Bommakanti, Kartik

Book

India and cyber power : the imperative of offensive cyber operations

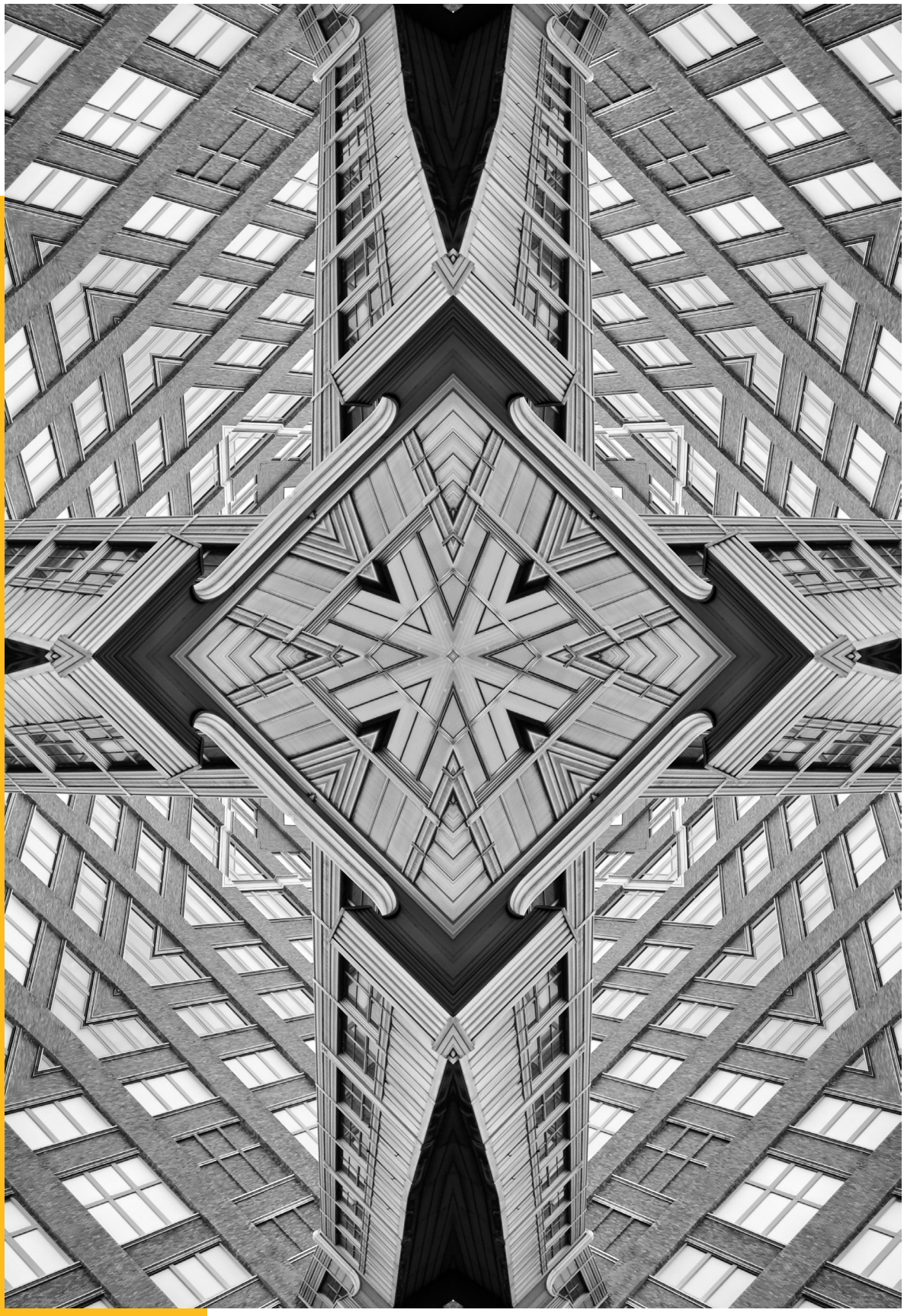
Provided in Cooperation with:
Observer Research Foundation (ORF), New Delhi

Reference: Bommakanti, Kartik (2022). India and cyber power : the imperative of offensive cyber operations. New Delhi, India : ORF, Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2022/11/ORF_OccasionalPaper_377_Cyber-Power.pdf.
https://www.orfonline.org/research/india-and-cyber-power/.

This Version is available at:
http://hdl.handle.net/11159/652718

OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 377 NOVEMBER 2022

India and Cyber Power: The Imperative of Offensive Cyber Operations

Kartik Bommakanti

Abstract

Defensive cyber operations are necessary to protect a network. At the same time,Offensive Cyber Operations (OCOs) cannot be neglected in military planning and should get as much attention as defensive cyber missions. Given the massive requirements for investment in cyber military capabilities geared for OCOs, this paper makes a case for the importance of OCOs for India. It outlines a roadmap for New Delhi to achieve effective OCO planning.

Attribution: Kartik Bommakanti, "India and Cyber Power: The Imperative of Offensive Cyber Operations," *ORF Occasional Paper No. 377*, November 2022, Observer Research Foundation.

Introduction

The question of whether India needs capabilities for Offensive Cyber Operations (OCOs) correlates two specific issues that the subsequent analysis seeks to address. The first involves determining whether cyber technologies should be employed for purely defensive ends or for both defensive *and* offensive objectives. This has implications for deterrence and escalation. Deterrence would require a combination of defensive and offensive cyber actions. Beyond deterrence and escalation, OCOs are equally necessary for effectively prosecuting kinetic operations in contemporary and future warfare. In the case of escalation, it can provide non-kinetic means of retaliation, though it has limitations.

A cyber-attack can also be carried out in conjunction with other instruments such as Electronic Warfare (EW) and space capabilities, as well as kinetic means in the form of air, naval, and land power. Indeed, as analysts have put it, action in cyberspace is an extension of warfare in the Electromagnetic Spectrum (EMS).[1] Action in the EMS in the form of EW dates back to the Second World War with the warring states working to jam each other's radar.[2] Depriving an adversary of the use of radio and radar by jamming would make them distrust their own technology. Contemporary OCOs are an evolution of Electronic Counter Measures (ECMs) and Electronic Counter-Counter Measures (ECCMs) subsumed under the broader rubric of EW. Cyber capabilities geared for offensive operations have a similar role.

More importantly, the debate about the efficacy of cyber power must necessarily involve analysing both offensive and defensive cyber capabilities. This is important because Indian policymakers and military practitioners need a clearer understanding of the relative strengths and weaknesses of cyber offence and, more generally, what cyber power can achieve. Cyber-attacks can be divided into two types: attacks that disrupt the effective operation of a weapons system, and another set that destroy or inflict damage on weapons systems.[3]

Introduction

Advocates of cyber offence, meanwhile, do not deny the importance of cyber defence, but make the case that states should not completely divest or give up cyber offensive capabilities. Some experts contend that in the cyber domain, offence and defence are not as neatly distinguishable: offence has no greater advantage than defence, or vice versa, as is the case with conventional deterrence. As these analysts contend, "Neither offence nor defence is dominant or inherently advantaged."[4] Rather the cyber domain lends itself to exploitation rather than coercion,[5] and requires persistence in the form of relentless initiative.[6]

It is critical to specify the conditions in which offence is either effective or ineffective in the cyber domain because of the nature of capabilities India must develop for offensive cyberspace operations. Cyber exploitation too, must be qualified, in terms of technical differences: exploitation is "non-destructive" and geared towards altering and stealing or exfiltrating information from an adversary computer or network and generally occur over a significant length of time; cyber-attacks, which are OCOs, are designed to destroy computer targets through cyberspace.[7] Nevertheless, both exploitation and attack do compromise data and can be viewed, at least according to some accounts, as variants of cyber offence.[8]

This present analysis will focus on the offensive applications of cyber capabilities, assessing their strengths and weaknesses. This will allow an alignment between expectations and reality through, and against cyber networks.[9] The most effective and high-impact offensive cyber operations are a mixture of "intelligence, operations and technical skill."[10] Intelligence assumes considerable importance and remains vital for the effective execution of OCOs. Without it, it will be impossible to gain knowledge about the characteristics and nature of target networks and tailor effective OCOs.

Two distinctions need to be made when evaluating OCOs: *event-based* and *presence-based operations*.[11] The latter encompass primarily strategic capabilities that involve protracted network intrusions of the

adversary and end with an offensive or attack.[12] The former cover tactical tools which are deployed in the course of ongoing operations on the field to generate localised impact.[13] (See Table 1)

Table 1: Presence-Based Vs. Event-Based Operations

	Presence-based operations	Event-based operations
Preparation	The cycle of targeting is long; involves establishing infrastructure. Characterised by agility, malware modularity, stealth, and geared to conducting research that exposes vulnerability.	Targeting cycle is short. Involves strong action marked by aggression. Must be deception-resistant. Involves using "intuitive tools" and geared to conducting research that exposes vulnerability.
Engagement	Initialisation of infection. Software, supply chain compromised remotely or via an insider. The process is protracted.	Software is compromised across devices. The payload is selected by the operator or automatically activates. The engagement is "quick or instantaneous".
Presence	Occurs over an extended period that can take years. Horizontal movement. Geared to supporting intelligence and support for Research and Development (R&D).	Presence in adversary network is minimal. Movement is automatic. There is a circumscribed presence or no persistence in enemy networks.
Effect	Involves a high-visibility attack producing a cascade. Alternatively, the effect can be slow and "clandestine".	The effects can be fleeting or durable on the targets.

Source: Daniel Moore, Offensive Cyber Operations: Understanding Intangible Warfare, (London: Hurst&Company, 2022)

Introduction

The first part of this analysis outlines the debate on the primacy of either cyber defence or cyber offence. The paper then looks at how cyber offence plays a role as a force multiplier for kinetic attacks and why they are unlikely to be adequate tools of escalation on their own. Although offensive uses of cyber capabilities have limited applicability and suffer from constraints, they can be effective if used selectively and appropriately in conjunction with other military instruments such as electronic warfare and kinetic attacks. The aim is to help Indian policymakers and military planners determine under what conditions cyber weapons should and *can* be used effectively. The paper closes with recommendations for building up India's OCO capabilities and underlines why there is an imperative to reform the current institutional and organisational structure of cyber command and control.

> "The debate about the efficacy of cyber power must involve analysing both offensive and defensive cyber capabilities."

Cyber Offence or Cyber Defence?

One school of thought on cyber power contends that it should not be used offensively because it is ineffective: cyber operations have limited psychological and coercive effect against adversaries.[14] As Ciaran Martin, founder of the UK's National Cyber Security Center observed: "[We] must be unambiguously in favour of safer technology… even if that sometimes makes deploying our own offensive cyber capabilities harder because a rising tide of security will, to some extent, lift all boats, including adversarial ones."[15] This implies that unilateral restraint can beget cyber restraint by adversaries. Further, cyber-attacks, according to Martin, could redound to the disadvantage of the attacker because cyber weapons such as viruses could infect the attacker's systems as much as it would the enemy's.[16]

Given the collateral damage cyber-attacks could cause, their deterrent value is at best modest. However, Martin does not explain why countries like North Korea and Russia—responsible for cyber-attacks such as WannaCry and Notpetya, respectively—do not suffer the effects of collateral damage or why cyber-attacks originating from these states never redound to their disadvantage. NotPetya, for instance, was a cyber-attack against Ukraine which affected not only the primary target but inadvertently, third parties, too.[17] Nevertheless, other experts concur with Martin's claims that in the cyber domain, the malware intended to destroy the primary target may end up affecting innocent systems.[18]

At best, Martin makes the case for offensive operations at the lower end of the cyber spectrum in cyberspace for very narrow objectives such as "hacking" to destroy propaganda by terrorist groups or disinformation.[19] The second use of offensive cyber power is "adversarial infrastructure destruction" against a hostile cyber group located in another country; the third use relates to "counter-

influencing" missions planting unhelpful information or "digital harassment". Cyber offense does not seek to disrupt, degrade and destroy.[20] The upper end of offensive cyber operations, which Martin opposes, include "kinetic" offensive operations that cause damage and disruption in the adversary country. Another use of cyber power is a comprehensive attack against the adversary's digital networks amidst a conflict.[21]

Other experts aver similarly that offensive cyber weapons cannot generate costs in terms of physical destruction the way kinetic or conventional weapons can, as the destructive effects of cyber warfare are highly circumscribed.[22] Martin is not unambiguously opposed to the offensive uses of cyber power, but believes the window and tools available under cyber capabilities are highly limited to actions such as disrupting and destroying websites operated by terrorist networks.[23] Most of his objections against offensive uses of cyber power are focused on large-scale OCOs, though there are more limited uses to OCOs at the tactical and operational levels of war, where OCOs might be effective and even more so when used in conjunction with other tools such as EW.

There is a second variant of the argument that offensive cyber warfare is problematic, and it goes further than the first as it explicitly prescribes that it be completely abandoned.[24] Pukhraj Singh, an adviser to the Indian government and armed services, recommends the pursuit of the "cult of the defensive".[25] While this may seem like an extreme view, there is generally a strong focus on cyber defence than offence in India. As C.K. Tyagi, a retired Indian Army (IA) Signals Corps officer put it: "Whenever we [Indians] discuss cyberwar, we talk only of cyber defence and protection of our CII [Critical Information infrastructure]…unless we build and maintain and offensive cyber force how will we as a nation retaliate to cyberattacks?"[26] Other IA officers from the Signal Corps share the view that while defensive cyber security is important, offensive cyber capabilities cannot be ignored.[27]

Cyber Offence or Cyber Defence?

They contend that defensive cyber security is more demanding than developing offensive cyber capabilities such as malware.[28] This is because defence is harder than offence in the cyber domain,[29] requiring a "…build up [of India's] offensive [cyber] capabilities".[30] This point may not sufficiently capture the extent of the effectiveness of offensive cyber missions or OCOs; after all, the efficacy of cyber offense does not always produce the destructive effects of a kinetic attack. However, that is the essence of *intangible warfare* as briefly noted earlier in this paper.

The *ease* of cyber-attacks, therefore, should not be confused with their *effectiveness*. On the other hand, as Gary Corn, an American expert put it in the context of Russia's cyber offensive: "It also underscores the strategic reality that threats of retaliation alone do not deter the nation's adversaries. Their malicious cyber campaigns are constant and unrelenting, and the U.S. cannot simply firewall its way out of this problem."[31] As mentioned earlier, the relative strengths between cyber defence and cyber offence are not fully settled. What is certain is that both have limits, and confining India to purely defensive cyber operations is likely to prove equally ineffective. Offensive capabilities are necessary, but have their own limitations. In a nutshell, as an expert observed to this author, in the cyberspace domain, "you cannot do offence without defence."[32]

At present, India's offensive cyber capabilities are weak.[33] New Delhi needs offensive cyber capabilities to deal with China and Pakistan.[34] There is consensus, at least among former and serving military practitioners with knowledge about India's cyber capabilities, that India requires more robust cyber warfare capabilities geared for offensive action.[35] To be sure, civilians such as National Security Advisor (NSA) Shiv Shankar under the previous United Progressive Alliance (UPA) government observed: "We have also seen technology create new domains for contestation, such as cyber space, where the speed of manoeuvre, premium on offense, and the nature of the battle-space make us rethink traditional concepts of deterrence. As

Cyber Offence or Cyber Defence?

technology has expanded the spectrum, the line between conventional and non-conventional warfare has blurred. The definition of force, the classic marker of power, has now expanded, thus changing the utility of force as traditionally configured."[36] Thus there has been recognition at the highest level of the civilian leadership that offensive uses of force is a regnant feature of cyberspace.

India faces significant challenges in cyberspace from both China and Pakistan, which could engage in cyber collusion against India.[37] Pakistan is likely to serve as a key Chinese proxy for cyber-attacks against India. The extent of that potential collusion is unclear, however. While India's capabilities vis-à-vis Pakistan remain reasonably robust,[38] they are weak, relative to China.[39] Beyond the specifically cyber-linked uses for offensive action, the integrated use of cyber and electronic warfare capabilities for offensive action requires closer evaluation.[40]

> "Former and serving military practitioners say India requires more robust cyber warfare capabilities geared for offense."

Cyber Offence: Insufficient Tool of Escalation on Its Own

Are cyber weapons adequate instruments of escalation? This question has received attention as escalation involves an intensification of conflict. In the cyber domain, responding to enemy action with counter-offensive operations, which would be escalatory, has limited efficacy. Escalatory responses that are specific to cyberspace are constrained by time.[41] There are limited windows to execute an attack in cyberspace and the damage visited upon any target is still limited compared to a kinetic attack.[42] Here, OCOs that are domain-specific or confined exclusively to the cyber domain may have limitations with regard to escalation and the degree to which they damage a target.

OCOs as escalatory mechanisms are not a panacea to rid war of its violent and destructive character; what they can do is aid the tactical and strategic efforts in wartime. They help shape the information environment in the battlefield and serve as a force multiplier by attacking enemy networks, which paves the way for a physical strike. Coordination between intelligence and military agencies responsible for executing OCOs is critical to their success. This qualification about OCOs especially in relation to escalation helps understand the limits of their applicability.

Cyber weapons are important offensive instruments in imposing countervailing costs against an opponent in the middle of a war or to pre-empt an opponent. For instance, India might want to take out the command network of the Western Theater Command (WTC) of China's People's Liberation Army (PLA) in the midst of active hostilities. The WTC controls certain cyber assets and its command network is dependent on computer software and hardware. The PLA considers the cyber domain tending to be "offense dominant".[43] At the minimum, the PLA sees OCOs as an integral element of warfighting. Take network warfare, the Chinese view and use non-governmental entities to execute OCOs in order to conceal their tracks and deceive

Cyber Offence: Insufficient Tool of Escalation on Its Own

the adversary about their identity and prevent attribution.[44] The Indian state and the service branches of the military do not see civilian hackers as a resource to tap for the conduct of OCOs.[45]

In the case of Pakistan, cross-domain responses may be necessary. Cyber need not counter cyber, but cyber could counter non-cyber. For instance, cyber-attacks could sometimes be indispensable against Pakistan-sponsored terrorism. An Indian foreign policy report, *Non-alignment 2.0*, recommended it in 2012: "At the lower end of the options spectrum is the employment of cyber and/or air power in a punitive mode. The use of air/cyber power has advantages over any land-based strategy: it could be swift, more precise, and certainly more amenable to being coordinated with our diplomatic efforts. Compared to any land-based options, the use of air/cyber power will come across as more restrained. To be sure, such action could invite retaliatory response from Pakistan. It is essential, therefore, that our coercive strategy not only caters for offensive use of air/cyber power but also for a defensive role."[46]

This prescription may have some merit, but it fails to account for an important tenet of OCOs – time and intelligence. Without these two key elements, it is difficult to see how India could successfully execute an OCO against Pakistan, let alone China. As discussed earlier, cyber weapons are not always readily available instruments of escalation. They are not the same as carrying out an air strike on the order of apex decision-makers as the Indian Air Force (IAF) did with the Balakot air attack in 2019 in response to Pakistan's terrorist outrage in Pulwama. The employment of offensive airpower is more readily available on short notice as it was against the Jaish-e-Mohammad terrorist training camp at Balakot by the IAF as opposed to an OCO against Pakistani and Chinese military networks, installations, command posts, power grids supplying electricity to Chinese and Pakistani installations, and weapons systems. However, contrary to the prescription of the Non-alignment 2.0 report, India needs the combined application of cyber

and air power for offensive action to be lethally effective, rather than a purely or dichotomous "air/cyber power" application.

Further, penetrating the cyber networks of Chinese and Pakistani critical infrastructure, command systems, military installations and weapons platforms may require a well-planned and coordinated *presence-based* operation. The latter operation can only take place over a significant amount of time, requiring cyber offensive instruments to be placed behind enemy lines on enemy servers and infecting specific nodes of the adversary's network, and it also necessitates that presence-based OCO remain undetected.[47] This requires pre-positioning the cyber weapons payload well in advance before its actual use, but when triggered the cyber payload has to strike the target as intended.[48] This may simply not happen if one part fails to trigger at the right time, which could render the OCO a failure.[49] There could also be an extraneous variable which the attacker cannot control.[50]

Perhaps the most visible and successful example of a presence-based operation was the *Stuxnet* virus that started infecting centrifuges at Iran's Natanz nuclear facility in 2008, discovered only two years later in 2010.[51] The damage to the centrifuges was real and significant. In other instances too, presence-based operations have caused considerable damage, such as the Idaho National Laboratory's 'Aurora Experiment' that demonstrated how generators can suffer significant physical damage due to a software vulnerability.[52] Otherwise, the effects of OCOs are not easily verifiable and the damage they cause may be more limited, which means that it is equally indispensable to develop post-attack cyber Battle Damage Assessment (BDA) capabilities.[53]

For their part, event-based attacks (see Table 1) require being close to the target and they lend themselves to quicker decision-making. This would require a response by military units located close to the enemy—whether China or Pakistan. However, those IA units located

in close proximity to Chinese and Pakistani military targets have to be capable of conducting CW or OCOs that can use a pre-packaged capability. Successfully mapping signals and local networks operated by the enemy could enable an event-based attack.[54] The targets may be assets located near border areas such as radar installations and anti-aircraft batteries reliant on computerised fire control systems. However, as noted earlier, the damage through exclusively cyber means in the form of an event-based attack may be limited or even temporary.

Beyond the role of defence and offence exclusively in the cyber domain and how defensive action and offensive action correlate closely to denial and punishment, it is important to consider how cyber power might merge other military instruments covering electronic warfare and space military power, especially in the context of conventional military operations. OCOs and the nature of cyberspace tends to intersect with other domains. Viewing them in domain-specific terms clouds the possibility of the OCOs being carried through an intersection with other areas of warfare. Indeed, the arguments in favour of cyber defence—whether in their minimalist or maximalist conceptions—are even less valid, particularly at the operational and tactical level of conventional conflict and operations. If anything, when cyber operations are combined with conventional operations in the form of a kinetic attack and other military means such as electronic warfare and space-borne capabilities, it will expose the limits of pursuing a cyber strategy based on the "cult of the defensive". This is where we turn to the historically deep connection between Signals Intelligence (SIGINT) and electronic warfare and contemporary OCOs.

Cyber Operations with Electronic and Kinetic Attack

There are specific areas where offensive action through cyber means as well as when used in conjunction or as complement will impact conventional military operations. Contemporary OCOs are the domain of SIGINT units of all militaries. Cyber operations, specifically OCOs, can serve as key force multiplier during conventional operations and more limited tactical action and contingencies, when merged with the IA's SIGINT units and also with the capabilities of the other two services, namely the Indian Air Force (IAF) and the Indian Navy (IAF) SIGINT. As noted earlier, OCOs are fundamentally an evolutionary aspect of *intangible warfare,* which covers EW and operations across the EMS. The quest to maintain battlefield supremacy means militaries around the world, especially those facing India such as China, have invested heavily and are increasingly strengthening their offensive cyber warfare capabilities.[55] Consider the role of cyber-attacks against Integrated Air Defence Systems (IADS). Ground-based Air Defence Systems (GBADS) are also vulnerable to cyber-attacks.

All IADS and GBADS, including several Indian ones, are connected to computers. Some examples are the Command and Control (C&C) Israeli Spyder Air Defence System (ADS)-Short Range (SR) and the Medium Range (MR) operated by the Indian Air Force (IAF) or the Akash ADS, also operated by the IAF and the Indian Army (IA) including the latest New Generation (NG) version of the ADS. The Indian armed services are most likely reliant on standard-issue radios, satellite communications, and civilian or dual-use telecommunications.[56] All these means of communication are vulnerable to hostile cyber penetration, especially by the PLA Strategic Support Force (PLASSF) and PLA Army (PLAA) deployed under the WTC. Conversely, the digitisation and computerisation of the PLA Joint Logistics Support Force (PLAJLSF) as well as the logistics units that are organic to the PLAA[57] in the Tibetan Autonomous Region (TAR) create target-rich opportunities for the conduct of OCOs by India.

Cyber Operations with Electronic and Kinetic Attack

Conversely, as mentioned earlier, preparing the ground for a cyber-attack is facilitated by prior espionage by the attacking entity or state. This was demonstrated by the Chinese RedEcho group's espionage and information collection from the electricity grid comprising State Load Dispatch Centers (SLDCs) along the Sino-Indian border in March and April 2022.[58] Although cyber espionage is not a cyber-attack or OCO, it helps prepare the ground for one. RedEcho's intelligence collection was in all probability directed at determining the nature of the cyber network supporting the electricity supply in Uttarakhand and Ladakh. The target of that cyber espionage were power facilities, which likely supply electricity to command centers of the IA along the Line of Actual Control (LAC) in Ladakh. This was likely a *presence-based* operation that is part of a protracted intelligence effort consisting of limited attacks that stretched over several months.

More such efforts may yet come. All this cyber intelligence effort could bear fruit in the event of a Sino-Indian war in the form of disabling OCOs by the PLASSF and organic cyber-attack units embedded with forward deployed forces of the PLAA and the WTC against the IA's command nodes. These will render their response incoherent and uncoordinated and thereby prepare the ground for China's physical or kinetic assaults against the IA's mobile and static targets. Chinese hackers' cyber effort was likely to map and collect information on the key characteristics of the cyber or computerised network on which the SLDCs are dependent. Even the cyber-attack by the RedEcho group, which the Indian government claimed it thwarted, was likely a limited probe meant to test the response and defensive security of India's cyber network geared to protecting critical infrastructure.[59]

The PLAJSF is striving for precision logistics reliant significantly on China's BeiDou Satellite Navigation (SatNav) System.[60] The JLSF is also developing a cloud platform, several databases, and a variety of networks for the pursuit of timely, expeditious and efficient logistics.[61] When fully activated, this is expected to give the Command

and Control (C2) of the JLSF logistics systems a common operating picture in battle.[62] Even if the JLSF is not as active in the TAR, which falls under the WTC, all logistics units operated by the PLAA whether by rail or road connected to depots, maintenance needs of vehicles transporting weapons and supplies, to forward deployed units along the LAC and fuel loads for vehicles performing a variety of logistics missions would rely on an extensive digitised network. This creates opportunities for the conduct of OCOs, especially in the event of battle.

As a consequence, penetration of communication and C2 networks using malware can disrupt the effective operation of logistics nodes, IADS, and GBADS. The attack could be executed in the form a Radio Frequency (RF), which is primarily an electronic action merging cyber and electronic warfare operations.[63] The US, for instance, has used exclusively cyber means to disable Iranian rocket and missile systems, which was executed by the US Cyber Command (USCYBERCOM) in 2019.[64] It took USCYBERCOM weeks of planning before the disabling attack against Iranian missile forces could be executed.[65]

However, it should also serve as a cautionary reminder to Indian military planners that *Non-alignment 2.0's* prescription for resorting to a successful cyber-attack without significant prior planning is at the least, extremely difficult. Cyber weapons are a product of an iterative process that involves rigorous testing of false positives.[66] The only qualifying factor is if India builds a large reserve of cyber warfare capabilities or lethal malware as the Russians, as one expert averred, even now potentially or very likely possesses, notwithstanding the setbacks the Russian military has suffered in Ukraine. The only qualifying factor would be Russia's unwillingness to use its OCO capabilities at the current juncture in its ongoing confrontation with Ukraine and the West more generally.[67]

India too, may have to develop a large reserve of OCO capabilities, which it might not employ against either Pakistan or China, because it might not be effective especially following a terrorist attack sponsored by the Pakistani Army. This is because Pakistan is likely to be more

alert to an Indian cyber response, negating its effectiveness. On the other hand, it could be done if enemy networks, whether Pakistan's or China's, have been penetrated by Indian hackers without being detected and have a readily available payload to deliver an attack against the target. It would only take a mere software patch by China or Pakistan for any Indian cyber-attack against a Pakistani weapons system, command node, or the computer network of a Chinese or Pakistani military installation to neutralise the Indian cyber-attack or make the cyber weapon used in the OCO to behave in unintended ways.

Malware could be inserted into the computer networks and C2 systems of the IADS and GBADS in a quest to Suppress Enemy Air Defence (SEAD). The US Air Force's (USAF) EC-130 Compass Call electronic attack plane has merged the capability of delivering both electronic and cyber-attacks.[68] EC-130 is an airborne platform that represents the intersection between what the American military calls Cyber Electromagnetic Activities (CEMA) and which is capable of delivering electronic and cyber-attacks. The USAF also operates RC-135 V/W Rivet Joint reconnaissance aircraft that are capable of geolocating signals and passing on reconnaissance intelligence for the execution of a cyber-attack.[69] The purpose of the EC-130 is to use the intelligence supplied by the RC-135 V/W Rivet Joint aircraft to deliver attack. The Compass Call system exploits the overlapping conditions created by the fusion between electronic and cyber domains. As a US Congressional Research Service (CRS) 2019 report explained: "The EC-130H Compass Call is normally used to jam enemy radars and communications. However, in recent years it has been used to transmit computer code [cyber-attack] to wireless devices using radio frequencies".[70] The Americans used the *Suter* network to deliver cyber-attacks against Ground Based Air Defence System (GBADS) and Integrated Air Defence System (IADS).[71]

The imperative to employ cyber-attacks for offensive counter air-attacks is gaining traction with other countries as well, such as the United Kingdom (UK).[72] The British Army (BA) is attempting to revive its Landseeker programme that is capable of executing

electronic support, but it is deficient in electronic attack. The BA also lacks CW capability, which it deems necessary, notwithstanding budgetary issues, if cyber operations are going to be pursued at the tactical and operational levels on the battlefield.[73]

The Indian Army, for its part, has its Samyukta integrated mobile electronic warfare capability. This EW system is one of the largest of its kind built as part of a joint venture between the Indian Army and the Defence Research Development Organisation (DRDO). It is capable of performing, at least according to the DRDO, electronic attack functions such as jamming and keyed for specifically tactical missions.[74] However, the Samyukta EW capability is not known to possess a CW capability.[75] Blending the complementarities between CW and EW into a single land-based mobile unit is a key requirement which India currently lacks.[76]

The Israelis, meanwhile, in September 2007 carried out a cyber-attack against surveillance radar, enabling fighter aircraft to destroy targets that were given coordinates against the Syrian nuclear site at Al-kibar. Although there is a considerable part of the Israeli attack that is shrouded in secrecy, there is consensus among cyber experts that the Israelis completed a successful cyber-attack from an airborne platform.[77] The Israeli cyber-attack provided misleading or false information regarding radar tracks of approaching Israeli aircraft and was performed parallel to an Israeli electronic and kinetic attack.[78] India must develop and acquire airborne capabilities for the delivery of cyber-attacks, which would tie into the imperative that was expressed by several cyber military experts this author engaged with for this paper.[79]

There are also ground-based systems or vehicle-mounted capabilities that combine EW and CW. For instance, the British Army's Landseeker acquisition is geared to combining EW and CW capabilities into an armoured vehicle such as potentially the BA's Boxer armoured vehicle or the US Army's TLS armoured vehicle.[80] CEMA is integral

to American and British efforts to maintain supremacy in the electromagnetic and cyber domains.[81]

At the tactical level of war where operations are underway in different domains, events unfold rapidly and are dynamic, necessitating offensive action though the cyber medium. Yet, there are limits to speedy offensive action in the cyber domain in all instances. Cyber weapons or cyber-attacks need to be well-tailored to take out a network for SEAD. Even in cases where electronic attack serves as a vector for a cyber-attack—as was the case with the Israeli attack against a Syrian ground-based air surveillance radar at Tell Ayab in Northern Syria—Israeli Special Operations Forces (SOFs) or Syrian deep-cover agents may have implanted malware or passed on sufficient information of the characteristics of the software on which the radar was dependent that enabled the cyber-attack.[82] The Israelis are believed to have used a kill switch to disable the radar, blinding the Syrians to the approaching Israeli aircraft that struck the nuclear facility at Al Kibar.[83] This empirical data is crucial for Indian military planners to make the decision to develop and invest in these capabilities. Specific Chinese and Pakistani military targets, whether static or mobile, may need to be subject to destruction using a blend of EW and CW capabilities.

Thus, cyber means might not always be effective although there will be massive pressure to pursue offensive cyber action because of the need to execute an attack with speed and stealth or secrecy, which are the constituent elements of surprise.[84] This is simply because the target network could be insulated from an instantaneous cyber-attack. This is where prior information or cyber espionage or intelligence is vital to understanding the characteristics of a target network, which enables code to be designed to destroy. If the cyber weapon is well-designed and remains undetected by the defender, follow-on attacks can exploit surprise. However, even a software patch, or an update in software and hardware within the target could render the attacking malware useless and make it behave in unintended ways or render the malware ineffective in destroying the target.[85] Consequently,

Cyber Operations with Electronic and Kinetic Attack

cyber-attacks are time-sensitive: they are effective when planned well in advance, but likely to be less effective "when reacting to a crisis where lead times are truncated."[86]

This point would also qualify what *Non-alignment 2.0* recommended: that cyber power be employed against India's adversaries, especially Pakistan, particularly in a crisis triggered by a Pakistani attack against India. However, as noted, reaction or response time is likely to constrain an effective cyber riposte, contrary to what 'Non-alignment 2.0' proposed. Unless, India already has a presence in Pakistani or Chinese cyber military networks or computer systems linked to their ground-based surveillance radars and IADS, developed a cyber code that can blind their radars, which have gone undetected by the Pakistanis or the Chinese enabling India to take them by surprise. When cyber power is used in conjunction with other instruments, military power can be "synergistic."[87]

In other instances, even if India successfully targets the electricity grid of Pakistan's Punjab province, for example, it would need significant prior knowledge of the computer network on which the grid is dependent. For Indian cyber military planners, the prime targets should be power grids supplying energy to vital C2 installations of the Pakistan Army and critical for the successful conduct of OCOs. Pakistan may not be as formidable a cyber challenge as China is for Indian military planners.[88] However, a key factor compounding India's cyber military challenge is the potential collusion in the cyber realm between China and Pakistan, which remains indeterminate.[89]

Cyber, Electronic and Space Power: Limits of Defensive Cyber Warfare

Cyber power intersects with space technology in crucial ways. Cyber warfare and electronic warfare can both be used for counterspace missions to disrupt the performance of orbiting spacecraft.[90] There exists a fair amount of evidence to indicate how a cyber-attack could be launched against space assets and their ground segment. There are three specific elements in a space network that are vulnerable to a cyber-attack**:** uplink, downlink, and satellite-to-satellite attacks. Cyber-attacks can disrupt uplink communications between their ground control segments and in-orbit satellites; in downlink, communications between satellite-derived internet service can experience denial of service to the extent that hackers could intercept and disrupt internet service from telecommunications satellites and jam and spoof signals from Global Positioning Satellite (GPS) systems.[91] Data can also be corrupted from satellite downlinks to ground stations and terminals used by the military.

Cyber means can also be used in a satellite-to-satellite attack. The attack could be directed against satellite sensors and subsystems while the attacking satellite is in close proximity or in Line of Sight (LoS) of the target satellite.[92] There are no real or specific examples so far in the latter case, but it is a plausible scenario that some analysts have examined and deemed likely to see development and use by major spacefaring countries in the coming decade.[93] Although military satellites are hardened and use encrypted communications that insulate them from a cyber-attack, they remain vulnerable.

Russia, for example, has combined electronic and cyber warfare to target the North Atlantic Treaty Organisation's (NATO) satellite capabilities.[94] It has also hacked mobile phones of Lithuanian soldiers during maritime exercises and personal devices of soldiers in the Baltics. NATO military capabilities are critically dependent on space-borne assets, enabling Russia to jam satellite communications. Some Western analyses consider that there is a "crossover" between the cyberspace and space, which means that offence is easier than

defence.[95] Irrespective of current operational challenges facing Russia in Ukraine, the Russians have demonstrated that OCOs are integral to military strategy. This foregoing analysis underlines that a premium on defensive cyber measures has its limits.

China has already established a unified service in the form of the PLASSF, which has integrated electronic, cyber and space warfare capabilities. It has been highly effective at creating capabilities that leverage technologies in the EW, cyber and space domains, which will be employed for offensive military missions across the EMS.

> “Some Western analysts consider that there is a “crossover” between the cyberspace and outer space, which means that offence is easier than defence.”

1. ***Traffic Analysis and Private Networks*:** The Indian armed services, especially the Indian Army (IA) will need to invest in and develop the service's traffic analysis capabilities. Traffic Analysis is crucial to understanding and assessing movement of data and communication through networks. Traffic analysis, also known as Network Traffic Analysis (NTA), is the process by which the communication patterns of data are detected, intercepted, recorded and analysed to identify threats and respond to them. Attacks against networks could manifest themselves in a variety of ways such as penetrating fibre optic cables and securing information of plain text from the cipher text. There are additional of types attacks: *eavesdropping*, which involves clandestine listening; *spoofing* which disguises itself as the more privileged and trusted source than the actual process and user;[96] *data relay*, or the interception of data that the attacker can use later; and *service denial*, or denying the user or entity a service or resource they expect to use. It also prevents access to files and erasing data from a computer network.[97]

The IA's NTA capabilities are weak and will need strengthening.[98] In the case of private networks, access to which is restricted only to a handful of users and encrypted, the Indian military, especially with the IA's adoption of 5G technology, will need four core areas of application to meet mission requirements: 1) those that involve battlefield Command and Control (C2); 2) those that involve military training exercises; 3) those involving logistic support missions; and 4) applications for running and supporting military equipment and operating weapons systems.[99] Each of these mission areas will have different transmission and communication requirements. The performance and architecture requirements using 5G technology will also vary for each mission area and specific private or encrypted networks will need to be developed for them using 5G technology. 5G has already proved its strength and represents a significant shift from 4G as it provides low latency, high speed, and dense communication rates.[100] With or without 5G, the IA's private networks remain weak and will need to be strengthened.[101]

2. ***Trained Personnel:*** The Indian military does not possess a sufficient number of well-trained personnel for the conduct of OCOs.[102] Recruiting hackers from the civilian domain is a necessity, albeit not without its own implications.[103] If the armed services, especially the IA were to recruit from the civilian sphere, these hackers must imbibe some of the military demands for undertaking a specific objective and mission. The advantage of having civilian hackers is their technical proficiency. They also give the Indian state cover in the form of deniability and anonymity. They can prepare and launch OCOs based on the IA's operational requirements and develop malicious code or malware. The challenges and demands of penetrating the encrypted networks of adversaries, such as the Chinese military's C2 networks, weapons systems, and logistics support systems, should serve as motivation to young Indian hackers in the civilian sector. The Military College of Telecommunications Engineering (MCTE) based in Mhow, in concert with the Corps of Signal (CoS), can be the lead entities in identifying young technical experts whose skills can be used for specific OCO-related tasks and missions.

3. ***Organisational Integration of Technical Agencies:*** Although some organisational changes have been made by the current government, there are no task forces focused on the conduct of OCOs.[104] Further, there are a number of agencies that deal with cyber security issues under the central government. These include the National Technical Reconnaissance Organisation (NTRO), Defence Cyber Agency (DCA), which is a tri-service organisation, Defence Intelligence Agency (DIA), Defence Information Assurance and Research Agency, which is now merged with the DCA, and the Defence Space Research Agency (DSRA). There are too many silos and turf battles between the three services, which entities such as the DCA do not have the authority to overcome. The DCA, which falls under the Integrated Defence Staff (IDS), cannot pursue integrated OCO-related missions if there are too many organisations. To be sure,

the DCA has the capability to hack into networks, execute cyber surveillance missions, set up cyber honey pots, recover deleted data, and penetrate encrypted communication channels.[105] From all available evidence, the DCA is primarily a tri-service agency geared to extending training support and technical advice to each individual service. It does not, however, wield any independent command authority. Nor does it perform the same functions as USCYBERCOM, whose mission role is defined as: "Direct, Synchronise, and Coordinate Cyberspace Planning and Operations…"[106] Thus, all the agencies listed above will need to be consolidated under a single unified service and command organisation comparable to USCYBERCOM or the PLASSF. Given the extent to which space, EW and CW overlap across the EMS—and the foregoing analysis revealed the complementarities between them—a single organisation that prevents stove-piping will help. Although service-specific cyber capabilities exist, an integrated and unified organisation will allow better coordination and execution of OCOs. Tactical units, right down to the IA's battalion, will need to be supported by a single organisation that combines all the functions of the Indian agencies listed above. There could and *should* be centralised directives and support and decentralised execution by lower echelon units.

4. ***Leveraging India's IT and Software Ecosystem:*** India has substantial strength in the field of computer software and Information Technology (IT), but its reservoir of human and technical capital in this sector remains untapped. It is concentrated heavily in the private and civilian sector. Since India's OCO capabilities are generally weak vis-à-vis China, and at best moderately strong against Pakistan, leveraging the private sector expertise is an imperative.

Conclusion

Militaries across the world place a premium on initiative and offensive élan, making it highly debatable and unlikely that the armed services of any global power including India will concede a cyber strategy predicated on a "cult of the defensive". Nevertheless, the Indian armed services, especially the Air Force and the Army, will need to recognise the limits of offensive action when reacting to crises.

Well-planned cyber-attacks in conjunction with electronic attack and kinetic attack, as Israel and America have demonstrated against enemy air defences, require attention and focused investment. Given the growing fusion between electronic, cyber and space technology that are applicable to military operations, investment in these capabilities will need high priority. Thus, developing capabilities as part of a strategy where cyber power plays a central role whether against Pakistan or China is well worth pursuing.ORF

Kartik Bommakanti *is a Senior Fellow with ORF's Strategic Studies Programme.*

Endnotes

1 Daniel Moore, *Offensive Cyber Operations: Intangible Warfare,* (London: Hurst&Company, 2022), pp .1-35

2 Robert Cockburn, "The Radio War", *IEE Proceedings A,* Volume 32, Issue 6, October 1985, pp. 423-434.

3 Withington, "Killer Code: Cyber-Supported SEAD".

4 Michael P. Fischerkeller, Emily O. Goldman and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace,* (New York: Oxford University Press, 2022), p. 25.

5 Fischerkeller, Goldman and Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, p. 26

6 Fischerkeller, Goldman and Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*.

7 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy,* 4. No. 63, 2010, p. 64.

8 Lin, "Offensive Cyber Operations and the Use of Force".

9 Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* (London: Hurst&Company, 2022), p. 9

10 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* p. 19

11 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* p. vii.

12 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*.

13 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*.

14 Inaugural Lecture Ciaran Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age", King's College London, London, United Kingdom, November 20, 2020 https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf

15 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age".

16 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age"; For more on collateral damage caused by cyber-attacks see Lennart Maschmayer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", *International Security,* Vol. 46, No. 2, Fall 2021, pp. 63-64.

Endnotes

17 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare*.

18 Jacob G. Oakley, *Waging Cyber War: Technical Challenges and Operational Constraints*, (Delaware: Apress, 2019), p. 99.

19 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age", p. 7.

20 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age".

21 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age".

22 Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation", *Strategic Studies Quarterly,* Fall, 2019, pp. 122-145

23 Martin, "Cyber Weapons are called a viruses for a reason: Statecraft and security in the digital age".

24 Pukhraj Singh, "The SolarWinds hack pokes holes in Defend Forward", Observer Research Foundation, May 8, 2021, https://www.orfonline.org/expert-speak/the-solarwinds-hack-pokes-holes-in-defend-forward/

25 Singh, "The SolarWinds hack pokes holes in Defend Forward".

26 Sanjeev Relia, *Cyber Warfare: Its Implications on National Security,* (New Delhi: Vij Books India Pvt. Ltd. 2015), p. 218.

27 C.K. Tyagi, *Understanding Cyber Warfare and Its Implications For Indian Armed Forces*, (New Delhi, Vij Books India Pvt. Ltd, 2013), p. 254.

28 Tyagi, *Understanding Cyber Warfare and Its Implications For Indian Armed Forces*.

29 Tyagi, *Understanding Cyber Warfare and Its Implications For Indian Armed Forces*.

30 Tyagi, *Understanding Cyber Warfare and Its Implications For Indian Armed Forces,* p. 290.

31 Gary Corn, "SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse", *Lawfare,* January 14, 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse

32 Author interaction with cyber expert.

33 This point was made by Indian Army officers serving and retired in interviews conducted by the author.

Endnotes

34 Author interview with serving and retired Indian Army officers.

35 This point includes retired and serving officers that the author interviewed.

36 See speech by NSA Shri Shivshankar Menon at NDC, "The Role of Force in Strategic Affairs", Ministry of External Affairs, New Delhi, October 21, 2010, https://www.mea.gov.in/Speeches- Statements.htm?dtl/798/Speech+by+NSA+Shri+Shivshankar+Menon+at+NDC+on+The+Role+of+Force+in+Strategic+Affairs

37 Aditya Bhan and Sameer Patil, "Cyber Attacks: Pakistan Emerges as China's Proxy", *Money Control,* 11 February, 2022, https://www.moneycontrol.com/news/opinion/cyber-attacks-pakistan-emerges-as-chinas-proxy-against-india-8081491.html

38 This was confirmed by both retired and serving IA officers.

39 Author interviews with serving and former IA officers.

40 This point was well established in author interviews with serving and retired officers of the IA.

41 Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation", *Strategic Studies Quarterly,* Fall 2019, pp. 123-124.

42 Borghard and Lonergan, "Cyber Operations as Imperfect Tools of Escalation".

43 Elsa B. Kania and John Costello, "Seizing the commanding heights: the PLA Strategic Support Force in PLA military power", *Journal of Strategic Studies,* Vol. 44, Issue 2, 2021, p. 28.

44 Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", *China Brief,* 15, No. 8, 17 April, 2015, pp. 3-7.

45 Interview with former Indian Army Signals Corps Officer.

46 Sunil Khilnani, Rajiv Kumar, Pratap Bhanu Mehta et al., *Non-alignment 2.0: A Foreign and Strategic Policy For India in the Twenty First Century,* New Delhi, 2012, p. 40, https://cprindia.org/research/reports/nonalignment-20-foreign-and-strategic-policy-india-twenty-first-century

47 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* pp. 94-95

48 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* pp. 94-95

49 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* pp. 94-95

50 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* pp. 94-95

Endnotes

51 Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon,* (New York: Crown, 2011).

52 Curtis Waltman, "Aurora: Homeland Security's secret project to change how we think about security", Muckrock, November 14, 2014, https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/

53 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* pp. 94-95

54 Moore, *Offensive Cyber Operations: Understanding Intangible Warfare,* p. 79.

55 Kania and Costello, "Seizing the commanding heights: the PLA Strategic Support Force in PLA military power", pp. 1-48

56 Thomas Withington, "Killer Code: Cyber-Supported SEAD", *European Security and Defence,* July, 2021.

57 "From "Ministry" to Military", What Should Our Army Joint Service Need to Stride Over", *Peoples Liberation Army News,* April 18, 2017.

58 "Chinese hackers target power grid near Ladakh", *The Hindu,* April 7, 2022, https://www.thehindu.com/news/national/chinese-hackers-target-power-grid-near-ladakh/article65299500.ece

59 "Chinese hackers target power grid near Ladakh".

60 Kevin McCauley, "Logistics Support for Cross-Strait Invasion: The View From Beijing", China Maritime Report No. 22, July 2022, p. 1, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1021&context=cmsi-maritime-reports

61 McCauley, "Logistics Support for Cross-Strait Invasion: The View From Beijing".

62 McCauley, "Logistics Support for Cross-Strait Invasion: The View From Beijing".

63 Withington, "Killer Code: Cyber-Supported SEAD".

64 Ellen Nakashima, "Trump Approved "Offensive" Cyber Strikes Against Iran's Missile Systems", *Washington Post,* June 23, 2019.

65 Nakashima, "Trump Approved "Offensive" Cyber Strikes Against Iran's Missile Systems".

66 Author Interview with cyber expert.

67 Author interaction with cyber expert.

68 Rachel S. Cohen, "Compass Call Appears to Take On a New Mission", *Air Force Magazine,* August 28, 2019, https://www.airforcemag.com/compass-call-appears-to-take-on-new-mission/

Endnotes

69 John Toepher, "SEAD From the Ground Up: SOF's Role in the Suppression of Enemy Air Defences", Thesis, Naval Postgraduate School, Monterey, California, June 2019, pp. 30-42, https://apps.dtic.mil/sti/pdfs/AD1080474.pdf

70 Catherine A. Theohary and John R. Hoehn, "Convergence of Cyberspace Operations and Electronic Warfare", *Congressional Research Service (CRS),* August 13, 2019, https://sgp.fas.org/crs/natsec/IF11292.pdf.

71 John Toepher, "SEAD From the Ground Up: SOF's Role in the Suppression of Enemy Air Defences", Thesis, Naval Postgraduate School, Monterey, California, June 2019, pp. 30-42, https://apps.dtic.mil/sti/pdfs/AD1080474.pdf

72 Thomas Withington, "Carry on up the Cyber!", *Armada International,* April 1, 2021, https://www.armadainternational.com/2021/04/carry-on-up-the-cyber/

73 Withington, "Carry on up the Cyber!".

74 "Programme Samyukta", Defence Research and Development Organisation (DRDO), https://www.drdo.gov.in/programme-samyukta

75 Author interviews with retired and serving Indian Army officers.

76 This is true specifically for the IA.

77 Thomas Rid, *Cyber War Will Not Take Place,* (New York: Oxford University Press, 2013), p. 42; Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies,* Vol. 35, Issue 1, 2012, p. 16.

78 Rid, *Cyber War Will Not Take Place,* p. 42. See also, Thomas Withington, "Cyber, Electronic and Kinetic attack pillars", *Armada International,* March 4, 2020, https://www.armadainternational.com/2020/03/error-404/

79 Interviews conducted by the author with serving and former Indian Army Officers.

80 Thomas Withington, "The British Army's EW Posture", *European Security and Defence,* June, 2021.

81 Withington, "The British Army's EW Posture".

82 Withington, "Cyber, Electronic and Kinetic attack pillars".

83 Toepher, "SEAD From the Ground Up: SOF's Role in the Suppression of Enemy Air Defences", p. 39.

84 Carl Von Clausewitz, *On War,* Edited and Translated by Michael Howard and Peter Paret, (Princeton: NJ, Princeton University Press, 1989), p. 198.

85 Jacob G. Oakley, *Waging Cyber War: Technical Challenges and Operational Constraints,* (Delaware: Apress, 2019), p. 99.

Endnotes

86 Toepher, "SEAD From the Ground Up: SOF's Role in the Suppression of Enemy Air Defences".

87 Echevarria, *Military Strategy: A Very Short Introduction*, p. 103.

88 Author interview with former Senior Indian Army officer who headed the Directorate General of Information System (DGIS).

89 Author interview with retired Indian Army Signals Corps officer.

90 Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space", Space Dossier 3, The United Nations Institute for Disarmament Research (UNIDIR), Geneva, May 2019, pp. 1-18.

91 See Beyza Unal, "Cyber-security of NATO's Space-Based Strategic Assets", Chatham House, Royal United Services Institution (RUSI), 2019, p. 6.

92 Luke Shadbolt, "Technical Study: Satellite Cyber Attacks and Security", HDI Global Specialty HE, July 2021, p. 11, https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf

93 Shadbolt, "Technical Study: Satellite Cyber Attacks and Security".

94 Brooks Tigner, "Electronic jamming between Russia and NATO is par for the course in the future, but it has its risky limits", Atlantic Council, November 15, 2018, https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/

95 Beyza Unal, "Cyber-security of NATO's Space-Based Strategic Assets", Chatham House, Royal United Services Institution (RUSI), 2019, p. 6.

96 Arun K. Somani and Tao Wu, "Monitoring and Detecting Attacks in All-Optical Networks", in Yi Qian, James Joshi, David Tipper and Prashant Krishnamurthy, *Information Assurance: Dependability and Security in Networked Systems*, (eds.), (Elsevier, 2008), pp. 307-347.

97 Somani and Wu, "Monitoring and Detecting Attacks in All-Optical Networks".

98 Author interview with Indian Army officer.

99 Jingjing Liao and Xinjian Ou, "5G Military Application Scenarios and Private Network Architectures", *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA)*, 2020, pp. 726-732

100 Liao and Ou, "5G Military Application Scenarios and Private Network Architectures".

101 Interview with Indian Army officer.

Endnotes

102 This was point underlined by all IA officers both retired and serving to the author.

103 This point was made former IA Signals Corps officer.

104 Author interview with IA officer.

105 Pradip R. Sagar, "Three-pronged Plan", *The Week*, June 1, 2019, https://www.theweek.in/theweek/current/2019/05/31/three-pronged-plan.html

106 "Our Mission and Vision", U.S. Cyber Command, https://www.cybercom.mil/About/Mission-and-Vision/

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

ORF 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