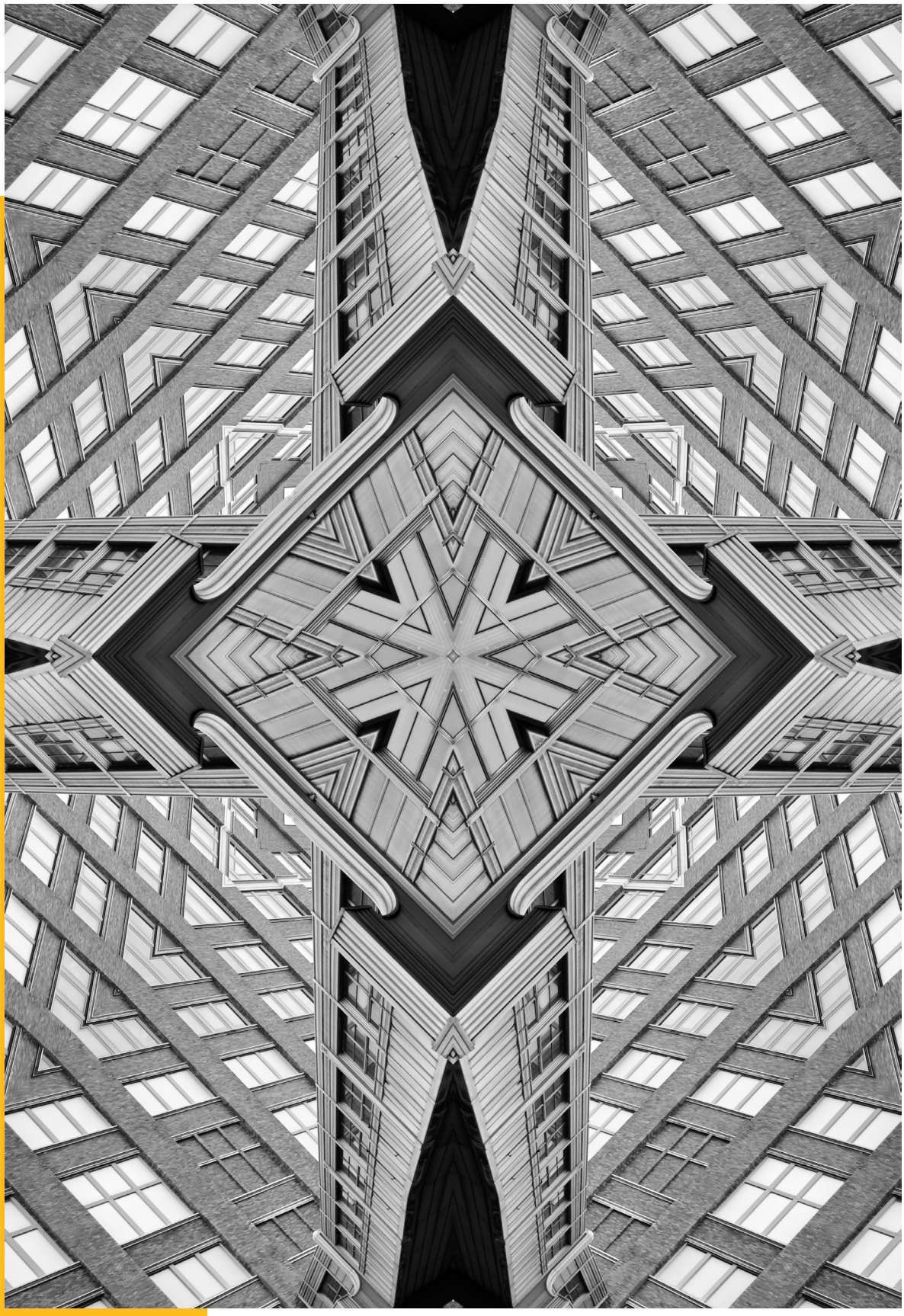
OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 409 SEPTEMBER 2023

Beyond Cyber Fires and Ukraine: PLASSF Impact on a Sino-Indian Conventional War

Kartik Bommakanti

Abstract

The ongoing Russia-Ukraine war has served as a laboratory test to assess the effectiveness of Cyber Warfare (CW) capabilities. It would be misleading, however, to extrapolate sweeping conclusions from this conflict about the relative ineffectiveness of CW. Rather, diligence should be exercised by Indian strategic and military planners in assessing the CW capabilities of the People's Liberation Army Strategic Support Force (PLASSF) and enhancing India's own preparedness. The PLASFF possesses substantial CW capabilities geared for enabling conventional military operations and missions. It is also highly capable of fusing the employment of CW, Electronic Warfare (EW), space capabilities and frontier technologies such as Artificial Intelligence (AI) for the effective conduct of conventional military missions against India.

Attribution: Kartik Bommakanti, "Beyond Cyber Fires and Ukraine: PLASSF Impact on a Sino-Indian Conventional War," *ORF Occasional Paper No. 409*, September 2023, Observer Research Foundation.

Introduction

In a Sino-Indian boundary war, the combined application of cyber warfare (CW) and electronic warfare (EW) is likely to be more relevant than CW alone, owing to the ongoing boundary stand-off between India and China as well as the impact of cyber operations on kinetic operations in a conventional war between the two countries. The Russia-Ukraine war has generated debate about the effectiveness of CW and EW as complements to conventional and kinetic military operations.[1] This paper examines the role of CW and EW as complementary elements. It argues that space-borne and counterspace capabilities could supplement the combined impact of CW and EW, both of which are likely to be used by China in a military confrontation with India.[2]

China's military was among the first to grasp the possibilities of the complementary use of CW and EW, through the Integrated Network Electronic Warfare (INEW),[3] which could be used independently as well as in kinetic battles. Integration is fundamental to CW as well as more generally to INEW. The People's Liberation Army Strategic Support Force (PLASSF), which is responsible for launching attacks against enemy networks in the battlefield, combines CW, EW, and space warfare (SW). PLASSF reports directly to the Central Military Commission (CMC) and would play a key role in aiding and supporting the People's Liberation Army (Army) (PLAA) and the People's Liberation Army Air Force (PLAAF) under the Western Theater Command (WTC) in a war with the Indian Army (IA) and the Indian Air Force (IAF).

While CW has been criticised[4] for its failures in the Russia-Ukraine war, India would be ill-advised to underinvest in CW capabilities. An American expert on Indian defence strategy has noted that since EW has been more effective than CW in the Russia-Ukraine war, India should invest more in EW;[5] this argument, however, fails to take into account the duration of the conflict. It also masks the extent to which Western assistance undermined the effectiveness of Russia's CW against Ukraine's networks as well as the inadequate concentration of Russia's CW capabilities in its initial military offensive.[6] It is thus imperative that India's strategic and military planners do not extrapolate from CW's supposed 'ineffectiveness' compared to EW in Russia's military campaign. It is not a binary choice for India's military leadership. Both CW and EW will be significant, irrespective of the former's

Introduction

relative ineffectiveness in the Russia-Ukraine war. Cyber sceptics analysing the Russia-Ukraine war have viewed CW in isolation, without considering Russia's EW and counterspace capabilities.[7] However, this approach may be ineffective in anticipating China's military strategy, and misleading, especially when assessing the use of China's cyber capabilities in a war with India in isolation.

The first section of this paper analyses the debate between cyber optimists and cyber sceptics and examines why Russia's cyberattacks were neutralised in the initial stages, enabling Ukraine to make a recovery. This section also dives into the distinctive characteristics of Russia's CW capabilities as well as Moscow's approach to information warfare (IW). The second section highlights that a Sino-Indian boundary war may undermine some assumptions regarding CW effectiveness due to China's formidable capabilities relative to Russia in CW and the fusion of the latter with other vectors of attack such as EW and counterspace capabilities. Thus, the evidence extrapolated from the Russo-Ukrainian war is inadequate for understanding the effectiveness of cyberattacks, as China's military is likely to pursue a limited set of objectives that would be driven by more effective employment of cyber capabilities. Additionally, China could effectively employ CW and EW in a limited aims war—an approach that Russia has not yet adopted in Ukraine. The third part assesses the Chinese military's synergised use of CW, EW, and SW through the People's Liberation Army Strategic Support Force (PLASSF) to undermine the performance of or target and destroy India's systems, such as command-and-control (C&C), communications, and weapons systems. The final section analyses the steps India needs to take to counter the Chinese military's use and application of cyber technology.

Why Russia's 'Poor' Cyber Performance Is Not the Full Story

There are two schools of thought around Russian CW performance in its conflict with Ukraine. The cyber optimists echo Jason Healy, who stated, "If Russia does attack Ukraine in the coming weeks, the opening salvo is likely to be with offensive cyber capabilities."[8] One set of American experts also stated that cyber warfare capabilities would witness "massive employment" by Russia, leading to a possible collapse of Ukraine's defences.[9] Meanwhile, cyber sceptics claim that Russia's cyber technology was sub-optimal even before the full-scale invasion of Ukraine.[10] There are three factors which could explain Ukraine's success in neutralising Russian cyberattacks, some of which were initiated prior to the invasion or coincided with the invasion.

First, Russia's cyberattacks were blunted by Ukraine's pre-war preparation. Before the Russian invasion in late February 2022, Ukraine served as a laboratory where Russian cyber operations were implemented without actual use of force or a tangible impact on the kinetic operations of both countries.[11] These operations also failed to achieve a measurable strategic effect in Ukraine.[12] Second, the Russian invasion was ambitious in its objective of seizing Kyiv and attacking along multiple axes to shock Ukraine into submission without exhausting all the means at Russia's disposal, notably airpower and cyber resources.[13] Cyber sceptics concede Jon Bateman's assessment that in a surprise launch of a war, attacking in the way Russia carried out its cyber onslaught against Ukraine may be effective if the conflict is of short duration, but not in bigger and protracted wars, as witnessed today in the Ukraine.[14] Cyber sceptics are further overstating the failure of Russia's cyber operations against Ukraine; notwithstanding Russia's CW effort, this 'failure' cannot be extrapolated to mean that China's cyber operations in a potential war with India will have the same outcome.

The third factor is that China is likely to make every effort to keep a war with India short; a long-drawn-out war would only redound to the PRC's disadvantage, which would be antithetical to 'winning without fighting' and securing a decisive victory at the lowest cost. Additionally, in a protracted war, the PLAA, PLAAF, and the WTC are likely to incur the same costs

as Russia in Ukraine. Western assistance to Ukraine enabled the latter to make a swift recovery after the initial wave of cyberattacks by the Russians, which partly explains Russia's purported CW failure.[15]

Ukraine's cyber defence against a formidable Russia is widely hailed. Since Russia's occupation of Crimea in 2014, Kyiv has invested heavily in a 'whole of society' approach to fend off Russian cyberattacks.[16] Ukraine suffered a cyber onslaught across several areas, including the energy, media, business, and non-profit sectors.[17] Russia was initially successful in neutralising Ukrainian communications by penetrating the latter's digital networks and military communications.[18]

An hour prior to the invasion on 24 February 2022, the Russian Main Directorate of the General Staff (GRU) hacked into a KA-SAT communications satellite owned by Viasat—an American communications company. Russia is believed to have combined EW with CW in the form of jamming and hacking to disrupt Ukrainian communications, which Ukrainian forces likely never fully identified.[19] These commands overrode data and disrupted satellite connectivity, neutralising thousands of routers that the Ukrainian military relied on for command and control communications.[20]

It is likely that Russia aimed to seize control of Ukraine's networks without resistance.[21] However, the number of attacks declined after the first five weeks of the conflict.[22] This decline cannot be attributed exclusively to Ukraine's cyber resilience and adaptation. Additional factors helped Ukraine make a recovery: corporate ownership and technical architecture were decentralised; engineers became more adaptable and agile;[23] the industry stepped up to support the war effort; and Ukraine had made significant pre-war efforts to render their cyber networks more resilient.[24] Finally, external assistance from the privately owned SpaceX, which made its Starlink satellite communications network available to the Ukrainian military,[25] assisted in Ukraine's recovery. Starlink's 2,000 space-based high-speed satellite internet service connected to 10,000 ground-based terminals, rapidly neutralising Russia's initial cyber success.[26] At least since the onset of war, as General Nakasone, Commander of the United States Cyber Command (USCYBERCOM) and Director, National Security

Agency (NSA) made clear, the USCYBERCOM has conducted range of operations covering Defensive Cyber Operations (DCOs), Offensive Cyber Operations (OCOs) and Information War (IW) on behalf of Ukraine.[27] This undermining of Russia's cyberattacks has led to cyber sceptics arriving at partially erroneous conclusions about CW. It is unlikely that Ukraine would have successfully blunted Russian efforts without Western assistance. Specifically based on the Russia-Ukraine war it is hard to complete a generalisation about lessons due to a prior grey zone conflict and significant use of resources by external actors and the private sector especially on behalf of Ukraine.[28]

Furthermore, Russia's CW capabilities are relatively weaker than those of China's.[29] Contrasting Russia's and China's CW capabilities will expose some of the frailties in Russian CW. A large proportion of Russia's Offensive Cyber Capabilities (OCC) is vested with cyber criminals rather than being concentrated with the Russian military.[30] Most highly skilled cyber operatives of the Russian Federation remain largely under the control of the domestic intelligence agency, the Federal Security Bureau (FSB). Until 2014, the latter, as well as the GRU and the Ministry of Internal Affairs are believed to have strongly opposed the establishment of a significant cyber-focus on military operations.[31] CW for military operations has never been the strong point of Russia. Moscow has framed neither strategy not doctrine around the offensive dimensions of cyber operations, and very few military personnel have been trained to employ them.[32]

Further, as the war against Ukraine has demonstrated, Russia has not effectively blended conventional military operations with cyber operations.[33] This is one of the key differences between Russia's use of CW and that of the PRC's, further indicating why India needs to be doubly cautious and guard against limiting the growth of its own defensive and offensive cyber capabilities for military operations. The PRC's offensive cyber capabilities exceed even those of the United States and Russia.[34]

Indeed, China is the foremost power in the field of cyber exploitation. Between 2012 and 2021, Chinese cyber warfare units carried out more zero-day vulnerability exploits than any other cyber power.[35] China's cyber-technical personnel stands at around 60,000, with a large number

of them dedicated to offensive cyber operations, which is ten times that of the USCYBERCOM;[36] according to the International Institute of Strategic Studies (IISS), 18.2 percent of the PRC's cyber units are focused on executing offensive cyber operations, in contrast to the USYBERCOM's 2.8 percent.[37]

For states such as India, which are confronting the PRC's CW and EW capabilities as well as Beijing's capabilities across the electromagnetic spectrum (EMS), the reality becomes even more daunting. India is unlikely to be a beneficiary of Western assistance as Ukraine (specifically from the US), owing to the latter's geographic importance to European security, as well as India's relative size and capabilities compared to Ukraine. Kyiv received assistance from the US and its allies from the North Atlantic Treaty Organisation (NATO) derived from the historically antagonistic relationship between the West and Russia. The geographic proximity of Ukraine to several European members of NATO threatened by Russian aggression further compelled the West to aid the Zelensky regime. NATO views Ukraine as a buffer state and thus strategically consequential for Western military alliance.[38]

On the other hand, American reluctance to extend cybersecurity cooperation to India is evident in its absence in the US-India initiative in Critical and Emerging Technology (iCET) concluded between the national security advisers of the two countries in January 2023.[39] Historically, a lack of mutual confidence in the cyber domain as well as "diplomatic discrepancies" have hindered closer cooperation between Washington and New Delhi.[40]

Thus, the limitations of Russia's cyber offensive against Ukraine must be viewed in the context of the external support received by Ukraine, as well as Ukraine's pre-war preparations.

The Importance of Cyber Fires in a Sino-Indian Boundary War

Despite the weaknesses of cyber technology in the Russia-Ukraine conflict, caution must be exercised in assessing its implications for India in a military contest with the PRC, as the Indian armed services cannot discount the vigorous and efficacious application of cyber warfare by the Chinese military.

The first issue to be considered is the duration of a potential Sino-Indian boundary conflict, in addition to the role of cyber operations in it. The duration of a conflict and the efficacy of cyber arms are inextricably linked, with the latter being as much a function of China's objectives as the effectiveness of its cyber capabilities. A short-duration limited-aims conflict—which is what the PRC is likely to pursue—would be decisive. A short, limited-aims conflict that employs cyber fires will likely be highly effective. A war fought for limited aims does not mean that it needs to be fought with limited means; the means are likely to be disproportionate, thus requiring total commitment.[41] Therefore, China is likely to employ CW and EW, alongside other vectors of attack such as counterspace capabilities.

China demonstrated its understanding of this requirement with the seizure of Indian-claimed territories in eastern Ladakh and managed to retain control in two of the five areas, with limited withdrawal. They have also deprived or blocked the IA from patrolling in several contested areas in Eastern Ladakh such as Depsang. Beijing was able to deploy large forces to seize the territories because of the exercises it conducts each year in the Xinjiang region, to which India responds with its own; however, India did not conduct exercises in 2020 due to the COVID-19 pandemic,[42] while the PLAA converted a military exercise into an attack to seize contested territory. The PRC is likely to seek a decisive victory at the lowest cost, dovetailing with extant PLA doctrine. It is also consistent with the Chinese strategy enunciated by Sun Tzu: "attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."[43,44]

Notwithstanding the Galwan clash, which claimed the lives of several Indian Army personnel and PLA soldiers in June 2020,[45] China has avoided pitched battle engagements with India since at least the 1960s;[46] after all, as then Chinese Defence Minister Zhang Aiping stated in 1983, it was imperative for China to fight at the lowest cost to secure the most challenging victory.[47] This can only be accomplished by way of the commander's competence in tactics and strategy, advanced military equipment and high quality military personnel.[48] This statement was made as the PRC emerged from a war with Vietnam in 1979, in which it incurred high costs, and Beijing has since avoided engaging in bruising military campaigns.

President Xi Jinping, in his speech to the 20th Party Congress in October 2022 observed that the Chinese military had to train under conditions of combat, equip itself effectively, be agile, adaptable and ensure complete competence in "informatised" and "intelligent warfare" which will make the PRC's security credible and allow China's management of crises, respond to threats and "win local wars".[49] This also entails leveraging technological innovation in civilian domain such as artificial intelligence (AI) and unmanned aerial vehicles (UAVs) for enhanced joint operations capability for the PLA to attain victory at the local or theatre level.[50] Xi's statement also indicates that the Western experience, such as the Persian Gulf War of 1990-91, also influenced the shift in China's approach under Jiang Zemin and subsequently under Hu Jintao.

However, there were two additional shifts, namely, greater offensive capability, which departed from an exclusive focus on a defense-in-depth strategy with an anti-access area denial (A2AD) strategy that requires power projection capabilities[51] and is also aimed at preventing third-party intervention; and China's shift from employing large forces to overwhelm the adversary and deter an attack, to an emphasis on smaller ground forces combined with qualitative improvements in missile forces, better support for naval power, and a more general effort to ensure that the quality of Chinese forces matches that of the US[52] and exceeds that of other states such as India.

The Importance of Cyber Fires in a Sino-Indian Boundary War

Disabling missile forces without kinetic interventions requires cyber tools. Cyber or malware attacks against tactical communications systems, command and control centres, and weapons systems at the operational and tactical level are likely to aid China in a potential Sino-Indian confrontation, thus demanding attention to a key facet of Chinese military thinking. Under what China calls System Destruction Warfare (SDW), the PLA's capabilities require comprehensive integration and the capability to identify and hold at risk all of the vital operational functions of the adversary.[53] The operational system consists of several elements that link organisations, functional processes, and enabling networks to ensure integrated joint operations by the warfighting domains of the service arms of the Chinese military spanning.[54] Aside from these key elements, the SDW also consists of five components—the command system, firepower strike system, information confrontation system, reconnaissance-support system, and support system.[55] SDW fundamentally involves paralysing the operational system of the enemy without need for the latter's annihilation. As one Chinese expert stated, SDW can secure victory without completely destroying the enemy's critical capacities.[56] SDW involves destroying the enemy's information network, C&C sensors, and leadership without resorting to kinetic means; the combined use of CW, EW, and counterspace-directed energy weapons such as lasers and microwave weapons are likely to be as effective as kinetic means.[57]

Indian military planners should expect precision attacks geared for destructive action against Indian military assets, which limit costs to the PLA. Kinetic operations are likely to follow, but only after the PLA establishes complete information superiority over the adversary.[58] Kinetic strikes against India's space assets and other intelligence, surveillance, and reconnaissance (ISR) nodes are unlikely to precede efforts to establish information dominance and are likely to be executed only if they aid information superiority. Information superiority involves non-contact warfare using precision strikes against the enemy's C&C and network architecture, which are necessary to aid surgical, precision, and decisive kinetic strikes that enable localised operations and eliminate the need for massed attacks and a war of annihilation.[59,60]

The Importance of Cyber Fires in a Sino-Indian Boundary War

China will emphasise qualitative effectiveness, timing, and targeting of the attacks rather than the quantity and strength of their forces. This requires attaining the "Three Dominances", i.e., the "command of the sea, command of the air and information dominance".[61] The latter is the most critical, as command of the air and the sea would be impossible without information dominance.[62] If China's war aims are restricted to limited territorial seizures from India—a likely possibility with regard to its historic claims over Arunachal Pradesh—it is likely to employ the means discussed above.

> "A short-duration limited-aims conflict—which is what China is likely to pursue—would be decisive."

PLASSF in Kinetic Operations Against India

The scope of China's military aims against India are critical to the success of the PLA against the Indian armed forces, especially the IA and the IAF. The Russian military's actions in Ukraine may enable the Xi-led leadership to understand how not to prosecute a war and the degree to which cyber weapons might be effective in the support of kinetic operations. Prosecuting a limited-aims war, with optimum use of both kinetic and cyber warfare capabilities, could be the only way in which the Chinese military can inflict a decisive victory on India.

The question remains as to how a Chinese military offensive against India would unfold. The PRC, following Russia's military campaign, may consider a war with more limited objectives along the Line of Actual Control (LaC) that involves shallow or limited territorial seizures rather than deep attacks into Indian territory such as seizing the whole of Arunachal Pradesh or, as China calls it, Tawang. Such a military campaign would involve limited land grabs along multiple fronts, and China could begin its military campaign with cyberattacks that might prove reasonably effective in destabilising India's C&C and communications architecture, followed by a barrage of artillery and missile attacks aided by their own computer, communication, command, control, intelligence, surveillance, and reconnaissance (C4ISR) capabilities against the Indian military's static and mobile targets. The PLASSF is China's integrated information warfare service that combines SW, EW, and CW capabilities to achieve information dominance in the early stages of military hostilities on China's immediate land and maritime frontiers,[63] and it could employ any of the capabilities available to it across the EMS.

The PRC possesses larger cyber forces than India, making it a potent cyber adversary.[64] Destruction and disruption are only one means of compromising communications and information networks; for instance, the PRC could conduct CW in the form of offensive cyber operations (OCOs) to inject false information into India's networks through India's satellite navigation (SatNav) system, the Navigation with Indian Constellation (NAViC), which performs positioning, navigation and timing (PNT) functions.[65] Deception, rather than subjecting the target to disruption and destruction, would be beneficial.[66] Since the NAViC relies on ground-

station control to ensure precision control and monitoring, there are significant opportunities for the PLASFF to use methods of deception.[67]

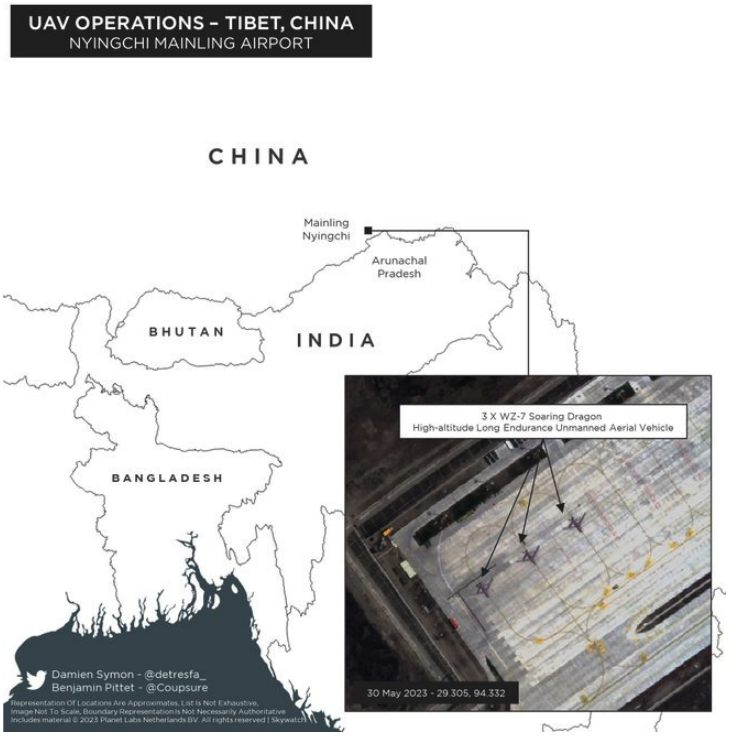
Manipulating the data in the control and monitoring mechanisms of satellites would degrade their performance without indicating the existence or cause of the issue, resulting in the adversary relying on the PNT system to launch missiles that end up missing their targets by a substantial degree.[68] Thus, cyberattacks against space-borne targets can be undertaken by engaging the ground segment of India's space programme.[69] An attacker can also take direct control of the onboard sensors of the spacecraft through the direct transmission of computer code to satellites through the ground station.[70] Assuming that the PRC will engage only in disruption or destruction and not in the deception of India's NAViC, it could compel Indian military commanders to switch to non-precision munition attacks.[71] This would result in India exhausting its munition stocks without imposing any tangible costs on the PLAA and PLAAF military targets.

China has already employed a combination of EW and CW targeting India's satellites, fighter aircrafts, and UAVs.[72] China's WZ-7 High-Altitude Long Endurance (HALE) UAVs, based out of the Nyingchi Mainling Airport, located 15 kilometres north of Arunachal Pradesh, actively collect ISR data (Figure 1). WZ-7 UAVs, active since 2018, have also been deployed at the PLAAF's Shigatse airbase, located 150 kilometres north of Gangtok, Sikkim.[73] The ISR functions of these HALE drones lay the foundations for offensive CW and EW missions against India's static and mobile military assets.[74] The WZ-7 HALE UAVs are also capable of generating targeting information derived from their electronics intelligence (ELINT), optical reconnaissance (OR), and radar reconnaissance (RR), enabling the Chinese to use their array of missiles for precision fires against India military targets.[75]

The Chinese military has also deployed a more advanced supersonic WZ-8 variant, which has sophisticated surveillance capabilities consisting of potent electro-optical cameras and sensors capable of generating mapping data in real time.[76] WZ-8's Synthetic Aperture Radar (SAR) can map terrain by night and under fog and cloud cover.[77] The WZ-8 has already conducted reconnaissance missions against South Korea and Taiwan.[78] It

can achieve up to Mach 3 speeds and was potentially designed as a weapon for A2AD missions. It was introduced at a parade in Beijing in 2019 to celebrate the 70th Anniversary of Chinese Communist Party (CCP), though there was no credible evidence of it being operationalised at that time.[79] While it is yet to perform an attack role, it can be modified sufficiently to execute attack missions, rendering it nearly impossible to detect and intercept.[80] Neither the US nor India has comparable drone capability. As the American defence expert Dean Cheng observed, "This is not just aimed at the United States or South Korea. Japan has to worry about it. India has to worry about it. All Southeast Asia has to worry about it."[81] The WZ-8 forms an important part of China's "reconnaissance strike complex", which aims to "Find the enemy, hit the enemy, kill the enemy."[82]

Figure 1: Chinese UAV Deployments for ISR Missions



Source: Damien Symon and Benjamin Pittet

Additionally, it is evident that China has closely studied the impact of other operational dimensions of CW across the EMS. Active electronic scanned array (AESA) radars that permit the simultaneous transmission of radio beams and software defined radios (SDRs) which change how radio waves are transmitted depend on computer systems to carry out operations across the EMS.[83] Software moulds how radios carry out transmissions, rendering it difficult to detect the transmission of radio or radar signals.[84] Transformation of software can easily alter a receiver to a transmitter, and AESA radars with small arrays are specifically suited to beam out radio energy at likely targets.[85] China's attempts to hack into computer systems used for satellite communications surpass Russian cyber capabilities; Beijing's cyber capabilities to prevent inter-satellite communications are rendered easier as satellites operate in clusters.[86] This type of hack would prevent space-ground communications by disrupting and degrading signal relays between the satellite and weapons system and visual and electronic data.[87] This is consistent with the PRC's quest to dominate the battlespace, which has two components. The first is the information domain, which encompasses SW, EW, and CW as discrete domains of warfare, such as air, water, and land. The PLASSF is responsible for securing and establishing dominance in these domains.[88] The second requirement for the PLASSF is close collaboration for the execution of joint operations regionally and globally with each of the service branches of the PLA, namely, the PLAA, the People's Liberation Army Air Force, the People's Liberation Army Navy, and the People's Liberation Army Rocket Forces (PLARF).[89] The PLASSF's functions can be described as hybrid, with at least one part, such as the space elements of the service, reporting to both the CMC and the theatre commands (TCs).[90] In order to boost joint warfare, the PLASFF deploys units with services for training and exercises.[91]

Although some of the issues surrounding C&C were unclear until 2020, the Chinese have made strides in coordinating and synchronising the PLASFF's functions with the TCs and the ground units of the PLAA. The Chinese official declaration is "CMC leads, theatres fight and services build".[92] Theoretically, this would imply that PLASSF personnel fall directly under the five TCs; in practical terms, however, the SFF, similar to the PLARF, which manages China's nuclear capability, reports directly

to the CMC, as both forces are deemed 'sufficiently strategic'.[93] However, it is likely that PLASFF computer engineers or software developers would be embedded in TCs and PLA ground units, especially in the Combined Armed Brigades (CAB) of the 76th Group Army of the PLA's Western Theater Command (WTC),[94] as Ukraine has done in the war with Russia.[95]

The PLAA and PLASFF have conducted combat exercises involving a red brigade belonging to the 80th GA and a blue brigade of the 81st GA in a highly informatised environment featuring satellite communications and testing communications between small, dispersed units, which will obviate annihilation by the enemy and ensure survivability.[96] The PLASFF and the PLAA have also conducted exercises involving a PLASFF base in confronting a brigade of the 83rd GA in a dense electromagnetic environment.[97] Lower echelon units of the PLAA at the brigade level and below get critical combat support for EW missions and Signals or Signals Intelligence (SIGINT). A service support brigade is attached to each of the GAs and consists of various elements, including logistics, medical, repair, ammunition, command and communication (signals and communication), and EW. The signals component of the brigade uses traditional and network communications across the entire GA combat zone.[98]

Earlier, all communications were handled at the divisional command level, with weak communications at lower echelons.[99] Given the emphasis on information-based operations across the PLAA, signals capabilities across all the tactical units have been augmented.[100] The signals component is geared to ensure cyber connectivity to PLAA units, defending communications network across units from jamming, electromagnetic attack, and hacking or 'cyber intrusion'.[101] The use of an EW regiment is highly consequential, indicating a strong commitment to both EW and CW at the tactical level of operations.[102] The EW regiment is divided along five distinct segments—electromagnetic attack and jamming; long-distance electronic surveillance; electromagnetic protection; network or cyber operations; and communications operations.[103] PLAA EW regiments are likely to be used to provide close operational support to the PLAA artillery and air defence (AD) brigades, similar to Russia's reconnaissance fire system.[104]

PLASSF in Kinetic Operations Against India

Having witnessed Ukraine's battlefield performance through employing AI-augmented algorithms and optimising sensor data from diverse sources such as commercial satellite imagery and intelligence instruments at the disposal of the West,[105] China is likely to replicate the application of AI-enhancing algorithms. 'Intelligent warfare'[106] or AI application will be critical for the amount of information that needs to be processed in real time and too excessive for humans to reasonably and accurately process.[107] This 'intelligent technology' will augment CW and EW and optimise the flow of information, significantly enhancing combat effectiveness in reducing sensor-to-shooter times and aiding the interruption of the decision cycle of the enemy in joint operations.[108] China has already tested and deployed AI-enabled swarm drones as part of its special forces (SF) units and armoured brigades for reconnaissance missions.[109] In 2017, China set a world record by demonstrating how a swarm of 1,000 drones could perform a range of complex technical tasks.[110] The technical sophistication in the AI application of Chinese inter-drone communication, synergy, and cooperation have only grown since;[111] for instance, if a single drone or a set of drones in a swarm malfunctions, the remainder step in to compensate for the technical tasks performed by the malfunctioning drone or drones.[112]

Since 2017, China has also tested high-altitude or spy drones, deployed 20 kilometres above the earth's surface, to communicate with one other.[113] These drones are part of China's near-space technology geared for ISR missions.[114] The development of this capability is still daunting for China, since the extremely thin air or vacuum-like conditions at that altitude generate electric currents that can damage equipment.[115] Although the idea is novel, Chinese technical experts concede that the effective military application of swarm drones at high altitudes remains an open question.[116] Consequently, there has been little evidence of significant progress since the 2017 tests.[117]

AI enhances the PLASFF's CW and EW. Informatisation and intelligentisation are inextricably linked, such that computing power and data are necessary for AI which, in turn, enables the accurate processing of vast information on which battlefield decisions are made.

Russia's EW has proven to be far more effective than CW for most of the war against Ukraine's communication and military targets and are estimated to have eliminated 90 percent of Ukrainian drones, depriving them of precision strikes.[118] This does not imply that CW should be ignored, but that, in a protracted war such as the Russo-Ukrainian war, EW is likely to be more effective. Given that China's approach to informatisation involves the large-scale fusion, wielding, and application of information to secure national objectives during both war and peace, the PLA is likely to exploit cyber tools as well as tools across the information spectrum. Although the PLAA has achieved mechanisation and made significant progress towards informationisation, the latter remains incomplete. Intelligentisation, which follows informationisation, involves the use and application of AI, paving the way for the PLAA to establish a significant gap between itself and its adversaries.[119] The PLAA sees all three elements—mechanisation, informationisation, and intelligentisation—not just as successive stages, but also as inextricably linked and mutually inclusive.[120]

Throughout the 1990s and the 2000s, the US did not consider the PRC to be a consequential military power in networked warfare.[121] This notion was quickly dispelled in the 2010s, with growing evidence of the PLA conducting military exercises involving informatised joint warfare.[122] China's attempts to surpass the US have widened its gap with India in CW, EW, and EMS capabilities, and more generally, in Network Centric Operations (NCOs). The Science of Military Strategy (SMS) "is a particularly valuable resource for understanding China's evolving strategic approach to network warfare. A study that aims to be as comprehensive as the *SMS* cannot afford to ignore network warfare due to the centrality of information warfare to modern war-fighting, and the process by which the *SMS* is written ensures that the information analysts receive on network warfare represents something approaching an authoritative consensus within the PLA."[123] This is where we turn to the role of other information sources which may be applied independently or fused and complementarily applied with cyber operations.

PLASF's Other Capabilities in a Sino-Indian War

A Chinese limited-aims military campaign may take place when India and the world are distracted by crisis and the former's attention is diverted from the contested frontier. Further, China is likely to pick a moment that prevents third parties from aiding India in the event of a war. Consider the 1962 Sino-Indian boundary war. It occurred in parallel with the Cuban Missile Crisis, and neither the US nor the Soviet Union could assist India in time; in fact, the latter colluded with the PRC, at least momentarily. By the time Washington came to New Delhi's aid, the war was over, with the Chinese withdrawing behind the McMahon Line in the eastern sector of the Sino-Indian boundary.

China's most recent military action against India took place in April-May 2020, during the COVID-19 pandemic, when it occupied five vacant areas in eastern Ladakh, leaving Indian forces de-alerted and demobilised. Consequently, the IA could not respond to the PLAA intrusions in time. At least two of these areas, namely, Demchok and the strategically critical Depsang, remain under Chinese control. Notwithstanding greater vigilance and alertness by the IA and IAF, the PRC's WTC will be crucial in exploiting opportunities that emerge either as a direct result of the domestic upheavals in India's restive north-east and the consequent redeployment of India forces or an international crisis sufficiently diversionary and distracting to stage an attack.

Further, the salami-slicing in Ladakh and the intrusions in the Yangtse in Arunachal Pradesh in December 2022 should be seen as part of the PRC's grey-zone strategy, which helped Beijing secure low-cost gains to probe the Indian military's weaknesses. A key lesson for China is that escalating from grey-zone warfare to conventional warfare, as Moscow did in February 2022, could come at significant costs,[124] whereas a grey strategy aids cost effectiveness for Beijing.

However, the Indian military should not count on the Chinese military confining their strategy to grey-zone warfare, as Beijing could escalate to a conventional limited-aims war with disproportionate means—which Moscow never did against Ukraine—which may enable the PRC to make sizeable territorial gains beyond what it did in eastern Ladakh. This is why

India's civilian and military leadership should remain alert and prepare methodically for a potential Chinese escalation from their current grey-zone warfare.

Another plausible scenario derives from the diversionary theory of warfare, which assumes regime weakness and domestic disorder as a cause of war.[125] Territorial conflict, as is the case between China and India, is likely to arouse intense emotions contributing to deep social unity and mobilise the public allowing and encouraging leaders to become bellicose.[126] Such problems can provide the Xi-led leadership, facing problematic domestic conditions, with an easier pathway to trigger a war.

The Chinese economy is struggling to revive following the lifting of the COVID-19 pandemic restrictions in December 2022.[127] The Xi regime's arbitrary use of state power has generated considerable uncertainty among the Chinese public,[128] which could trigger popular unrest and discontent. Consequently, in order to divert the attention of the Chinese public from domestic discontent and resentment towards the Xi-led leadership, the Chinese leadership may escalate with a conventional attack, especially in the eastern sector of the Sino-Indian boundary, where Chinese claims have historically been more salient.

Finally, a remote, yet likely scenario involves Pakistan's role in opening a second front. Pakistan's role in aiding a potential Chinese attack could come in the form of limited probes along the Line of Control (LoC) or even a general mobilisation of Pakistani forces across the stretch of the International Border (IB), generating sufficient diversionary pressure on India, thereby upsetting the IA, IAF, and the Indian Navy's (IN) military deployments.

Therefore, China will attack when India least expects it, when it senses sufficient weaknesses in India's conventional capabilities and deployments.

The likely trajectory of China's military onslaught will involve the PLASSF's EW capabilities against India's space-borne navigation system, with NAViC[129] being among the first key targets of disruption, by employing jamming (EW). Among the most used forms jamming as an offensive

and a defensive weapon is communication jamming technology.[130] While disrupting Indian satellite uplink and downlink communications through EW is likely to be the PLASSF's preferred method, it could also hack the communications in a way that enables and supports the PLAA and the PLAAF's ground and air operations, respectively.

The PRC also possesses Direct Ascent Anti-Satellite (DA-ASAT) capabilities, which can target spacecrafts not just in the low earth orbit (LEO), but also in the geostationary orbit (GEO). India's NAViC satellites in GEO which can be targeted by DA-ASAT include the Dong Neng-2 (DN-2), which was first tested in 2013 from a launch site in Korla in Western China.[131] DA-ASAT can take out space-borne targets in GEO, although it is likely to take 4-5 hours for interception, allowing sufficient time for India's GEO spacecraft to execute evasive action.[132] Owing to their limited numbers, the loss of even one geostationary satellite (GEOSAT) due to a successful DA-ASAT strike would constitute a serious setback, impairing Indian wartime operations.

Beyond kinetic attack counterspace technologies, a successful electromagnetic pulse (EMP) attack would damage any communications satellites in GEO. The PRC is known to possess High-Altitude Electromagnetic Pulse (HEMP) capability, also known as Super-EMP, which is a weak nuclear device that can be detonated at the high altitude of 70-100 kilometres above the earth to produce an EMP field of up to 10-100 kilovolt per metre (kV/m), which can melt and destroy the electrical circuit and electronic components of satellites.[133] The use of this capability by the Chinese in a military contingency is remote, as this may cause collateral damage to other orbiting spacecrafts, including Chinese satellites.[134] However, an EMP capability can be harnessed as a microwave attack against orbiting spacecrafts which, along with a HEMP attack, could destroy the battlefield communications of the adversary and establish Chinese information superiority through restricting the tactical performance and survivability of informatised equipment.[135] However, technology related to high energy attacks in the space domain are still in an incipient stage.[136] States such as the Russian Federation, the United States and several others [including the PRC] have poured resources in to Research and Development (R&D) in Directed Energy Weapons (DEWs) such as

high energy lasers and developed some limited operational capabilities. Nevertheless, DEWs are still being laboratory tested and there is no known credible laser technology that can be effectively used for military missions.[137] Regardless of this assessment, the Chinese are rapidly making investments to match the US in kinetic kill capabilities launched from the ground and space to jam and obfuscate satellites.[138] Alternatively, the PLASSF could fuse CW, EW, and SW capabilities in a coordinated assault that may not involve kinetic operations, but are restricted to the seizure and control of India's space, electronic, and cyber networks. This could be instrumental in engineering India's 'surrender without fighting'—the "highest state of war"—thereby enabling China's control of escalation and management of crisis.[139]

The PLASSF was also established with the aim of enabling the PLA to undertake combined arms warfare—an organisational shift that the PLA is yet to master, although there have been signs of progress since its inception in 2015. China has taken specific measures in terms of their capabilities, which include following the following dictum: "The CMC in overall command, TCs managing combat, and services managing force construction."[140] The PLASFF's primary mission is to serve as an enabler of joint operations for TCs.[141] The space mission of the PLASSF will enjoy "primacy" compared to their "terrestrial counterparts".[142] For instance, the PLASFF's space mission will be responsible for identifying radar signatures, infrared heat signatures, and electronic signal emissions; and preparing a profile of targets based on imagery intelligence (IMINT)[143] along the LaC and military facilities, thus forcing concentrations, weapons systems, and installations deeper inland in India. This effort will help identify, track, and target weapons systems and platforms. All collected information will be relayed to intelligence-gathering entities in the operational and tactical units of the TCs for air defence, early warning, and surveillance, and the information can be used to target the sensors, radars. and communications networks of the IA and IAF through cyberattacks and jamming.[144] All PLA conventional missile strike missions will be supported by the PLASSF in the form of identification, detection, guidance, and post-attack battle damage assessment.[145] As a single integrated force, it will be able to aggregate information from a range of sources to boost domain awareness[146] and provide corresponding target acquisition and precision-strike capabilities

to TCs and their lower echelon units such as the group armies and the combined arms brigades (CAB). The only crucial caveat is how the Chinese command architecture will work in wartime as opposed to peacetime. In the latter case, the PLASSF will tend to be tightly controlled and report to the CMC, since it is considered to be too strategic.[147]

In a military offensive against India, the WTC with support from the PLASSF will be at the sharp end of the spear. We have already witnessed a partial glimpse of the PLA's use of disinformation that revealed no hint of its attack plan, which led to the seizure of five areas claimed by India in Ladakh in April-May 2020, precipitating a massive stand-off between both countries that persists to this day. More importantly, the success of the WTC and PLASSF, in concert with the CMC led by Xi Jinping, represents a good example of China's control of information to execute an occupation of territory by employing thousands of troops. Russian cyberattacks, which also involved the complementary employment of EW, lasted five weeks. A Chinese military offensive against India that lasts five weeks might be sufficient to secure limited territorial gains to rout Indian forces. This ties back to Bateman's argument that CW is likely most effective in short-duration conflicts.[148] In a limited-aims military campaign to secure marginal territorial gains, the cyber capacities of the PLASFF as well as its EW and space-borne and counterspace capabilities are likely to be effective for the duration of the conflict. Keeping the conflict short will enable the PLA maximal or optimal exploitation of cyber tools against India.

Even if cyber tools may not be as effective on their own, the PLASSF has other vectors of attack available, such as EW and DA-ASATs, and the complementary use of these capabilities with CW may prove effective. Fundamentally, cyber operations necessitate a relentless reconnaissance in cyberspace, development of cyber capabilities and the exploitation of cyber effects, which can be effectively used to gain advantages over the adversary in a war.[149] Reconnaissance and attack missions are tightly linked in the cyber domain, where cyber offence and intelligence capabilities are a necessity[150] for the Chinese military. The core of the PLA's strategy will involve penetrating and neutralising the IA and the IAF's communication and digital networks, which are central to executing combined air-land battle operations by the IAF and the IA, including the latter's combat

arms. The PLA views the cyber domain as "inherently offense dominant", necessitating a "strong attack mentality",[151] thus requiring the PLASSF to be involved in the relentless preparation and development of capabilities that seek to identify and exploit vulnerabilities in adversary weapons and networks.[152]

Since the Eleventh Five-Year Plan (2006-2010), there has been considerable progress in informatisation in PLA training at its bases. PLA units at these bases have built up their information systems to address the training requirements of informatisation as well as provide guidance and adjustments for effective cyber operations in joint operations.[153] Relentless troop training in cyber operations and command is key to combat effectiveness. However, the PLA has found cyberspace to be challenging for both training and command as it has considerable differences from other domains such as sea, air, land, and space.[154] Cyberspace combat command training involves integrating and fusing information from multiple sources such as air and space reconnaissance intelligence, hydrological and meteorological data, and information derived from the EMS; training that simulates cyber command combat training for offensive and defensive cyberspace and the verification and testing of cyber weapons; developing proficiency in the use of cyber weapons by exploiting and destroying the adversary's network communications, software operations, information processing capacities, control over computers, and creating problems for adversary equipment; and guidance and control, which are at the core of all activities involving the integration of training information, allocations for training resources, and setting up training patterns.[155] It also involves fusing multidomain information and linking and coordinating with multiple nodes of the PLA, resulting in time-efficient, flexible, and easy-to-use supporting software and hardware.[156]

To understand China's surveillance and reconnaissance missions against India's ground and air combat deployments along the LaC, the PLA's actions under the WTC and PLASSF need to be examined. This will further highlight the importance of INEW (CW and EW) in the event of an outbreak of military hostilities.

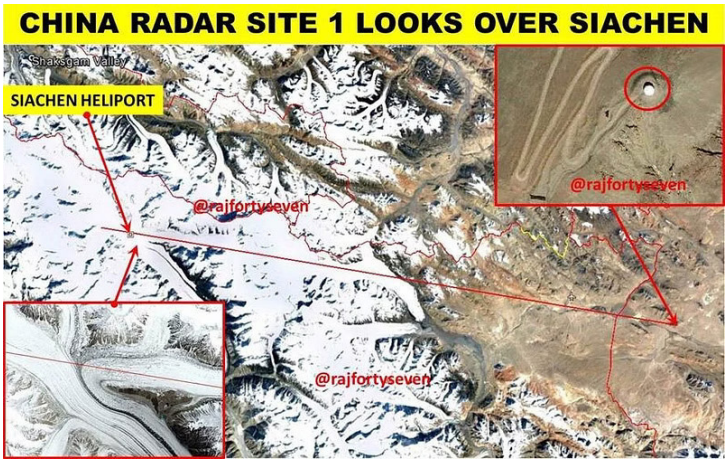
PLASF's Other Capabilities in a Sino-Indian War

From at least 2017, which predates the current boundary stand-off between India and the PRC, China has made significant investments in radar installations along the Sino-Indian boundary.[157] Earlier, China's ISR infrastructure-related investments were focused on their coastal regions,[158] whereas post-2017, China has established radar stations in the Depsang area, close to the Siachen glacier in the Sirjap area, and Demchok, which enable China to detect all ground-based and aerial activity on the Indian side.[159] These radome radars can monitor up to 125 kilometres inside Indian territory (Figures 2, 3, and 4) and certainly present challenges for the IA and the IAF; additionally, they possibly gather information with the help of installed sensors that analyse signals from IA and IAF installations as well as moving objects such as fixed-wing and rotary aircraft, alongside military ground traffic. To be sure, the IAF can take out these targets as well as China's advanced long-range and air surveillance radars such as the JY-27 A now deployed in locations close to Pangong Tso and Mianwali in Pakistan.[160] But these radars will be integral to enabling China's precision missile strikes and supporting robust air defence systems. They could also enable pre-emptive strikes against IAF and IA installations by the Chinese air force allowing the PLAAF to seize the initiative.

Radar sensors provide considerable data. They emit electromagnetic waves, and the signal reflection enables them to gauge flight time.[161] They are also known as Frequency Modulated Continuous Wave (FMCW) radar; the sensor emits a chirp and the time lag or interval for the received chirp helps determine the distance of the object.[162] The sensors are also capable of detecting microwave emissions. Such data can support China's electronic attack against the IAF's airborne communications.

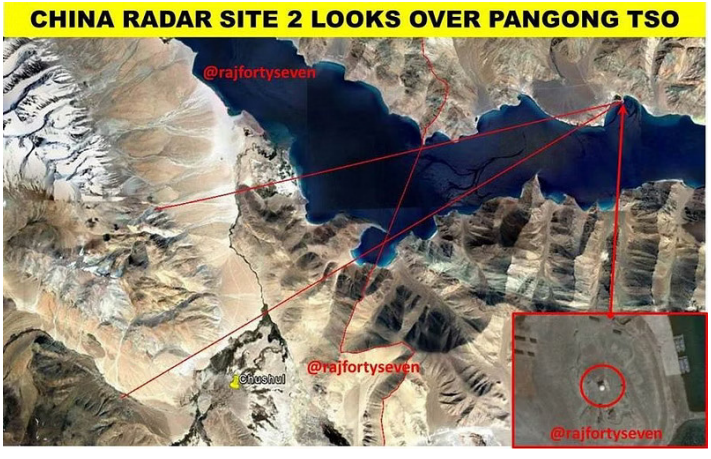
Radar sensors will be a key source of information for China to aggregate crucial data to execute precision kinetic strikes against India's static, mobile, and airborne targets. In addition, China's space-borne and airborne sensors are likely to help with the geolocation of Indian radar and communications installations, ground-based air defence (GBAD) systems, missile bases, and IA and IAF base facilities. Beyond these static installations, China's airborne and space-borne sensors are likely to play a key role in determining multiple characteristics of enemy targets, such as their shape and structure, thus paving the way for real-time kinetic assaults.[163]

Figure 2: Chinese Radar Sites Overlooking Siachen



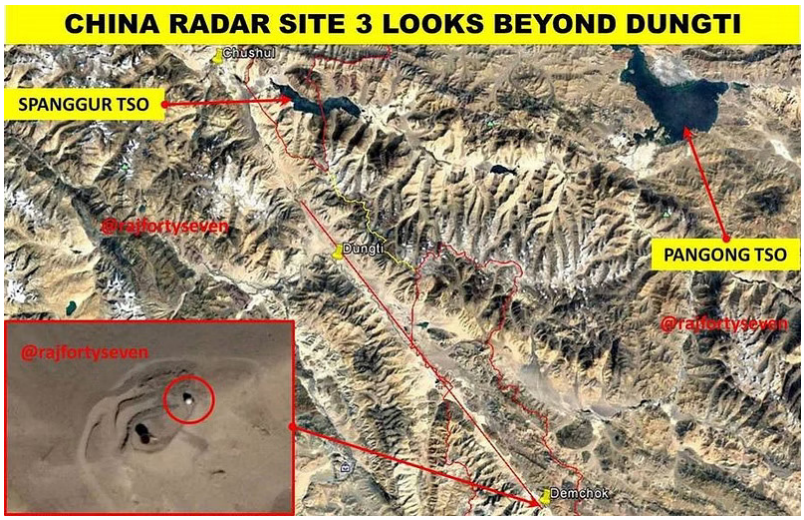
Source: Bhat (2017)[164]

Figure 3: Chinese Radar Site in the Demchok Area



Source: Bhat (2017)[165]

Figure 4: Additional Chinese Radar Sites in Chushul, Demchok and Pangong Tso



Source: Bhat (2017)[166]

On the eastern side of India's boundary with the Chinese, the latter have undertaken measures to bolster their positions along the Tibetan Plateau. The WTC is the primary TC dedicated to military operations against India. The 76th and 77th GAs of the PLAA are integral to WTC ground missions against India and across land frontiers with other states. However, the Southern Theater Command of the PLAA is also likely to play a critical role in military operations, especially in the eastern section of the boundary;[167] the latter will be more rapidly mobilised as a reserve force to the Tibetan theatre for military operations against India.[168] Each of the GAs has brigades dedicated to specific operational functions, including an artillery brigade, an air defence brigade, an army aviation or air assault brigade, a special forces brigade, an engineering and chemical defence, and a sustainment brigade.[169] The combat vehicle variants used consist of heavy tracked armoured vehicles, medium-wheeled armoured vehicles, and light high mobility vehicles such as high mobility, mountain, air assault, and motorized brigades.

There was considerable apprehension and dire predictions about the impact of cyber capabilities in the run up to the Russian invasion of Ukraine in 2022. While cyber optimists claimed that cyber technology can deliver independent effects and complement conventional operations, it was the cyber sceptics who appear to have been vindicated by Russia's "poor" cyber performance. However, Russia employed limited combined CW and EW capabilities, with fewer CW resources than expected or required. Additionally, Russia's military strategy has generally involved looting, abduction, rape, and the destruction of whole cities and towns without clear and concrete goals.[170] Further, Russia's failure to dedicate the necessary cyber resources to curb the invasion has left it fighting a protracted war. Today, Russia's war against Ukraine has become sluggish and is unlikely to serve as a template for how China might fight a war with India. Military officers with knowledge of India's CW and EW do not consider Russian 'failures' to indicate that India should not invest in CW;[171] instead, they recommend that New Delhi should redouble its efforts to secure a potent CW capability. They also reiterate that India cannot sit idly while the PLASFF or Network Division make significant investments and become repositories of potent capabilities.[172]

Polynomial-based encryption mechanisms will make way for quantum and post-quantum techniques, rendering the former redundant.[173] China is likely ahead of Russia when it comes to the application of quantum, quantum key distribution, and post-quantum techniques.[174] Consequently, India has to contend with a formidable adversary in the PRC, which is making dedicated investments in frontier technologies to augment Beijing's strength in the areas of CW, EW, and across the EMS.

While CW may have its limits in a prolonged war, its efficacy in enabling kinetic operations in a shorter limited-aims war cannot be ignored. It would be erroneous to contend that, because cyber fires had a limited effect in Russia's military campaign, China's cyber capabilities in a war against India are nothing to be alarmed about; CW, used in conjunction with EW, likely played a significant role in the initial stages of the Russo-Ukraine war and is likely to have a similar impact in a Sino-Indian war, especially if the scope of Chinese objectives is limited.

The key test and challenge for PLA strategists is to ensure that a future Sino-Indian war is brief and prosecuted decisively at low costs, dovetailing with the dictum of "winning without fighting". Penetrating and capturing or disrupting India's military cyber networks would be key to ensuring this. The mission requirements of the PLASSF and the warfighting arms of the PLA against India will constitute "systems destruction warfare". One expert noted that China is increasingly developing a deep aversion to taking casualties in a war, due to the decades-long one-child policy leaving limited able-bodied men fit for military duty.[175] Thus, it becomes imperative for China to prosecute a decisive, low-cost military campaign with India. Capturing India's cyber networks that contain the IA's C&C and tactical cyber networks connecting units from the infantry, armour, artillery, land-based conventional missile forces, and air defence is crucial for the PLASFF, especially at the outset of a conventional attack against Indian forces.[176] The disruption and neutralisation of communications between the IAF and the IA's air-land battlefield cooperation will also be a vital initial target.

However, China has not mounted nearly the same volume of cyberattacks against India that Russia has against Ukraine. China's cyber penetration of India's critical infrastructure is largely geared for reconnaissance missions, which serve as the basis for future cyberattacks.[177] This is equally true for cyber reconnaissance missions undertaken by the PLASSF as well as its units seconded to the WTC against the IA and IAF's communications networks and C&C. China is likely to keep its offensive cyber forces in reserve, using them only at a strategically opportune moment.

Even if Russia had a clear goal of neutralising Ukrainian resistance by seizing control of the latter's military information and communication networks and paving the way for the swift capture of Kyiv, the means adopted were insufficient to secure concrete goals. Russia's failures are indicative of the necessity of speed and appropriate measures for China's success against India. China has recognised that the complementarities between CW and EW in the form of INEW can be synergised and leveraged for information operations. Further, there are additional capabilities in the PRC's arsenal: for example, the PLASFF could employ an EMP capability against Indian satellites.[178] China is also known to be intensively developing

'Assassin's Mace' technologies, such as directed energy weapons, although there is considerable opacity around the development of these niche yet potent capabilities.[179]

The only caveat or discernible weakness would be at the level of command. Recently, American expert Charles Hooper averred that, "despite recent organisational reform efforts, the PLA remains essentially a political entity with a warfighting mission…its [PLA] approach to learning and leadership is heavily influenced by its own organisation, as well as traditional Chinese culture and education."[180] Centralisation of command could hinder the implementation of PLASSF and cyber units embedded with TCs and GAs. Lack of trust among senior PLA officers to delegate authority to lower-echelon officers could also be an impediment.[181] Together, these could pose potential pitfalls for China. However, the centralisation of command cannot be overstated, and Indian strategic and military planners should not assume that it will fail or remain a crucial chink in the Chinese armour. Beijing has several advantages in the PLASFF's information operations, both independent and in support of the TCs and their subordinate units, which will help with the unity of command and execution of operations.

> "The challenge for PLA strategists is to ensure that a future Sino-Indian war is brief and prosecuted decisively at low costs."

Recommendations and Conclusion

New Delhi needs to develop a unified service that combines EW, CW, SW, and SIGINT. The relationship between reconnaissance and CW operations necessitates a dedicated force like PLASFF. Notwithstanding recent progress following efforts by the Modi government to introduce legislation in parliament to create integrated theater commands (ITCs),[182] building a PLASFF-type force will not be easy. Additionally, IA officers have recommended the establishment of a Joint Inter-Services Network,[183] albeit without specifying whether it should be an agency-level organisation or a tri-service command-level one. The plethora of Indian agencies involved in SIGINT as well as the range of activities associated with the EMS limit its capacity to support the armed services, especially in wartime.[184] However, the PLASFF and its role in supporting TCs has demonstrated that, if joint operations are to be successfully and effectively conducted, a single integrated information warfare service like PLASFF is a necessity and must be paired with ITCs for the Indian armed forces.

One of the key challenges facing India is that its armed services still act in silos, notwithstanding recent advances made in theatrisation,[185] with each of the three services operating its own satellites and the IA set to get its own shortly.[186] Further, there is the absence of integrated and joint planning among the three armed services in the areas for space, counterspace, cyberspace, and EW operations and missions. The establishment of ITCs following considerable resistance, especially from the IAF, should render it easier to establish a command level and unified information warfare service.[187]

The Defence Cyber Agency (DCA), which is a tri-service organisation, could be expanded to perform functions such as direct combat support to the services and the ITCs. The latest move by the Indian government to establish the 'Command Cyber Operations and Support Wings (CCOSW)' is a long-overdue and necessary step to protect the communication and cyber missions for grey-zone and conventional military operations.[188] The CCOSW is primarily an IA agency, though it is unclear whether the CCOSW will only service the defensive security of the army's net-centric missions and not its offensive cyber capabilities. At this juncture, it is possible that the IA seeks to strengthen its defensive cyber capabilities before proceeding to develop the capacities for offensive cyber operations.[189]

Recommendations and Conclusion

Defensive cybersecurity is a necessity for all three services. Building cyber resilience, especially into the IA's networks, is key for India. While cyber resilience is indispensable to develop a network-centric force, it is nevertheless insufficient, and the ITCs will be crucial for conventional military missions.[190] With the status of the ITCs being legalised following new legislation by the Modi government,[191] greater synergy will likely crystallise for CW, EW, SW, and counterspace missions.

India also needs a Space Ground Integrated Information Network (SGIIN), which China is already developing. New Delhi needs to demonstrate greater urgency in acquiring a SGIIN capability. SGIIN will play a vital role in boosting the ISR capabilities of the Indian armed forces and will facilitate joint operations. In the event of a Sino-Indian military conflict, India is unlikely to be a beneficiary of generous support such as that extended by SpaceX in Ukraine. A network of small satellites (SmSats) is necessary for India, irrespective of the downsides of this capability.

Finally, investment in AI and its applications—similar to China's swarm drones—is a necessity for India. AI will significantly enhance China's informationised capabilities. Meanwhile, it remains a key weakness for India. India should also emulate China's WZ UAVs, which present a formidable capability and could be critical for India to hold its own in the face of growing Chinese strength in the domains of EW, CW, and across the EMS. The advantages of possessing UAVs that can perform both ISR and strike missions will go a long way in arresting the capability gap between the Indian and Chinese militaries.

Kartik Bommakanti *is Senior Fellow at ORF.*

The author thanks **Satish Tezaa** *for his research assistance.*

Endnotes

1 See especially Jon Batemans comments on why Russian cyber operations were "ineffective" in Jon Bateman, Nick Beecroft and Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare", Q&A Carnegie Endowment for International Peace, December 19, 2022, https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667

2 The PLASFF is a command entity that combines CW, EW and space capabilities. See when PLASSF was established. "The Inaugural meeting of the Rocket Force Strategic Support Force, the leading organization of the army, was held in Beijing", *People's Daily Online,* January 2, 2016, https://politics-people-com-cn.translate.goog/n1/2016/0102/c1024-28003584.html?_x_tr_sch=http&_x_tr_sl=zh-CN&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

3 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organisations and Capability", in Roy Kamphausen, David Lai, and Andrew Scobell, ed., *Beyond the Strait: PLA Mission Other Than Taiwan,* (Carlisle, PA: Strategic Studies Institute, 2009), pp. 259-261.

4 See for example, Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", Carnegie Endowment for International Peace, Washington D.C., December, 2022.

5 See Joshua T. White' comments on EW being superior in effectiveness than CW and the importance of investing in jamming and anti-technologies technologies, which are part of EW in Raj Shukla, Joshua T. White, Lauren Kahn and Ashley J. Tellis on the Russia-Ukraine War, *ThePrint,* December 7, 2022, https://www.youtube.com/watch?v=94YdTI9lFsc.

6 Bateman's comments on why Russian cyber operations were "ineffective".

7 This analysis is a good example of an excessive focus on cyber fires or attacks. Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications".

8 Jason Healey, "Preparing for Inevitable Cyber Surprise", *War On the Rocks,* January 12, 2022, https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/

9 William Courtney and Peter Wilson, "If Russia Invaded Ukraine", *The Hill,* 8 December, 2021, https://thehill.com/opinion/international/584805-expect-shock-and-awe-if-russia-invades-ukraine/?rl=1

10 Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", *International Security,* Vol. 46, No. 2, Fall 2021, pp. 51-90.

Endnotes

11 Lennart Maschmeyer and Nadiya Kostyuk, "There Is No Cyber 'Shock and Awe': Plausible Threats In the Ukrainian Conflict", *War On the Rocks,* February 8, 2022, https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/

12 Maschmeyer and Kostyuk, "There Is No Cyber 'Shock and Awe': Plausible Threats In the Ukrainian Conflict".

13 Chris Gordon, "Lack of Airpower in Ukraine Proves Value of Air Superiority, NATO Air Boss Says", *Air&Space Forces Magazine,* March 22, 2023, https://www.airandspaceforces.com/airpower-ukraine-air-superiority-hecker/, See Bateman comments in in Jon Bateman, Nick Beecroft and Gavin Wilde, "What the Russian Invasion Reveals About the Future of Cyber Warfare".

14 Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 3.

15 William Banks, "Cyberattacks and the Russian War in Ukraine: The Role of NATO and Risks of Escalation", *Georgetown Journal of International Affairs,* August 8, 2022, https://gjia.georgetown.edu/2022/08/08/cyberattacks-and-the-russian-war-in-ukraine-the-role-of-nato-and-risks-of-escalation%EF%BF%BC/

16 Julia Voo, "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict", *Evolving Cyber Operations and Capabilities,* James A. Lewis and Georgia Wood (eds.), Center for Strategic and International Studies, Washington D.C., May 2023, p. 16

17 Voo, "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict", p. 16

18 Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications".

19 Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications". More recent evidence suggests the same. See Mehul Srivastava, Felicia Schwartz and Demetri Sevastopulo, "China building cyber weapons to hijack satellites, says US leak", *Financial Times,* April 21, 2023, https://www.ft.com/content/881c941a-c46f-4a40-b8d8-9e5c8a6775ba, See also for an overview on how cyber attacks can be directed at ground nodes in Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", Space Dossier – 3, *UNIDIR,* p. 9, https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf

20 Srivastava et al., "China building cyber weapons to hijack satellites, says US leak".

Endnotes

21 The author thanks Dr. Manoj Joshi for this point.

22 Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 13.

23 Thomas Brewster, "Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them", *Forbes,* March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/?sh=13c05ef65a4c

24 Gordon Corera, "Inside a US military cyber team's defence of Ukraine", *BBC News,* 30 October, 2022, https://www.bbc.com/news/uk-63328398

25 Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 11.

26 Michael Sheetz, "About 150,000 people in Ukraine are using SpaceX's Starlink internet service daily, government official says", *CNBC,* May 2, 2022, https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html

27 Cited in Alexander Martin, "US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command", *skynews,* June 1, 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

28 Voo, "Lessons from Ukraine's Cyber Defense and Implications for Future Conflict", p. 16.

29 Kyle Alspach, "Russian hackers get the headlines. But China is the bigger threat to many US enterprises", *Protocol,* August 3, 2022, https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity

30 Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations", Working Paper, Carnegie Endowment for International Peace, Washington D.C., December 2022, p. 7, https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf

31 Keir Giles and Anthony Seaboyer, "Russian Special Forces and Intelligence Information Effects", Defence Research and Development Canada, Ontario, March 2019, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc340/p810875_A1b.pdf

32 Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations", p. 8

33 Grace B. Mueller et al., "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures", Center for Strategic and

Endnotes

International Studies, Washington D.C. July 2023, p. 8, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-07/230713_Mueller_CyberOps_RussiaUkraine.pdf?VersionId=BwNbsmkThLIPVpB0tctC59kwVpZ2aXeI

34 *2022 Annual Report to Congress: U.S.-China Economic and Security Review Commission,* Washington D.C., 2022, p. 438.

35 *2022 Annual Report to Congress: U.S.-China Economic and Security Review Commission*.

36 International Institute if Strategic Studies, "Chapter Ten: Military Cyber Capabilities", *The Military Balance,* 122:1, 2022, p. 508

37 International Institute if Strategic Studies, "Chapter Ten: Military Cyber Capabilities".

38 Boaz Atzili and Min Jung Kim, "Buffer zones and international rivalry: internal and external geographic separation mechanisms", *International Affairs,* Volume 99, Issue 2, March 2023, pp. 645-665.

39 FACT SHEET: United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology (Icet), January 31, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/

40 Jennifer McArdle and Michael Cheetham, "Indo-US cyber security cooperation", *Seminar,* Issue 655, 2014, https://www.india-seminar.com/2014/655/655_jennifer_&_cheetham.htm

41 Wars may have limited aims, but the commitment with which they are fought will need to be maximum which is well explained in Michael Howard, "When are wars decisive?", *Survival,* Vol. 41, no.1, Spring 1999, p. 127.

42 Manoj Joshi, "Eastern Ladakh, the Longer Perspective", Occasional Paper No. 319, Observer Research Foundation, 2021, p. 3, https://orfonline.org/wp-content/uploads/2021/06/ORF_OccasionalPaper_319_Ladakh.pdf

43 Sun Tzu, *The Art of War,* in *The Seven Military Classics,* translated with historical introductions and extensive commentary by Ralph D. Sawyer, (New York: Basic Books, 1993), p. 161

44 Amrita Jash, "Fight and Win Without Waging War: How China Fights Hybrid Warfare", *CLAWS Journal,* Winter, 2019, pp. 96-109.

45 For a chronology of events leading to the Galwan clash see Shishir Gupta, "What does the 2020 Galwan clash say about India and China?", *Hindustan Times,* June 16, 2022, https://www.hindustantimes.com/india-news/what-does-the-2020-galwan-clash-say-about-india-101655355460675.html

Endnotes

46 Probal Dasgupta, *Watershed 1967: India's Forgotten Victory Over China,* (New Delhi: Juggernaut, 2020).

47 Paul H.B. Godwin, "Changing Concepts of Doctrine, Strategy and Operations in the Peoples Liberations Army 1978-1987", *The China Quarterly,* No. 112, December 1987, p. 576.

48 Godwin, "Changing Concepts of Doctrine, Strategy and Operations in the Peoples Liberations Army 1978-1987".

49 Xi Jinping, "Hold High the Banner of Socialism with Chinese Characteristics and Strive for Unity to Build a Modern Socialist Country in All Respects", *Report to the 20th National Congress of the Communist Party of China,* 16 October, 2022, pp. 48-49, https://www.fmprc.gov.cn/eng/zxxx_662805/202210/t20221025_10791908.html.

50 Dong Wentao, "The Enlightenment of Epidemic Prevention and Control to Winning Local Wars of Informatization in the Future", *Guangming Daily*, April 19, 2020, https://tech.sina.cn/2020-04-19/detail-iirczymi7102494.d.html

51 Evan A. Feigenbaum and Charles Hooper (Q&A), "What the Chinese Army is Learning From Russia's Ukraine's War", Carnegie Endowment for International Peace, Washington D.C., July 21, 2022, https://carnegieendowment.org/2022/07/21/what-chinese-army-is-learning-from-russia-s-ukraine-war-pub-87552.

52 Feigenbaum and Hooper, "What the Chinese Army is Learning From Russia's Ukraine's War".

53 Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III and Mark Cozad, "People's Liberation Army Operational Concepts", Research Report. RAND Corporation, Santa Monica, California, p. 8, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf

54 Burke, et al., "People's Liberation Army Operational Concepts".

55 Jeffrey Engstrom, "Systems Confrontation and System Destruction Warfare: How the Peoples Liberation Army Seeks to Wage Modern Warfare", RAND Corporation, Santa Monica, California, 2018, p. 25

56 Shou cited in Burke, et al., "People's Liberation Army Operational Concepts".

57 Burke, et al., "People's Liberation Army Operational Concepts", pp. 8-13.

58 Burke, et al., "People's Liberation Army Operational Concepts", pp. 8-13.

59 *The Science of Military Strategy,* China Aerospace Studies Institute, (Montgomery: AL, 2013), pp. 50-52, See also Burke, et al., "People's Liberation Army Operational Concepts", pp. 8-13

Endnotes

60 Peng Guangqian, and Yao Youzhi, eds., The Science of Military Strategy, Beijing, China: People's Liberation Army Academy of Military Science Press, 2001.

61 *The Science of Military Strategy,* pp. 160-161.

62 *The Science of Military Strategy*.

63 Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 9-10

64 This point has been confirmed by some serving and former Indian Army officers with expertise in Signals Intelligence (SIGINT).

65 See how deception could play out in the form of OCO against an adversary see Erik Gartzke and Jon Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies,* 24, 2015, pp. pp. 48.

66 Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace".

67 Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace".

68 Austin Long, "A Cyber SIOP?: Operational Considerations for Strategic Offensive Cyber Planning", in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations,* by Herbert Lin and Amy Zegart (eds.), (Washington D.C.: Brookings Institution Press, 2018), pp. 105-133.

69 See Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", p. 9.

70 Catherine A. Theohary and John R. Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare", *Congressional Research Service,* Washington D.C. August 13, 2019, https://sgp.fas.org/crs/natsec/IF11292.pdf, Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", p. 9.

71 Although Long does not specifically use China and India as an example, but his point is valid and applies to how the Chinese might employ their capabilities. See Long, "A Cyber SIOP?: Operational Considerations for Strategic Offensive Cyber Planning", pp. 105-133.

72 Author interview with former senior general officer of IA.

73 Andreas Rupprecht and Gabriel Dominguez, "Chinese air force equips 16th Air Division with WZ-7 HALE UAVs", *Janes,* November 11, 2021, https://www.janes.com/defence-news/news-detail/chinese-air-force-equips-16th-air-division-with-wz-7-hale-uavs

74 This is confirmed to author by an Indian Army Officer.

Endnotes

75 Parth Satam, "Threat from China's WZ-7 Drones", *Defence Research and Studies (DRaS),* December 23, 2022, https://dras.in/threat-from-chinas-wz-7-drones/

76 Christian Shepherd et al., "China readies supersonic spy drone unit, leaked document says", *The Washington Post,* April 18, 2023, https://www.washingtonpost.com/world/2023/04/18/china-supersonic-drone-taiwan-leaks/

77 Shepherd et al., "China readies supersonic spy drone unit, leaked document says".

78 Curtis Lee, "Leaked US Intel Suggests First Chinese WZ-8 Drone Unit Established", *navalnews,* April 21, 2023, https://www.navalnews.com/naval-news/2023/04/leaked-us-intel-suggests-first-chinese-wz-8-drone-unit-established/

79 Shepherd et al., "China readies supersonic spy drone un it, leaked document says".

80 Shepherd et al., "China readies supersonic spy drone unit, leaked document says".

81 Cited in Shepherd et al., "China readies supersonic spy drone unit, leaked document says".

82 Cited in Shepherd et al., "China readies supersonic spy drone unit, leaked document says".

83 Theohary and Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare".

84 Theohary and Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare".

85 Theohary and Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare".

86 Srivastava et al., "China building cyber weapons to hijack satellites, says US leak". See also Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain: A Modem Wiper Rains Down on Europe", *SentinelLabs,* March 31, 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

87 Srivastava et al., "China building cyber weapons to hijack satellites, says US leak".

88 John Chen, Joe McReynolds, and Kieran Green, "The PLA Strategic Support: A "Joint" Force for Information Operations", in *The PLA Beyond Borders: Chinese Military Operations in Regional and Global Context,* ed. Joel Wuthnow, Arthur S. Ding, Philip Saunders, Andrew Scobell, and Andrew Yang, (Washington D.C.: National Defence University Press, 2021), p. 151.

89 Chen et al., "The PLA Strategic Support: A "Joint" Force for Information Operations".

90 Chen et al., "The PLA Strategic Support: A "Joint" Force for Information Operations", p. 168.

Endnotes

91 Chen et al., "The PLA Strategic Support: A "Joint" Force for Information Operations", p. 168.

92 Cited in John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", in *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*, 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. 491

93 See for example Anil Chopra, "Peoples Liberation Army Strategic Support Force – A Comprehensive Look", *Air Power Asia*, March 8, 2021, https://airpowerasia.com/2021/03/08/peoples-liberation-army-strategic-support-force-a-comprehensive-look/

94 Scott D. Applegate, "Cyber and Political Hackers – Use of irregular Forces in Cyberwarfare", *IEEE Security and Privacy Magazine*, 9 (5) September 2011, p. 19. More specifically see Nicholas Lyall, "China's Cyber Militias", *The Diplomat*, March 1, 2018, https://thediplomat.com/2018/03/chinas-cyber-militias/. Nigel Inkster, "China's Cyber Power", *Adelphi Series*, Volume 55, Issue 456, 2015, pp. 83-108.

95 The Ukrainian Army has at least one software developer embedded with each battalion. See David Ignatius, "How the algorithm tipped the balance in Ukraine", *The Washington Post*, December 19, 2023, https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

96 "Leaping-2017-Zhu Rihe": From the perspective of the Red Army brigade's actions to see the new changes in the army's system and organization after the reshaping of the exercise", *Xinhuanet*, September 7, 2017, https://www-xinhuanet-com.translate.goog//politics/2017-09/07/c_1121625327.htm?_x_tr_sch=http&_x_tr_sl=zh-CN&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

97 "Fierce confrontation in electromagnetic space: the strategic support force unveils the mystery", *CCTV.com*, May 17, 2018, http://military.cctv.com/2018/05/17/ARTIjjonCY3EwBqyLfOvJ1fn180517.shtml

98 "Chinese Tactics", ATP 7-100.3, August 2021, Headquarters, Department of the Army, Washington D.C. August, 2021, p. 2-12, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf

99 "Chinese Tactics".

100 "Chinese Tactics".

101 "Chinese Tactics".

102 "Chinese Tactics".

103 "Chinese Tactics".

104 "Chinese Tactics".

Endnotes

105 Ignatius, “How the algorithm tipped the balance in Ukraine”.

106 *China’s National Defence in the New Era,* The State Council Information Office of the People’s Republic of China, July 2019, Foreign Languages Press Co. Ltd. Beijing, China.

107 “The basic direction of quasi-network and electricity integration operations”, *PLA Daily,* December 13, 2022. See also, Amy J. Nelson, and Gerald L. Epstein, “The PLA Strategic Support Force and AI Innovation”, Tech Stream, Brookings, December 23, 2022, https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/

108 “The basic direction of quasi-network and electricity integration operations”, *PLA Daily,* December 13, 2022.

109 Elsa B. 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. This was also confirmed by an Indian Army officer.

110 Scott N. Romanuik and Tobias Burgers, “China’s Swarm of Smart Drones Have Enormous Military potential”, *TheDiplomat,* February 3, 2018, https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential/

111 This is confirmed by an Indian Army officer.

112 This is confirmed by an Indian Army officer.

113 “China Tests Spy Drones In Near Space ‘Death Zone’: Report”, *NDTV,* October 31, 2017, https://www.ndtv.com/world-news/china-tests-spy-drones-in-near-space-death-zone-report-1769303

114 “China Tests Spy Drones In Near Space ‘Death Zone’: Report”.

115 “China Tests Spy Drones In Near Space ‘Death Zone’: Report”.

116 “China Tests Spy Drones In Near Space ‘Death Zone’: Report”.

117 Colonel Mandeep Singh (Retd.), “The Coming Chinese Drone Swarm”, *Delhi Defence Review,* July 30, 2018, https://delhidefencereview.com/2018/07/30/the-coming-chinese-drone-swarm/

118 David Axe, “Russia’s Electronic-Warfare Troops Knocked Out 90 Percent of Ukraine’s Drones”, *Forbes,* December 24, 2022, https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=2a6a6615575c

Endnotes

119 Yun Bo. "Strong Army Forum: Adhere to the integration and development of mechanization, informationization and intelligence", *PLA Daily,* November 22, 2022, http://www.mod.gov.cn/gfbw/jmsd/4926673.html

120 Bo. "Strong Army Forum: Adhere to the integration and development of mechanization, informationization and intelligence".

121 Anthony S. Cordesman, "Chinese Strategy and Military Power in 2014", Center for Strategic and International Studies, Washington D.C., November 2014, p. 122.

122 Cordesman, "Chinese Strategy and Military Power in 2014".

123 Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", China Brief, Volume: 15 Issue: 8, The Jamestown Foundation, April 16, 2015.

124 This is an interesting analysis, but it would be wise for India's leaders to prepare for conventional escalation. Tobias Burgers and Scott N. Romanuik, "China's Real Takeaway From the War in Ukraine: Grey Zone Conflict is Best", *The Diplomat,* October 6, 2022, https://thediplomat.com/2022/10/chinas-real-takeaway-from-the-war-in-ukraine-grey-zone-conflict-is-best/

125 Karl R. DeRouen Jr., "The Indirect Link: Politics, the Economy, and the Use of Force", *Journal of Conflict Resolution,* 39 (3): pp. 671-95.

126 Jaroslav Tir, "Territorial Diversion: Diversionary Theory of War and Territorial Conflict", *The Journal of Politics,* Vol. 72, No. 2, 2010, pp. 413-425.

127 Adam S. Posen, "The End of China's Economic Miracle", *Foreign Affairs,* August 2, 2023, https://www.foreignaffairs.com/china/end-china-economic-miracle-beijing-washington

128 Posen, "The End of China's Economic Miracle".

129 "Satellite Navigation Services", Indian Space Research Organisation (ISRO), Bengaluru, https://www.isro.gov.in/SatelliteNavigationServices.html

130 Zhenhua Liu, Chuanwen Lin and Gang Chen, "Space Attack Technology Overview", *Journal of Physics: Conference Series,* 1544, 2020, p. 7.

131 Franz-Stefan Gady, "Revealed: China Tests Secret Missile Capable of Hitting US Satellites", *The Diplomat,* November 11, 2015, https://thediplomat.com/2015/11/revealed-china-tests-secret-missile-capable-of-hitting-us-satellites/

132 See decision time available for Matthew Mowthorpe, "Space resilience and the importance of multiple orbits", *The Space Review,* January 3, 2023, https://www.thespacereview.com/article/4504/1.

Endnotes

133 "China: EMP Threat: The Peoples Republic of China's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack", by Dr. Peter Vincent Pry, Executive Director, EMP Task Force on National and Homeland Security, Washington D.C., June 10, 2020, pp. 3-4, https://apps.dtic.mil/sti/pdfs/AD1102202.pdf

134 The costs would be significant for almost all states operating satellites at a minimum in LEO, see Robert "Tony" Vincent, "Getting Serious About The Detonations of High Altitude Nuclear Detonations", *War On The Rocks,* September 23, 2022, https://warontherocks.com/2022/09/getting-serious-about-the-threat-of-high-altitude-nuclear-detonations/

135 Zhao Meng, Da Xinyu, and Zhang Yapu, "Overview of Electromagnetic Pulse Weapons and Protection Techniques Against Them", Winged Missiles, PRC Air Force Engineering University: May 1, 2014.

136 Liu et al., "Space Attack Technology Overview", p. 7.

137 Liu et al., "Space Attack Technology Overview", p. 7.

138 "Chinese space technology capable of jamming satellites is 'on the march', top Pentagon official says", *South China Morning Post,* July 10, 2021, https://www.scmp.com/news/world/united-states-canada/article/3140634/chinese-space-technology-capable-jamming-satellites.

139 Chen Zongwei and Xu Yuhao, "Power in con-combat military operations", Guangming Military, August 23, 2022, https://www.secrss.com/articles/46133

140 Cited in Chen et al., "The PLA Strategic Support: A "Joint" Force for Information Operations", p. 171.

141 Elsa B. Kania and John Costello, "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power", *Journal of Strategic Studies,* Vol. 44, Issue 2: The People's Liberation Army in its Tenth Decade, Edited by James Char, p. 20

142 John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", China Strategic Perspectives, No. 13, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defence University Press, Washington D.C., 2018, pp. 37-38, https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/INSS_china-perspectives_13.pdf

143 Costello and McReynolds, "China's Strategic Support Force: A Force for a New Era".

144 Costello and McReynolds, "China's Strategic Support Force: A Force for a New Era.

145 Costello and McReynolds, "China's Strategic Support Force: A Force for a New Era.

Endnotes

146 Kania and Costello, "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power".

147 John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for New Era", China Strategic Perspectives, No. 13, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, (Washington D.C.: p. 15, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

148 Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 3.

149 Elsa B. Kania and John K. Costello, "The Strategic Support Force and the future of Chinese Information Operations", *Cyber Defense Review,* Spring, 2018, p. 109.

150 Kania and Costello, "The Strategic Support Force and the future of Chinese Information Operations".

151 Kania and Costello, "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power", p. 28.

152 Kania and Costello, "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power".

153 He Chao et al., "Research on Generalisation of Cyberspace Combat Command Training Platform", *Computer Science and Application,* Vol. 12, No. 4, April, 2022, https://www.hanspub.org/journal/PaperInformation.aspx?paperID=50684&btwaf=88878717

154 Chao et al., "Research on Generalisation of Cyberspace Combat Command Training Platform".

155 Chao et al., "Research on Generalisation of Cyberspace Combat Command Training Platform".

156 Chao et al., "Research on Generalisation of Cyberspace Combat Command Training Platform".

157 Col. Vinayak Bhat (Retd), "China's string of radars in Ladakh track every move of the Indian Army", *ThePrint,* August 25, 2017, https://theprint.in/opinion/chinas-string-radars-ladakh-track-every-move-indian-army/7976/

158 Bhat, "China's string of radars in Ladakh track every move of the Indian Army".

159 Bhat, "China's string of radars in Ladakh track every move of the Indian Army".

160 Bidisha Saha, "Making sense of Chinese advanced air surveillance radars near Indian border", *India Today,* April 19, 2023, https://www.indiatoday.in/india/story/making-sense-of-chinese-advanced-air-surveillance-radars-near-indian-border-2362084-2023-04-19

Endnotes

161 Nidhi Rastogi et al., "Explaining RADAR features for detecting spoofing attacks in Connected Autonomous Vehicles", p. 3, https://arxiv.org/pdf/2203.00150.pdf

162 Rastogi et al., "Explaining RADAR features for detecting spoofing attacks in Connected Autonomous Vehicles".

163 "The basic direction of quasi-network and electricity integration operations", *PLA Daily,* December 13, 2022, http://www.news.cn/mil/2022-12/13/c_1211709258.htm

164 Col. Vinayak Bhat (Retd.), "China's string of radars in Ladakh track every move of Indian Army", *ThePrint,* August 25, 2017, https://theprint.in/opinion/chinas-string-radars-ladakh-track-every-move-indian-army/7976/

165 Bhat (Retd.), "China's string of radars in Ladakh track every move of Indian Army".

166 Bhat (Retd.), "China's string of radars in Ladakh track every move of Indian Army".

167 Suyash Desai, "Assessing the Role of the PLA Southern Theater Command in a China-India Contingency", *China Brief,* Vol. 23, Issue:3, The Jamestown Foundation, February 17, 2023, https://jamestown.org/program/assessing-the-role-of-the-pla-southern-theater-command-in-a-china-india-contingency/

168 Desai, "Assessing the Role of the PLA Southern Theater Command in a China-India Contingency".

169 Ziyu Zhang, "China's military structure: what are the theatre commands and service branches?", *South China Morning Post,* August 15, 2021, https://www.scmp.com/news/china/military/article/3144921/chinas-military-structure-what-are-theatre-commands-and-service

170 Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences and Implications", p. 13

171 Both retired senior officer and serving officer made this point in an interview with the author.

172 Author interview with senior IA officer and serving officer.

173 Author interview with serving IA officer.

174 Author interview with serving IA officer.

175 I want to thank an expert for this point who requested anonymity.

176 The author thanks the Dr. Manoj Joshi and Dr. Rajeswari Pillai Rajagopalan for this point.

177 *2022 Annual Report to Congress: U.S.-China Economic and Security Review Commission,* pp. 438-441.

Endnotes

178 Although this piece does not say so, but it can be inferred. Mowthorpe, "Space resilience and the importance of multiple orbits".

179 Kania and Costello, "Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power", p. 29

180 See Charles Hooper comments in Evan A. Feigenbaum and Charles Hooper, "What the Chinese Army Is Learning From Russia's Ukraine War", Carnegie Endowment for International Peace, Washington D.C., July 21, 2022, https://carnegieendowment.org/2022/07/21/what-chinese-army-is-learning-from-russia-s-ukraine-war-pub-87552

181 Feigenbaum and Hooper, "What the Chinese Army Is Learning From Russia's Ukraine War".

182 Rajat Pandit, "Government sets stage for integrated military commands, introduces bill for inter-services organisations", *The Times of India,* March 16, 2023, https://timesofindia.indiatimes.com/india/government-sets-stage-for-integrated-military-commands-introduces-bill-for-inter-services-organisations/articleshow/98673712.cms?from=mdr

183 Lt. Colonel Poshuk Ahluwalia, "Limited Wars Under Conditions of Informationisation and Capability Development", *Pinnacle – The ARTRAC Journal,* Vol. 18, 2019, p. 59.

184 An expert reviewer of this paper requested anonymity made this point.

185 Author interview with retired General officer of Indian Army.

186 Author interview with retired General officer of Indian Army.

187 This point was made by both serving and retired IA officers to the author.

188 "Indian Army raising new units to counter China, Pak in cyber warfare: Report", *Hindustan Times,* April 27, 2023, https://www.hindustantimes.com/india-news/indian-army-raising-new-units-to-counter-china-pakistan-in-cyber-warfare-reports-101682581848934.html

189 A cyber expert did state to this author that without defensive cyber security for network defence, you cannot have capabilities geared for offensive missions. In many ways offence is built on strong defence.

190 This was underlined to the author by both serving and retired Indian Army officers to the author. See also "India moves ahead with creation of theatre commands for integrated war-fighting", *The Economic Times,* June 18, 2023, https://economictimes.indiatimes.com/news/defence/india-moves-ahead-with-creation-of-theatre-commands-for-integrated-war-fighting/articleshow/101078591.cms?from=mdr

191 "As theatre commands take shape, Lok Sabha clears Inter-Services Organisation Bill", *The Hindu,* August 4, 2023, https://www.thehindu.com/news/national/as-theatre-commands-take-shape-parliament-clears-inter-services-bill/article67157616.ece

Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page).

OBSERVER RESEARCH FOUNDATION

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