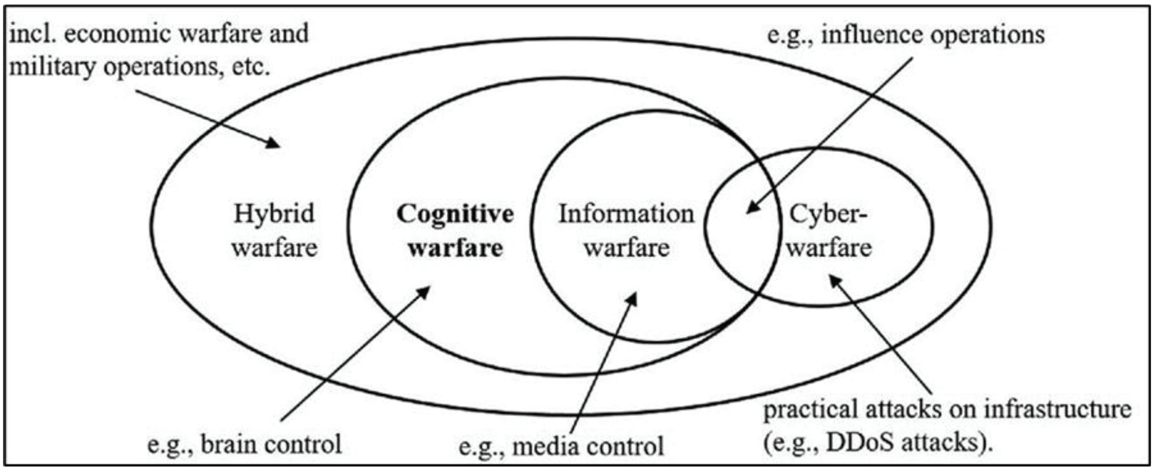
Table 1: Cognitive Domain Technologies

Cognitive Influence Technology	Subliminal Influence Technology
• **Cognitive survey technology** translates psychological indicators into quantifiable signals to assess the adversary's psychological disposition.	• **Subliminal information processing technology** collects and pre-treats content.
• **Cognitive interference technology** to conduct attacks against adversary's wellbeing, using lethal and non-lethal means.	• **Subliminal information implantation technology** used to implant subliminal messages into content and to create 'synthetic information'.
• **Cognitive strengthening technology** used to improve own cognitive abilities.	• **Subliminal information detection technology** for defensive operations against adversary using subliminal technology.

Source: https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/

Cognitive Warfare, in the context of Chinese actions in Taiwan has been defined as "activities undertaken to manipulate environmental stimuli to control the mental states and behaviors of enemies as well as followers in both hot and cold wars" (Hung and Hung, 2022). A distinction is made by these authors between Information Warfare where the inputs are controlled versus Cognitive Warfare where focus is on input as well as output in terms of cognition and behaviour, thereby implying incorporation of weaponized neuroscience to target deeper emotions and feelings. The US Department of Defense (DoD) annual report (Horowitz and Kahn, 2021) on Chinese Military Power outlines investments in machine learning and data analytics for areas including tactical and strategic decision support and AI-enabled wargaming.

Figure 2: Cognitive Warfare in Context


incl. economic warfare and military operations, etc.
e.g., influence operations
Hybrid warfare
Cognitive warfare
Information warfare
Cyber-warfare
e.g., brain control
e.g., media control
practical attacks on infrastructure (e.g., DDoS attacks).

Source: https://doi.org/10.1093/jogss/ogac016

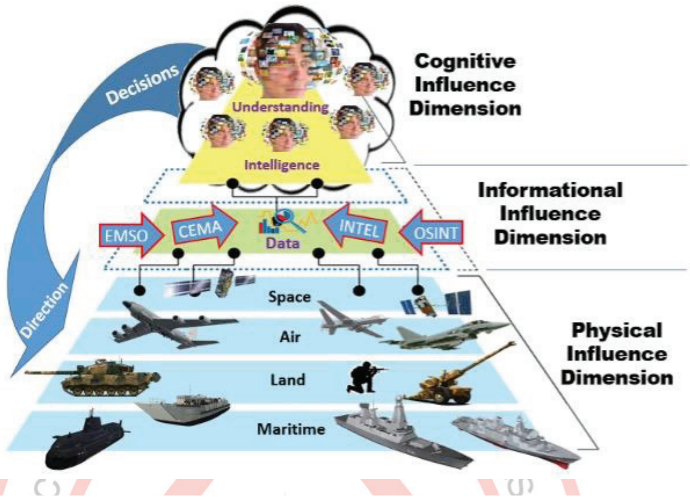
The report also describes continued Chinese investments in autonomous air, ground, and naval systems, some with limited AI capabilities and the use of AI for social media analysis and propaganda. The report also gives out basic and applied research priorities for China in the military AI space moving forward such as "brain-inspired software and hardware, human-machine teaming, swarming, and decision making".

Psychological Warfare (targeting human cognition) has been classified as one of the seven pillars of Information Warfare (Libicki, 1995). Another model by Crilly and Mears suggests adding "physical, informational, and cognitive influence **dimensions**" to the four physical **domains** of land, air, maritime and space, are as follows (Crilly and Mears, 2022):-

- ***Physical Influence Dimension.*** Contains four traditional domains of air, land, sea and space in a battle for physical territory.

- ***Informational Influence Dimension.*** Contains the virtual 'effects' groupings of information operations, cyber and Electromagnetic Spectrum (EMS) weapon systems in a battle for information.
- ***Cognitive Influence Dimension.*** Contains both individual and collective societal human thoughts in a battle for the human brain or cognition.

Figure 3: Influence Dimensions and Physical Domains

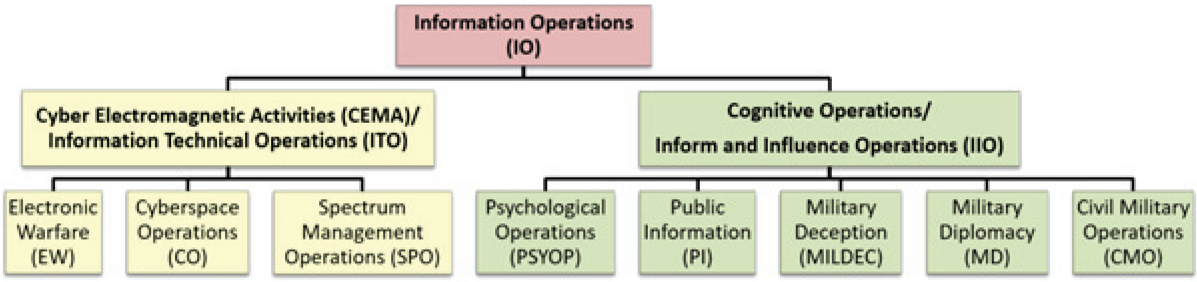

Decisions
Understanding
Intelligence
Cognitive Influence Dimension
EMSO
CEMA
Data
INTEL
OSINT
Informational Influence Dimension
Direction
Space
Air
Land
Maritime
Physical Influence Dimension

. **Source: https://wavellroom.com/2022/01/26/mddo/**

The Information Warfare Doctrine of the Indian Army, promulgated in 2010, has Psychological Warfare, Cyber and Electronic warfare under one umbrella while some Indian scholars refer to Information Warfare as consisting of defensive and offensive elements including operational security (OP SEC), EW, psychological operations, deception, physical attacks on information structures (Ahluwalia, 2020).

An alternate explanation of the various forms of Information Warfare has also been given with a distinction between **Information Technical Operations (ITO) and Inform and Influence Operations (IIO)** wherein the former needs technical expertise and the latter, an acute understanding of social studies and human behaviour (Panwar, 2021).

Figure 4: Nuanced Organogram of Information Operations


Information Operations (IO)
Cyber Electromagnetic Activities (CEMA)/ Information Technical Operations (ITO)
Cognitive Operations/ Inform and Influence Operations (IIO)
Electronic Warfare (EW)
Cyberspace Operations (CO)
Spectrum Management Operations (SPO)
Psychological Operations (PSYOP)
Public Information (PI)
Military Deception (MILDEC)
Military Diplomacy (MD)
Civil Military Operations (CMO)

Source: https://futurewars.rspanwar.net/grey-zone-operations-in-the-infospace-dimension-imperatives-for-india/

Entropy Warfare

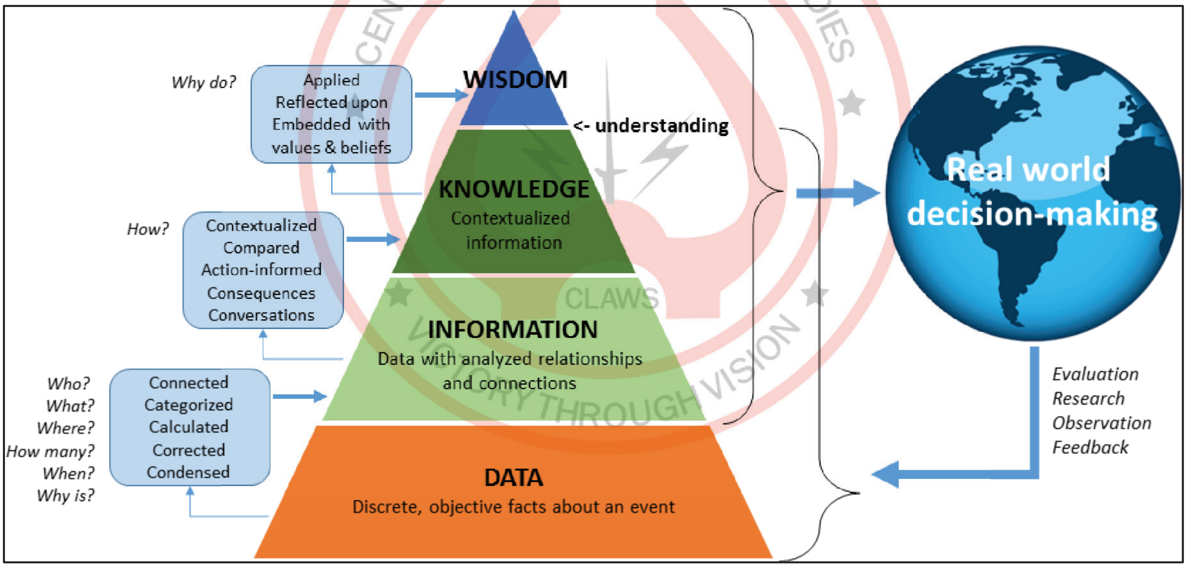
Instead of deconstructing the types of warfare, a more quantifiable approach would be to see the impact or effects of these forms of warfare on target systems. The main aim of war has always been to bend an enemy to one's will and a means to that end is to defeat the enemy's ability to resist (Herman, 1999). Since the target is enemy's will and cohesion, the thermodynamic term of 'entropy', a measurable physical property that is most associated with uncertainty, becomes relevant. **Entropy** is a measure of the disorder or randomness of a system, and it tends to increase over time. Entropy warfare derives its origin from the fact that an entity or military force must maintain certain cohesive properties grounded on orderly construction and operation. In military parlance, one factor that is consistently identified as key to military strength is the 'notion of unit cohesion', often expressed as esprit de corps, with certain indicators being morale, moral influence, training, or discipline. Once a unit starts losing cohesion, its entropy level increases until, at maximum entropy, it becomes a mob of individuals incapable of coordinated combat action. Same would be the case for a Nation as well as and when the national identity is challenged and seeds of dissidence deeply ingrained.

Unlike the Clausewitzian focus on friction in battlefield, the entropy warfare model focuses on the **combined effect of friction, disruption, and lethality on a unit or team behaviour** (Herman, 1999). Friction comprises those activities the unit performs that increase its entropy level. Disruption includes those activities conducted by the enemy to expand the unit entropy level while Lethality is the firepower a unit must directly use to reduce an enemy through physical contact. Combination of friction and disruption would be like psychological warfare, which would cause disorganization. A combination of lethality and disruption would be targeting a commander or a communication node whereas targeting an essential vehicle column or a logistic link would be a combination of lethality and friction. Combined application of all three components would result in extreme entropy and breakdown of targeted unit/ agency. Essentially, this is a shift from traditional attrition based models with increased focus on other intangible aspects like cognition, cohesion, and morale.

In relative terms wherein more of any of the three factors i.e. friction, disruption and lethality imply more entropy, corresponding effect on entropy would be more when the cognitive component is targeted. At the national level, these would manifest as desired outcome of a Political Warfare, while at the military level it would be breakdown of Command and Control (C2) due to a deluge of conflicting information or due to lack of clear directions. The adversaries target the cognitive domain by preventing linkages between cognitive and physical domains by continuously attacking information networks while protecting own.

As one author highlights, Situation Awareness is the glue that binds a known past with unknown future (Herman, 1999). In this context, since input data gets transformed from Data to Information, to Knowledge and then Wisdom (DIKW), therefore, targeting information space and thereafter human cognition will be a force multiplier towards entropy creation.

Figure 5: DIKW Pyramid and Situational Awareness

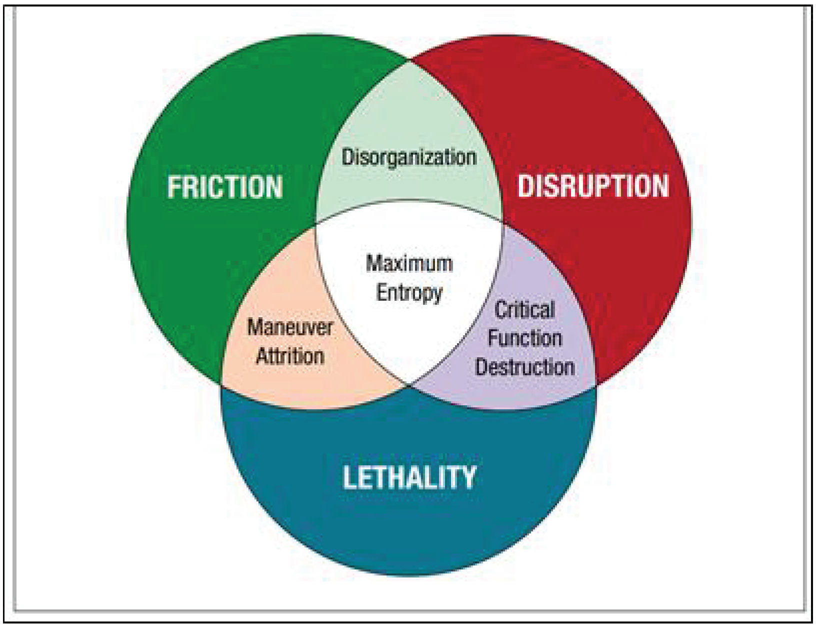


Source: https://www.usiofindia.org/publication-journal/trends-in-new-generation-warfare-lessons-for-india.html

China and Entropy Warfare

> **Winning the conflicts of tomorrow, both large and small—or better yet, preventing, limiting, or mitigating them—will increasingly depend on how the new intangibles, including everything from satellite-based tactical intelligence to strategic perception management at the geopolitical levels, are exploited.**
>
> — (Arquilla & Ronfeldt, 1997)

Figure 6: Components of Entropy Warfare



Source: https://apps.dtic.mil/sti/tr/pdf/ADA426666.pdf

The Chinese Central Military Commission (CMC) officially introduced *san zhong zhanfa* or the Three Warfares (comprising of psychological, media and legal warfare), in its Political Work Guidelines of the People's Liberation Army published in 2003 (Stokes, 2013). The conceptual framework organises different information-related non-kinetic operations for influencing adversary behaviour into three categories i.e. Strategic Psychological Operations, Overt and Covert Media Manipulations, and Exploitation of National and International Legal Systems (Livermore, 2018). The objective of the Three Warfares is to 'control public opinion, organise psychological offence and defence, engage in legal struggle, and fight for popular will and public opinion'. This requires efforts to unify military and civilian thinking, divide the enemy into factions, weaken the enemy's combat power, and organise legal offensives (Burke, Gunness et. Al, 2020). The Three Warfares combined with Political Warfare and Propaganda provide useful leverage options to secure Chinese national interests while also exercising escalation control in Entropy Warfare and preventing destructive conventional conflicts.

The 2020 Chinese Science of Military Strategy states that "a new type of People's War system built on the basis of strong comprehensive national power to meet the requirements of informatized local warfare will surely become a new strategic cornerstone for winning future wars" (China Aerospace Studies Institute, 2020). Political warfare is clearly the tactic that will support an "entropic warfare" win —paralyse a target country's ability to respond or defend itself and hence allow Beijing to "win without fighting". US diplomat George Kennan described Political Warfare as "the employment of all the means at a nation's command, short of war, to achieve its national objectives" (Jones, Harding et. al, 2023). Certain actions carried out as part of this include intelligence operations, cyber operations, information and disinformation operations, united front work, irregular military actions (including those by militia and private security companies) and economic coercion.

In addressing the 20th National Congress of the Chinese Communist Party (CCP) on October 16, 2022, China's President Xi Jinping stated that quickly elevating the People's Liberation Army (PLA) to a world-class army was a strategic requirement and that China would adhere to the integrated development of the PLA through the concept of 'three-izations' — mechanization, informatization, and intelligentization (Takagi, 2022). Calling it the Chinese Dream, President Xi aims to transform the PLA to a world class force that can fight and win global wars by 2049.

PLA has recognized 'systems confrontation' to be the mode of warfare in the 21st century wherein militarised conflict is perceived to be a contest between opposing operational systems. System destruction warfare constitutes the PLA's theory of victory (Engstorm, 2023). System destruction warfare emphasizes striking selectively but precisely and decisively against critical aspects of the enemy's capabilities, in particular "centres of gravity in enemy systems, including leadership institutions, command and control centres, and information hubs". System of systems is seen as the foundation that will achieve integrated joint operations and win informationised local wars. As per 2022 China Military Power Report, **Multi-Domain Precision Warfare** i.e. a blend of networking, AI, precision weaponry and joint operations, will support the "system-of-systems" approach by identifying vulnerabilities in an adversary's operational system to launch kinetic and/ or non-kinetic precision strikes for system collapse.

Entropy Warfare could manifest at multiple levels to break the will of the populace. While social media networks will be targeted to influence minds of the population, focused targeting of communication networks will deny information flow to higher commanders. Other measures like trade embargo, selective infringement of airspace and maritime boundaries will happen, combined with demonstrated capability of targeting in various domains, as part of coercion. Against Taiwan, China has used information warfare, cyberattacks, economic coercion, and military demonstrations while using diplomatic manoeuvres to prevent Taiwan entering into other Free Trade Agreements and diplomatic alliances (Carugati, 2022). Targeting of key political and military leaders, though unproven, has also been resorted to. All these steps are being undertaken with the underlying aim of cognitively making the populace believe that reunification of Taiwan with China is the only option (Parton, 2021).

Actions by China in the Pacific Island countries, especially in Solomon Islands wherein the Islands switched diplomatic recognition from Taiwan to China and later signed a security arrangement with a seemingly unpopular Prime Minister Sogavare, have been cited as part of a multi - domain approach (Paskal, 2022). Chinese actions in Sri Lanka, Maldives, and Nepal, can be seen as part of a well-orchestrated plan integrating all the domains, to counter the growing influence of India in the region (Ramiah, 2023). Long term lease of Hambantota Port and the controversial visit of Yuan Wang 5, a next generation space tracking vessel, to the same port in August 2022 amidst oblique protests from India are visible manifestations of such a well-planned strategy.

A Rand study acknowledged that Russia, China, Iran, and North Korea identifies superiority in the information domain as critical to success in a multi-domain conflict, while also estimating that Russian and Chinese strategies seek to exploit the vulnerabilities in interdependent systems of their opponents to minimise their advantage in every domain (Black, Lynch et. al., 2022). In the 'intelligentised warfare' phase of the PLA, machines with high computing skills will be introduced to make command and strategic decisions. Technologies, such as AI and machine learning, and game theory will be utilized to accurately analyze and determine the opponent's intentions, and this information will be provided to commanders (Ranjan, 2022).

A detailed analysis of Chinese operational thoughts indicates three concepts that will guide the PLA towards becoming a "fully modernized military by 2035 and world class military by 2050":

- ***War control*** (and therefore campaign success) depends on information dominance. Kinetic and non-kinetic attacks on leadership, C2 nodes, sensors, and information hubs to disable enemy's information networks while guarding own for accurate information and rapid decision making at a pace faster than the enemy.
- ***Shrinking combat space***, but an expanded war space. In Chinese military writings, combat space is the geographic area where actual physical conflict occurs while war space encompasses both the physical and nonphysical domains of the war, including the political, economic, diplomatic, and informational spheres. The cognitive space will be engaged with Three Warfares, to control public opinion, organise psychological offence and defence, engage in legal struggle, and fight for popular will and public opinion. This requires efforts to unify military and civilian thinking, divide the enemy into factions, weaken the enemy's combat power, and organise legal offensives.
- ***Target Centric Warfare (TCW)*** defeats the adversary's operational system (Burke, Gunness et.al., 2020). Critical points in enemy's operational system will be attacked to achieve decisive effects with minimal collateral damage, which implies identifying critical vulnerabilities and then attacking them with speed, precision, and intensity. Big Data and Artificial Intelligence will be exploited to collect and collate information and the side with algorithmic advantage will dominate war with human-computer hybrid operations and neural network decision making, "cloud brain" and "virtual warehousing" technologies and capabilities (Burke, Gunness et.al., 2020).

PLA Cyberspace Force (CSF) and Information Support Force (ISF)

> **Without space control, information control will be impossible, air control, sea control, and land control will also be like dominoes, and fall quickly one after another.**
>
> —(Science of Military Strategy 2020)

With Information Dominance as the key focus, it is a natural guesstimate that the main executing agencies for Entropy Warfare would be the PLA Cyberspace Force (CSF) and Information Support Force (ISF), part of the four **Arms** recently announced by Central Military

Commission (CMC) on 29 April 2024 (Dahm, 2024), while dissolving the Strategic Support Force (SSF). Post announcement of ISF creation and SSF dissolution, the erstwhile departments of SSF, vis. the Space Systems Department (SSD) and the Network Systems Department (NSD) were redesignated as Aerospace Force (ASF) and Cyberspace Force (CSF) and placed under direct command of the CMC.

For creation of SSF, China had pursued what can be called a "bricks, not clay" approach to reorganization. Instead of building whole organizations from scratch, the PLA made structural changes by renaming, resubordinating, or moving whole existing organizations and their component parts and then redefining their command relationships within the PLA. The SSF integrated all information warfare elements with its moot mission being provision of strategic information support and executing strategic information operations. The SSF was responsible for all aspects of information in warfare including intelligence, technical reconnaissance, cyber-attack/defence, electronic warfare, and aspects of information technology and management (Burke, Gunness et. Al, 2020). According to Chinese President, the SSF was a "new type operational force to maintain national security" and "an important growth point" for the PLA's "new quality operational capability" (Pollpeter, Michael, Chase & Heginbotham, 2017). The whole process has now been further streamlined in April 2024, with the announcement of four Services (Army, Navy, Air Force and Rocket Force) and four Arms (ASF, CSF, ISF and the Joint Logistic Support Force). ASF can be identified as responsible for space operations and strategic intelligence, while CSF and ISF are responsible for information operations integrating the three aspects of strategic information warfare i.e. Cyber Warfare, Psychological Operations and EW. CSF would have a relatively major role to play in Entropy Warfare even as ASF would assist with enhanced situational awareness.

- ***ISF.*** In 2015, the CMC Joint Staff Department controlled what was known as the Information Assurance Base (IAB) also called the Information Support Base (ISB). As part of the below-the-neck reforms, the IAB, designated the 61001 Unit, was moved to the SSF and renamed the "Information Communication Base (ICB). The ICB commanded several geographically distributed information communication brigades assigned to support PLA theatre commands (Dahm, 2024). ISF, announced in April 2024, has primarily integrated all the elements of Information Communication Base (ICB).
- ***ASF.*** Formally known as SSD, this Arm of the PLA brought under its command military space related forces and capabilities nationwide in late 2015. These

forces and capabilities were traditionally run by the now defunct PLA General Armament Department (GAD). They include space launch capabilities such as the Jiuquan Satellite Launch Centre (Base 20), Taiyuan Satellite Launch Centre (Base 25), Xichang Satellite Launch Centre (Base 27) and the relatively new Wenchang Space Launch Centre in Hainan. They also include space telemetry, tracking and control capabilities such as the Beijing Aerospace Flight Control Centre, Xian Satellite Control Centre (Base 26), and China Satellite Maritime Tracking and Control Department (Base 23) which maintains a fleet of Yuan Wang space tracking ships.

- ***CSF.*** Formally known as NSD, this Arm of the PLA (organized around the erstwhile 3PLA, premier cyber espionage organization {Costello, 2016}) runs the PLA's national-level signal intelligence (SIGINT), cyber operations, electronic warfare (EW) and psychological warfare forces and capabilities. As the Chinese 2020 Science of Military Strategy says, "whoever holds the dominance in cyberspace will win the initiative in the war; whoever loses this centre will fall into strategic passivity". PLA Base 311, the psychological warfare force, which had attempted to influence public opinion in Taiwan by exploiting local social media has also reportedly moved under the CSF. Various other agencies like the EW forces (GSD Electronic Countermeasures Department), Louyang Foreign Language Institute (PLA Information Engineering University), Unit 61398 (allegedly responsible for computer hacking against the USA, as part of Technical Reconnaissance Bureau), and the GSD Technical Reconnaissance Department with its 12 TRBs were also reportedly transferred (Nan & Clarke, 2021).

The PLA places a strong emphasis on dismantling the adversary's system of systems, with decapitation and paralysis rather than outright destruction being the ultimate objective. This approach is tied to the long-standing Chinese focus on winning without fighting - an older Maoist-era phrase that translates today to shaping an adversary's decision making through actions below the threshold of outright war, accomplishing strategic objectives without escalating to open conflict (Costello & McReynolds, 2018). Though some argue that Chinese Warfare literature is mirroring Western concepts, what clearly emerges is the planned use of CSF and ISF as pre-emptive weapons across multiple domains to reduce strategic imbalance. These actions, as a part of the escalatory ladder, also stays within the Grey Zone thereby not leading to largescale conflict. If such an approach of ‘targeting the superior with inferior’ is adopted, the actions will have plausible deniability and assured entropic win (Mulvenon).

There have been earlier reports of RedEcho (China linked) hackers targeting the Indian national power grid, as a show of force (Gill, 2021) as well as Russian and Chinese psychological influence campaigns targeting the US Presidential campaigns (Barnes, 2023). Though not Chinese, similar psychological targeting was earlier resorted to by Cambridge Analytica in the 2016 US Presidential Campaign and later in the ‘Leave EU campaign’, using harvested data from 87 million Facebook profiles. Since largescale datasets of the adversary are needed to completely operationalise planned actions of Entropy warfare, there have been numerous reports of data leaks and hacks from various servers all over the World. There have also been reports of Chinese hackers taking intellectual property like for example designs from sites of various US and European firms, while there were unconfirmed reports of similar attacks against India on Aadhaar biometric information, post Galwan clashes (NDTV, 2021).

Whole of Nation Approach with Military Civil Fusion

While ISF and CSF are handling operational and tactical intelligence in conjunction with Theatre Commands and other operational agencies, agencies like the CMC - PWD (erstwhile Political Works Department and now under the Central Military Commission) handles human and open-source intelligence and the JSD IB (Intelligence Bureau under the Joint Staff Department) ensures ideological loyalty and propagation of Party ideals among Party cadres. This is indicative of a decoupling of political aspects of Three Warfares from the operational aspects (Panwar, 2020). As PLA Arms like CSF and ISF contribute to the ‘Disruption’ component of Entropy Warfare, PLARF and other Services add to the ‘Lethality’ part. As China transforms its warfighting norms towards Algorithmic Warfare with greater emphasis on ‘Human in the loop’ transitioning to ‘on the loop’ and later ‘out of the loop’, Multi Domain Integrated Joint Operations and Precision Warfare will be augmented with deeper influence actions by agencies like the United Front Work Department (UFWD) across a wider spectrum. Various reports are available of actions by agencies like the UFWD, Confucius Institutes, Chinese Students and Scholars Associations (CSSAs) etc. as part of a United Front strategy to ‘control the narrative’ and destroy opposition from within through influence operations (Bowe, 2018).

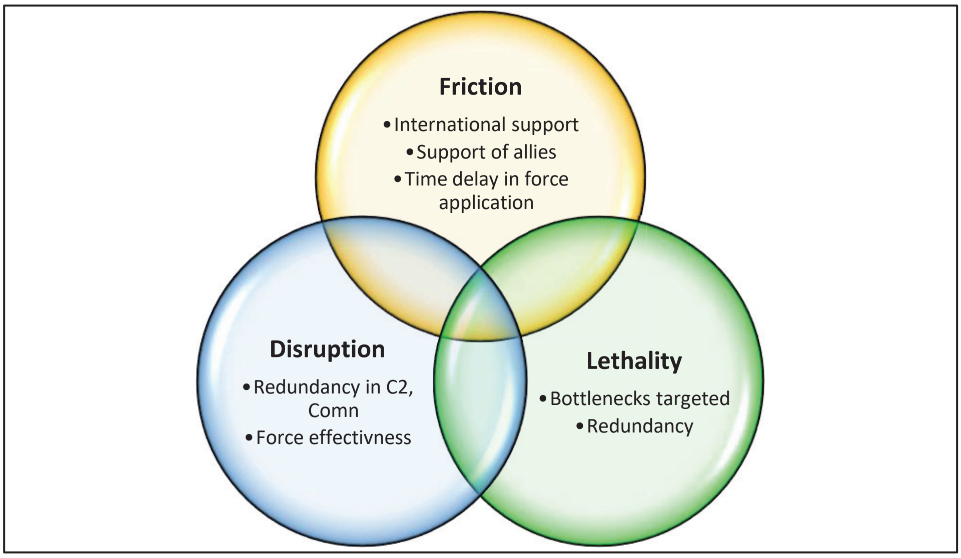
How the newly formed CSF and ISF would coordinate cyber defence and protection with the Ministry of Public Security (MPS) and Cyberspace Administration of China, both of which are charged with maintaining the security and defence of China’s critical information infrastructure is to be seen in the future. Of China's myriad agencies with cyber portfolios, the Ministry of State Security (MSS) and PLA are the two primarily responsible for cyber operations including both espionage and offensive action. The Mandiant Report of 2014, the Xi-Obama Agreement on cyber enabled intellectual property theft in 2015, and the creation of the SSF each in various ways forced a realignment of responsibilities between the two agencies, with the MSS focusing on foreign intelligence, political dissent and economic espionage, and the PLA redoubling its focus on military intelligence and warfighting (Costello and McReynolds, 2018).

By restructuring the PLA, China has closely integrated aspects of integrated Network Electronic Warfare (INEW) and the Three Warfares. While the ownership of some aspects like EW, cyber and cyber defence is shared with Networks Electronic Bureau (NEB) and Information and Communication Bureau (ICB) of JSD, there is a more visible integration of various levels and domains, with centralised control for an Entropic Warfare victory. The capabilities of PLA to execute IW and integrate aspects of civil-military fusion to fast-track technology and other systems to achieve complete dominance and thereby induce entropy in adversaries has been challenged by many strategists (Nelson and Epstein, 2022). Lack of transparency, excessive secrecy, and classification of these reforms as 'above the neck' and 'below the neck', can be cited as reasons for lack of complete understanding of new departments and developments. A centrally controlled full spectrum, multi domain, whole of nation, civil-military fusion supported approach will ensure that the identified target develops entropy and finally collapses. This integrated approach would also co-opt agencies like the Militia, PLA's own Propaganda Department, and diaspora to support central narratives while simultaneously destroying/ mitigating opposing ones.

Manifestation of Entropy Warfare

The actions at national level as part of Entropy Warfare were seen in previous sections. A combination of political and Three Warfares along with other instruments of national power would be used to degrade target nation's ability to resist. While satellites like Yaogan 41 would provide real-time/ near real time situational awareness (Clarke, 2023), various state agencies including Chinese diaspora would contribute towards strategic intelligence. Toolkits for winning the 'battle of narratives' and ensuring support for '*jus ad bellum*' would be rolled out, even as target populace will find conflicting narratives on state owned media thereby eroding their trust in state machinery including Government.

Figure 7: Three Components of Entropy Warfare



Source: Prepared by Author

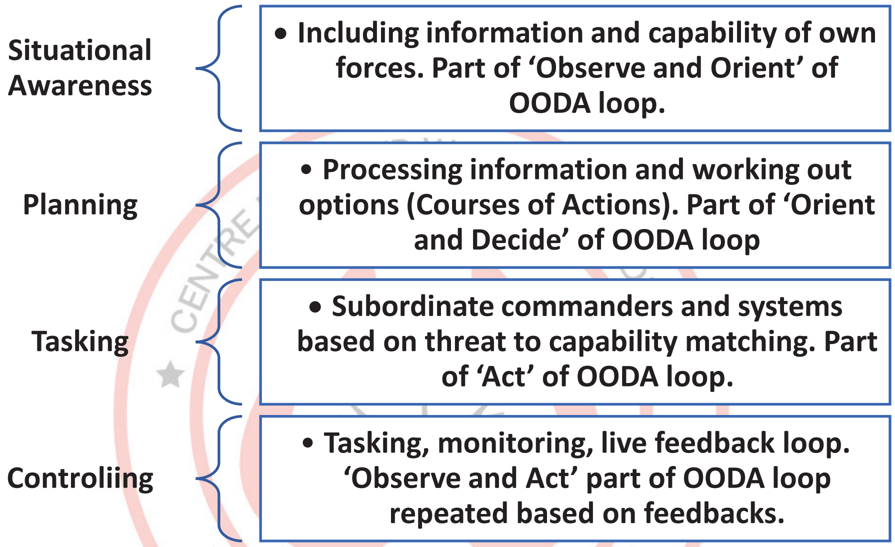
At the military level, communication bottlenecks would be targeted and own OODA loops disrupted. While PLA Rocket Force and air components would strike critical targets as part of its Air Missile Campaign, asymmetric forces would address key areas as a prelude to main force application. Command and control arrangements will be degraded and communication between kinetic components would be interdicted. Malicious software would make data and AI based systems unavailable and add on to the friction and disruption components of entropy. Radars and communication nodes would be destroyed or disabled as part of EW while all efforts will be made to influence the cognitive component. Having ensured combat isolation of specific target areas, certain key elements would be sought to paralyse the enemy's operational system: -

- Strikes that degrade or disrupt the 'flow of information' within the adversary's operational system.
- Degrading or disrupting that 'operational system's essential factors', which include, but are not limited to, its command and control (C2), reconnaissance intelligence, and firepower capabilities.
- Degrading or disrupting the 'operational architecture' of the adversary's operational system. These would include physical nodes of the previously mentioned capabilities, for example, the entire C2 network, reconnaissance intelligence network, or firepower network.

- Disrupting the ‘time sequence and/ or tempo’ of the enemy’s operational architecture. This is to degrade and ultimately undermine the operational system’s own “reconnaissance-control-attack-evaluation” process.

The components of Command and Control (C2, as part of C4I2SR - Command, Control, Communications, Computers, Intelligence, Information, Surveillance, Reconnaissance) which can be targeted to create entropy are (Jacques):

Figure 8: Components of C2 extracted from 'An Information Warfare Perspective on Entropy Warfare'



Situational Awareness

- Including information and capability of own forces. Part of ‘Observe and Orient’ of OODA loop.

Planning

- Processing information and working out options (Courses of Actions). Part of ‘Orient and Decide’ of OODA loop

Tasking

- Subordinate commanders and systems based on threat to capability matching. Part of ‘Act’ of OODA loop.

Controliing

- Tasking, monitoring, live feedback loop. ‘Observe and Act’ part of OODA loop repeated based on feedbacks.

Source: https://www.academia.edu/17407598/ENTROPY_WARFARE

Jammed GPS navigation and communication systems will affect movement of forces including reserves and aerial platforms and increase requirement of redundant networks. Targeting software based on datasets and cloud/ edge data will become untrustworthy once the seeking system of a missile or the fire direction computer itself offers confusing inputs. Battle drills and sub unit level leadership and tactics will be tested and optimal combat efficiency degraded as the entropy generating forces would aim to isolate the battlefield and separate the C2 elements. As drones and robots replace some or many of the physical combat components, the resilience of humans in or out of the loop of human machine teaming will be tested.

Countering Entropy Warfare

It is evident that a whole of nation approach is needed to avoid the manifestation of Entropy Warfare at any level, primarily because the adversary is using multiple domains and all pillars of national power to make it effective. While strategic alliances supplemented with economic backing is needed to prevent spread of entropy through ideological leanings and debt traps in susceptible nations, powerful alliances can deter attempts to initiate Entropy Warfare in fragile countries with no major backing.

An analysis of the ongoing Russia - Ukraine conflict also reveals varying grades of Entropy Warfare, using various pillars of national power, social media, and AI enabled systems including drones and loitering ammunition (Sharma, 2022). Russia used AI to conduct cyberattacks and create deep-fake videos. Meanwhile, Ukraine used facial recognition technology to identify Russian agents and soldiers, as well as for analyzing intelligence and planning strategies (Takagi, 2022). Both sides have used a variety of drones to disrupt C2, target key installations as well as obtain intelligence for targeting like Russian Orlan 10, Ukrainian {Turkish) Bayraktar TB10, etc. (BBC, 2023). In April 2022, a Bayraktar drone was used in the attack which sank the Russian warship 'Moskva' in the Black Sea. Analysis of social media and AI in controlling narratives, gives some deep insights into information and disinformation, and makes one question the veracity of any news article (Perez and Nair, 2022).

Winning the '**Battle of Narratives**' become an important part of countering Entropy Warfare. In the Israel – Hamas conflict, Jus ad bellum for Israel to initiate large scale actions against Hamas was the 7th October targeting of 1200 Israelis, but as the war has progressed, social media narratives of increased civil casualties and strikes against hospitals, have slowly turned international and public opinion away from the initial carnage. Increasing number of social media followers for young Tik Tok and Instagram citizen reporters from Gaza is directly proportional to the increasing number of Palestinian supporters within the US Senate, despite attempts by Israel to '***hasbara'***, or 'to explain' by permitting visits to 07 October attack sites and even the Al Shifa hospital site to expose Hamas atrocities (Cortelessa and Bergengruen,2023).

In Entropy Warfare terms, Hamas with its tunnelled networks, financial support, and readily available human shields can counter the disruption and lethality capabilities of Israel, while simultaneously increasing operational friction for the Israeli forces. To counter these parallel attacks through Telegram, X (erstwhile Twitter) and other social media platforms, Israel will need a larger war effort to discredit disinformation. AI trained tools are needed to scan for disinformation campaigns and malicious content as it is humanely impossible to scan such large quantum of data/ posts generated by bots and software. Use of AI algorithmic systems like Gospel has been projected by Israel as steps taken to reduce civilian deaths and reduce human error, while detractors cite AI biases and legal implications of such targeting (Brumfiel, 2023).

One study even proposes having a 'cognitive warfare monitoring and alertness platform' to increase awareness of target populace and improve resilience against such attacks. Incidentally, there is another PLASSF (Platform to Layered Application Service to Support Cyber Security Framework) which is a software platform developed by the US Defense Advanced Research Projects Agency (DARPA) to address the challenges of entropy warfare. It provides a layered approach to cyber security that includes hardware and software protections at every level of the system that is from the hardware to the application layer. The PLASSF platform is designed to detect and respond to attacks, by monitoring the system for unusual behaviour and applying countermeasures in real-time. It uses machine learning algorithms to identify patterns in data and detect anomalies that may indicate a cyberattack. USA is setting up Joint All-Domain Command & Control (JADC2) which will replace the current domain and control systems with a single system that connects the existing sensors and shooters and distribute the available data to all domains (sea, air, land, cyber, and space) and forces that are part of the US military. There have been reports of USA developing a system called "**Entropy**" for psychological warfare operatives to effectively monitor media and feed actionable inputs (Pomerleau, 2020). For offensive actions (lethality and disruption), the focus is on developing Swarms of Swarms (Drones) which is also called Autonomous Multi-Domain Adaptive Swarms-of-Swarms (AMASS) [DARPA project]. Most details are classified, but as per some inputs, it will enable multiple swarms of small aerial, ground, and underwater drones to work together to knock out enemy defences. China has already demonstrated this technological capability in 2020 and 2021, including capability to release from different platforms.

Lessons for India

In India's immediate neighbourhood, as well as on unresolved border issues, there have been instances of muscle flexing, including a test of capability of the 'battle of narratives. Visit of the Indian Vice President to Arunachal Pradesh in October 2021, was followed up with a series of posts on social media platforms like Weibo reiterating Chinese claims on the region. The visit of Prime Minister Narendra Modi to Arunachal Pradesh on 09 March 2024 was similarly followed up with diplomatic protests. Chinese engagements as part of Belt and Road Initiative, String of Pearls, etc. have been actively countered with own diplomatic overtures like ‘Look East Policy’, Sagarmala, etc. even as debt traps and linked long lease arrangements see a swinging of influence dimensions in these neighbouring nations.

Certain takeaways for India and the Armed Forces from these deliberations of Entropy Warfare and role of SSF are enumerated.

- **Strategic Alliances.** Alliances and partnerships like QUAD and AUKUS are needed for strategic as well as for technology transfers. They also aid in preventing encirclement of the immediate neighbourhood by inimical agencies. In September 2018, India and the United States signed the Communications Compatibility and Security Agreement (COMCASA) to share high-end encrypted communication and satellite data and provide a legal framework for defence technology transfer (Khan, 2023).
- **Having Unity.** To stay united especially against external threats (Pradhan, 2023). Hamas chose to strike Israel at a time when public discontent was high with even the PM facing protests. In a large democracy like India, it’s a difficult task to ascertain and establish funding and motivation of each political movement, and to identify whether some of the actions are fuelled by Political warfare/ entropy inducing actions of an adversary.
- **Force Modernisation.** Need to fast track own modernisation process with right mix of economy and civil-military fusion. Intelligent loitering ammunition and drone swarms could be some additions even as robots and technological aids like exoskeletons and bionic implants can be introduced with adequate safeguards.
- **Counter-agency for ISF and CSF.** There is a necessity for establishing a formal structure to counter the enemy’s Entropy warfare while protecting own vulnerabilities. It also requires to integrate various domains of space, cyber, EW and IW.
- **Strengthening Information Systems and Infrastructure.** Capabilities of AI can be exploited to dynamically identify and mitigate own vulnerabilities while exploiting the adversary’s weaknesses. Strengthening the critical care infrastructure to counter increasing number of attacks (Ghosh, 2022) by state and non-state actors including ransomware attacks will reduce efficacy of entropic strikes.

- **Developing Data Awareness.** Machine learning algorithms need larger data sets for both training as well as testing. If the aim is to develop systems for faster decision making, the algorithm will need large scale inputs to formulate and finalise the influencing factors in such decisions. Capturing the right data, its storage and sharing across platforms with inbuilt AI assisted safeguards, combined with big data analytics, is the need of the hour.
- **Trust in Systems.** Adversary could target the systems and thereby create a trust deficit which can become detrimental to organisational cohesion and efficiency. Need to train and operate more with systems and machines to develop mutual trust.
- Regulate **digital and data sovereignty** and regulate social media outlets and restrict online speech, with focus on targeted disinformation and paid media. There is a need to develop **societal resilience to manipulation**, to promote **responsible online behaviour**, and **inoculate against disinformation tactics** (Singh, 2023). Having a team of good Samaritans to highlight nation building efforts will be a positive step (Barthwal, 2022).
- Ensuring that **data is without biases** and systems follow established ethical, moral, and legal guidelines.
- Need for a safe **electromagnetic and data spectrum** with adequate safety protocols for interconnected devices/ systems to operate.
- Maintain an **upper edge in 'cognitive warfare'** by having adequate monitoring systems and pro-active information dissemination policy.
- **Joint Professional Military Education (PME)** incorporating the tenets of technology and skills for countering disruption that can be caused by the adversary. This should also focus at developing jointness.
- **Distributed Simulation Systems.** Increased training on AR/ VR platforms with scenario painting by AI systems. Like Chat GPT, these AI systems can collate and present deep learning-based scenarios which will enhance the training of individual soldiers for wider scenarios in a faster timeframe with lesser cost.
- Long term **HR management** to create a cadre of professionals with social and technological skills to understand and counter enemy Entropy Warfare.

- **Junior Leader training** and increased focus on small team operations with redundancy to work 'isolated' in a technology constrained environment. For example, navigation using maps and compass.
- **Indigenous technology and social media platforms.** To counter external control and disinformation campaigns including disruption attempts.
- **Civil- Military Fusion and Dual use technology.** Incubation workshops and increased projects as part of *Atmanirbharta* to harness domestic talent and be self-reliant.
- **Importance of strategic communication (Pandala, 2018).** To have a better coordination of strategic narratives and to avoid disinformation at various levels. Important to develop a cadre of experts under the ADG Strategic Communications and empower DG IW to combat misinformation and false propaganda (The Economic Times, 2019).
- **Improving education standards, reducing unemployment, and tracking external funding to various groups.** For Entropy warfare to be successful, the target population must be vulnerable and susceptible. This can be mitigated through holistic development of communities (CLAWS Seminar, 2017).
- **Dispersed Concentration.** Will help in preventing disruption and reducing friction in force application. Robust communication and perfected battle drills will improve combat effectiveness.

Conclusion

> **In the era of intangible weaponry, some of the biggest guns of all are deployed by the media.**
>
> —(Arquilla & Ronfeldt, 1997)

Contestation of minds, which is the final level of war and warfare will continue as ever before. New terminologies will be coined and old ones redefined but War, in its truest sense will continue to be violent, with accompaniments of friction, fear, uncertainty, and all elements of so called 'fog of war'. As technological advancements are made, traditional battlespaces will expand with increased reach even into our homes. As Hoffman says, autonomy will change the nature of war in several ways. While it is still arguable whether the nature or character of war would be affected, the role of political direction will be weakened by forcing response delegation to lower echelons for faster forms of attack (Hoffman, 2017). It will be easier for foreign governments to manipulate their adversary's populations while permeating influence of social media and technology will make it difficult to isolate own population from the expanding war space.

While deep learning forms of AI will augment the intuition and judgment of experienced commanders and reduce OODA loops, increased human-machine teaming and data enmeshed C2 systems will increase vulnerabilities and enhance probability for an entropic collapse. A clear understanding of the layered domains of warfare including kinetic and non-kinetic forms will enable military leaders to stay ahead of the knowledge loop and have an OODA advantage with less entropy.

Works Cited

Narang, A (2019). *China's Strategic Deterrence*. Pentagon Press. P. 19.

US Department of Defense. (2019, November 5). Remarks by Secretary Esper at National Security Commission on Artificial Intelligence Public Conference. https://www.defense.gov/News/Transcripts/Transcript/Article/2011960/remarks-by-secretary-esper-at-national-security-commission-on-artificial-intell/.

Panwar, R.S. (2021, October 19). Grey Zone Operations in the Infospace Dimension: Imperatives For India. *Future Wars*. https://futurewars.rspanwar.net/grey-zone-operations-in-the-infospace-dimension-imperatives-for-india/.

Beauchamp-Mustafaga, N. (2019, September 6). Cognitive Domain Operations : The PLA's New Holistic Concept for Influence Operations, *The Jamestown Foundation China Brief* ,1(16). https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/.

Hung, T.C. and Hung, T.W. (2022, July 19). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies,* 7(4). https://doi.org/10.1093/jogss/ogac016.

Michael C. Horowitz and Lauren Kahn, (2021, November 4). DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military. *Council on Foreign Relations*. https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape.

Libicki, Martin C. (1995, August). '*What is Information Warfare?'* Washington, DC: Institute for National Strategic Studies, *National Defence University*. https://typeset.io/papers/what-is-information-warfare-2fded8mhcz.

Crilly, M. and Mears, A. (2022, January 26). Multi Dimensional and Domain Operations. *Wavell Room*. https://wavellroom.com/2022/01/26/mddo/.

Ahluwalia, V.K. (2020, June). Manoeuvre Warfare in the Information Age, CLAWS, No. 231. https://www.claws.in/publication/manoeuvre-warfare-in-the-information-age/.

Panwar, R.S. (2021, October 19). Grey Zone Operations in the Infospace Dimension : Imperatives for India, *Future Wars*. https://futurewars.rspanwar.net/grey-zone-operations-in-the-infospace-dimension-imperatives-for-india/

Herman, Mark, (1999). Modelling the Revolution in Military Affairs. *Joint Force Quarterly*. https://apps.dtic.mil/sti/tr/pdf/ADA426666.pdf.

Misra, P., Prashant Misra (2022, March). Trends in New Generation Warfare: Lessons for India. *Journal of the United Service Institution of India, CLII(627).* https://www.usiofindia.org/publication-journal/trends-in-new-generation-warfare-lessons-for-india.html.

Arquilla, J. and Ronfeldt, D. (eds.) (1997). In Athena's Camp: Preparing for Conflict in the Information Age. *RAND Corporation*. https://www.rand.org/pubs/monograph_reports/MR880.html.

Stokes, M. and Hsiao, R. (2013, October 14). The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics. *Chinese People's Liberation Army Political Warfare.* https://project2049.net/wp-content/uploads/2018/04/P2049_Stokes_Hsiao_PLA_General_Political_Department_Liaison_101413.pdf.

Livermore, D. (2018). China's Three Warfares : In Theory and Practice. *George Towm Security Studies Review*. https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

Burke, E.J., Gunness, K., Cortez, A., Cooper III, and Cozad, M. (2020). People's Liberation Army Operational Concepts. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA394-1.html

China Aerospace Studies Institute (2022, January). In Their Own Words : Science of Military Strategy 2020. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

Seth G. J., Harding, E., Doxsee, C., Harrington, J. and McCabe, R. (2023, August 02). Competing Without Fighting. *CSIS*. https://www.csis.org/analysis/chinas-strategy-political-warfare.

Takagi, K. (2022, November 16). Xi Jinping's Vision for Artificial Intelligence in the PLA. *The Diplomat*. https://thediplomat.com/2022/11/xi-jinpings-vision-for-artificial-intelligence-in-the-pla/.

Engstorm, J. (2018, February 1). System Confrontation and System Destruction Warfare. *Rand Corporation*. https://www.rand.org/pubs/research_reports/RR1708.html.

Carugati, R. (2022). Is War over Taiwan Coming? *Network for Strategic Analysis*. https://ras-nsa.ca/wp-content/uploads/2022/06/Policy-Report-19-Is-War-Over-Taiwan-Coming.pdf.

Charles Parton, OBE (2021, May). Taiwan in the next decade – No war, but much tension. *Council on Geo Strategy*. https://www.geostrategy.org.uk/app/uploads/2021/05/Explainer-GPE01-13052021.pdf.

Cleo Paskal (2022, April). China's Agreement for Security with Solomon Islands & Implications for Security in the Pacific. *Foundation for Defense of Democracies. https://www.fdd.org/analysis/2022/04/29/chinas-agreement-with-solomon-islands/* .

Sulochana Ramiah (2023, February). China's Entropic War Operations in South Asia Seek to Undermine India: Experts. *Asian Institute of Diplomacy and International Affairs*. https://www.aidiaasia.org/research-article/china-s-entropic-war-operations-in-south-asia-seek-to-undermine-india-experts .

James Black, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paille and Fiona Quimbre (2022). Multi Domain Integration in Defence, *Rand*. https://www.rand.org/pubs/research_reports/RRA528-1.html.

Om Ranjan (2022, December). The PLA and Intelligentised Warfare. *IDSA. https://idsa.in/idsacomments/the-pla-and-intelligentised-warfare-oranjan-011222.*

Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III and Mark Cozad (2020, September 29). People's Liberation Army Operational Concepts. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA394-1.html.

Science of Military Strategy 2020. Available at 2022-01-26 2020 Science of Military Strategy.pdf (af.edu).

Dahm, M. (2024, April 26). A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force. *China Brief.*

A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force - Jamestown

Pollpeter, K., Chase, M., and Heginbotham, E. (2017). The Creation of the PLA Strategic Support Force and its implications for Chinese Military Space Operations. *Rand Corporation*. The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations (rand.org).

Costello, J. (2016, December 31). China's Cyber-Focused Military Unit Emerges from the Shadows, *The News Lens* China's Cyber-Focused Military Unit Emerges from the Shadows - The News Lens International Edition.

LI Nan & Ryan Clarke (2021, August 25). The new Strategic Support Force of Chinese Military and Implications for Regional Security. *East Asian Institute, National University of Singapore.* EAIBB-No.-1606-PLASSF-and-Regional-Security-2.pdf (nus.edu.sg)

John Costello, Joe McReynolds (2018, October). China's Strategic Support Force: A Force for a New Era. *Center for the Study of Chinese Military Affairs*. china-perspectives_13.pdf (ndu.edu).

James Mulvenon (1999). The PLA and Information Warfare. *Indianstrategicknowledgeonline.com*. [PDF] 9. THE PLA AND INFORMATION WARFARE | Semantic Scholar

Prabhjote Gill (2021, March 01). Chinese hacked into India's power grid just to show that they can. *Business Insider*. Chinese hacked into India's power grid just to show that they can (businessinsider.in).

Julian E Barnes (2023, December 18). China increased US Election influence in 2022, Intelligence Report says. *New York Times*. China Increased U.S. Election Influence in 2022, Intelligence Report Says - The New York Times (nytimes.com).

Chinese Hackers targeted Aadhaar database, NDTV, 22 September 2021. Chinese Hackers Targeted Aadhaar Database, Times Group: Report (ndtv.com) and Chinese hackers took trillions in intellectual property from about 30 multinational companies - CBS News.

Panwar, R.S. (2020, June 16). China's Special Support Force and its Implications for India. *Future Wars*. Future Wars China's Strategic Support Force and its Implications for India – Part II (rspanwar.net).

Alexander Bowe (2018, August 24). China's Overseas United Front Work. *US China Economic and Security Review Commission*. China's Overseas United Front Work - Background and Implications for US_final_0.pdf (uscc.gov).

Amy J. Nelson and Gerald L. Epstein (2022, December 23). The PLA's Strategic Support Force and AI Innovation. *Brookings.* The PLA's Strategic Support Force and AI Innovation (brookings.edu)

Stephen Clarke (2023, December 16). A top-secret Chinese spy satellite just launched on a supersized rocket. *Ars Technica,* A top-secret Chinese spy satellite just launched on a supersized rocket | Ars Technica.

Theron, Jacques (2008). An Information Warfare Perspective On Entropy Warfare. *Academia.edu*. (74) ENTROPY WARFARE | Jacques Theron - Academia.edu

Sanur Sharma (2022, March 16). Russia's AI Enabled Military Ecosystem and Its Algorithmic Warfare. *IDSA*. Russia's AI Enabled Military Ecosystem and Its Algorithmic Warfare | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in).

BBC (2023, December 29). How are 'kamikaze' drones being used by Russia and Ukraine? - BBC News.

Christian Perez and Anjana Nair (2022). Information War in Russia's War in Ukraine. *Foreign Policy.* Information Warfare in Russia's War in Ukraine – Foreign Policy

Eric Cortelessa and Vera Bergengruen (2023, December). Inside the Israel Hamas Information War. *Time*. Inside the Israel-Hamas Information War | TIME.

Geoff Brumfiel (2023, December). Israel is using an AI System to find targets in Gaza. *NPR*. Here's how Israel is using artificial intelligence to find targets in Gaza. : NPR

Mark Pomerleau (2020, September 11). *C4I4SRNET*. Pentagon's AI center to field new psychological operations tool (c4isrnet.com)

Dr Tanveer Ahmad Khan (2023, April 24). Limited Hard Balancing: Explaining India's Counter Response to Chinese Encirclement. *Journal of Indo-Pacific Affairs*. Limited Hard Balancing: Explaining India's Counter Response to Chinese Encirclement > Air University (AU) > Journal of Indo-Pacific Affairs Article Display.

SD Pradhan (2023, October). Understanding Hamas Israel Conflict : Lessons for India', *Times of India*. Understanding Hamas-Israel conflict: Lessons for India (indiatimes.com).

Soumik Ghosh (2022, September 15). Seven major attacks in the last two years. *Economic Times.* Securing India's critical infrastructure: Biggest challenges and how to overcome them, ET CIO (indiatimes.com).

Brijesh Singh (2023, October). Israel Hamas war shows the formidable power of narrative. *Nikkei Asia*. Israel-Hamas war shows the formidable power of narrative - Nikkei Asia.

Namita Barthwal (2022, February). Information Warfare and India's Level of Preparedness. *CLAWS*. Information Warfare and India's Level of Preparedness – Center For Land Warfare Studies (CLAWS).

Shruti Pandala (2018). Rethinking Strategic Communication in the age of Information Warfare', Defence Reforms : A National Imperative. *IDSA* New Delhi. Defence Reforms: A National Imperative | Manohar Parrikar Institute for Defence Studies and Analyses (idsa.in).

Shaurya Karanbir Gurung (2019, March 09). *Economic Times*. Defence ministry approves information warfare branch for Indian army - The Economic Times (indiatimes.com)

CLAWS Seminar report (2017). Perception Management and Constructing a Positive
Narrative in Jammu and Kashmir.
CLAWS.720794065_PerceptionManagementandConstructingaPositiveNarrativeinJK(2).pdf
(claws.in).

Arquilla, John and David Ronfeldt, eds.(1997). In Athena's Camp: Preparing for Conflict in the Information Age. *RAND*. https://www.rand.org/pubs/monograph_reports/MR880.html

Hoffman, F.G. (2017). Will War's Nature Change in the Seventh Military Revolution?. *Parameters* 47. "Will War's Nature Change in the Seventh Military Revolution?" by F. G. Hoffman (armywarcollege.edu).

Vinod Khandare, Vinit Goenka et. al. (2019), *Data Sovereignty: The Pursuit of Supremacy*, Om Publications.

About the Author

Brigadier G Praveen, SM was commissioned into 14 GARH RIF in December 1997 and is an alumnus of NDA, Advanced Command and Staff College, United Kingdom and CDM. A battle casualty of Op VIJAY, he later commanded his unit in J & K in HAA/ CI. His instructional and staff appointments include Assistant Adjutant, Indian Military Academy, GSO 1 Military Operations Directorate, Col GS Strike RAPID, Col Q Sub area and Directing Staff at CDM. He has served in two high intensity peacekeeping operations of MONUSCO and UNMISS, as Chief Logistic Officer and Deputy Chief of Staff Force HQ, respectively. A post graduate of Kings College London and a doctoral research fellow with Osmania University, he is a regular contributor to various professional journals. He is presently commanding a Mountain Brigade.

No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from C L A W S The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.