

SPECIAL **REPORT** no. 209

Emerging Technologies and India's Defence Preparedness

**Kartik Bommakanti, Yogesh Joshi, Shimona Mohan,
Karthik Nachiappan, Antara Vats**



APRIL 2023

Introduction

Rapid transformation in so-called ‘disruptive technologies’ is changing the landscape of military capability and strategy. Emerging technologies such as autonomous weapons, cyber weapons, weaponisation of space, and Artificial Intelligence, by themselves or in combination with conventional modes of warfare, are determining success or failure in contemporary battlefields—not only the conventional but sub-conventional and nuclear. India, as a latecomer to indigenous capability generation in modern military hardware, faces the urgent task, to paraphrase Prime Minister Narendra Modi, of combining the third and fourth industrial revolutions in military capabilities.

However, incorporating these emerging technologies in India’s military preparedness is only part of this transformation. Technology by itself hardly wins wars; it needs to be included in military strategy and tactics. Facing a growing threat from Pakistan and China, how is the Indian military coping with the challenge of emerging technologies? What kind of capabilities is the Indian military developing in these fields? Finally, how do these new platforms fit into India’s military strategy vis-à-vis its regional rivals, Pakistan and China?

Attribution: Kartik Bommakanti, et al., “Emerging Technologies and India’s Defence Preparedness,” *ORF Special Report No. 209*, April 2023, Observer Research Foundation.

This special report, jointly authored by researchers from the Observer Research Foundation and the Institute of South Asian Studies, National University of Singapore explores how the Indian military is dealing with the challenges and opportunities provided by four critical emerging technologies—i.e., Autonomous systems, Cyberwarfare, Space, and AI—in transforming its warfighting potential and strategy.

Modern warfare is highly networked, where sensors and shooters are intricately connected across war-fighting platforms and command and control (C2) structures. In the first section of the report, Kartik Bommakanti and Shimona Mohan describe the role of Space-Ground Integrated Information Networks (SGIIN) in fostering India's capability to wage networked warfare. They argue that India needs to temper its overemphasis on ground-based sensors and balance it with the optimum use of space-based platforms for the efficient conduct of network warfare. In achieving an optimum distribution of battlespace networks between ground and space, small satellites can play a vital role.

The second section, authored by Yogesh Joshi, explores the role of autonomous weapons particularly unmanned aerial vehicles or drones, in India's military strategy. Unlike the argument made by various analysts and military decision-makers that emerging technologies such as drones are going to change warfare altogether, Joshi argues that battlefield success will be more dependent on better integration of autonomous weapons into traditional core competencies of militaries such as combined arms manoeuvres and camouflage. Autonomous weapons cannot and *should not* be considered as an independent vector of force projection.

The third section investigates the role of Artificial Intelligence in India's emerging military capability and strategy. Antara Vats argues that the Indian military has taken seriously the impact of AI on the future of warfare, whether in beefing up its firepower, increasing the accuracy of platforms, speeding up its decision-making processes, augmenting its ISR capabilities, and generating more efficiency in its logistical processes. Vats underlines how India is leveraging its foreign policy to augment its AI capabilities through collaboration with various countries with advanced AI bases.

Lastly, Karthik Nachiappan examines India's cyber warfare capabilities and the emerging role of cyber weapons in India's defensive and offensive military strategies. He argues that even as India faces formidable cyber adversaries and has been a target of their cyber operations, the Indian establishment has focused inordinately on defensive cyber operations and cyber offence has

not made inroads into the deterrence calculus. It is, therefore, important to lay out the landscape around offensive cyber operations in India—attitudes to cyberspace, institutions that govern cyberspace and its effects on cyber operations—before analysing whether India can adopt an offensive cyber approach.

“Emerging technologies, by themselves or in combination with conventional warfare, are determining success or failure in contemporary battlefields—not only the conventional but sub-conventional and nuclear.”

Strengthening SIGINT for NCO through an Indian Space-Ground Network

Why do the Indian armed forces need to strengthen their Space-Ground Integrated Information Network (SGIIN) to strengthen their Signals Intelligence (SIGINT) capabilities for the effective conduct of Network Centric Operations (NCO)? Satellites today perform communications, data relay, sensing and navigation functions, but they operate in silos or independently of each other. An SGIIN capability will redress this deficit by linking satellites in multiple orbits to mobile and static terrestrial users, creating a potent and well protected space-ground network, which will provide considerable advantages to the Indian military.

The current challenge is that space-based information networks are heavily reliant on the development and establishment of ground networks. Consequently, a number of functions

of a network are dependent on the ground segment such as routing, switching, and network management.¹ The subsequent analysis assesses why the Indian armed forces need an SGIIN. The United States' (US) Transformational Satellite (TSAT) Programme, which is now defunct² and the future People's Republic of China (PRC)'s SGIIN, can serve as templates for Indian decision-makers to develop an indigenous space-to-ground capability. China has also a planned GuoWang mega constellation consisting of 13,000 satellites and launched under the country's 13th Five Year Plan,³ which has superseded Beijing's more limited Low Earth Orbit (LEO)-based constellations such as the Hongyan and Hongyun.⁴ SGIIN or TSAT-like capability is akin to an "internet in the sky" that is expected to service the communications, data and situational awareness requirements of the war fighter.⁵

This section outlines the imperative for the Indian armed forces to acquire an SGIIN-like capability—an essential requirement for the conduct of NCO—and explains the different architectures that the US and China are pursuing; and highlights a key feature of a TSAT or China’s SGIIN-like network, the Tracking and Data Relay Satellites (TDRS), which are as critical to a prospective Indian space-based information network or an SGIIN capability in wartime for the effective conduct of NCO missions. It underlines the role of Small Satellites (SmSats) in the establishment of an SGIIN, whose deployment is primarily in LEO. To be sure, a set of satellites in Geostationary Orbit (GEO), Medium Earth Orbit (MEO) and LEO, will need to be interconnected for an effective and functional space-ground network.

There are several advantages to the development and acquisition of an SGIIN capability if it is realised as opposed to satellite systems of the past, which also remain in use. The former is akin to an internet system that integrates space, air and ground networks utilising Internet Protocol Version 6 (IPv6), and provides communications access to a wide network of users that are deployed and mobile. As Table 1 shows, an integrated space-borne information architecture similar to the US’s TSAT or China’s SGIIN satellite constellation brings considerable benefits and therefore,

acquiring a space-based information network is in the best interests of all three forces of the Indian military. There are tactical advantages which an Indian SGIIN capability would bequeath: improved multi-domain awareness, decision support to commanders, lethality by increasing sensor-to-shooter capabilities for the warfighter, improved survivability, and timely and secure communications across media—optical, voice and data for the effective conduct of network centric operations. From a strategic standpoint, India’s possession of an SGIIN capability helps deal with the military challenge posed by China. An SGIIN capability in the hands of China and not with India, also gives the PLA the advantage to employ its space-ground capability to produce a decisive outcome in a military contest against India. At the same time, India’s acquisition of a multi-orbit space-to-ground capability will also help the Indian military perform better across the battlespace. Additionally, an Indian SGIIN capability proffers a key strategic benefit—deterrence, helping the Indian armed services prevent a war from being initiated by China. In the event deterrence fails, SGIIN can also play an enabling role for the execution of NCOs. Ultimately, the possession and integration of SGIIN could mean the difference between victory and defeat, which have their own strategic consequences.

A TSAT capability will provide Tier 1 data transfer services that will help the Indian armed services attain net-centricity. It consists of: 1) a space segment; 2) a ground-based operations and management segment; and a 3) terminal segment.⁶ Both a TSAT and SGIIN will help dispense or at least limit dependence on a large number of terrestrial stations, because very few local ground stations will be required to attain global coverage.⁷ As Figure 1 illustrates, the TSAT-type architecture of satellites, which readers might find dated, is one way of deploying and developing a space-based integrated information network. It showcases the features of a TSAT system.

Regardless of architecture, the TSAT is a constellation of at least five Geostationary Satellites (GEOSATs), which forms the space backbone of a space-borne information network interlinked via laser communications. Laser and optical communication are fundamental to a space-borne information system. GEOSATs are high throughput satellites that go up to 50 Mbps downlink and 5 Mbps uplink (and in some new constellations, throughput can be as much as 300 Mbps).⁸ Nevertheless, they have high latency which is the voice and data transmission time from space to ground. GEOSATs also give a wider Field of View (FoV) as Figure 3 shows enabling detection of missile launches and tracking capabilities, giving

critical early warning capabilities to Indian decision-makers and military commanders. They are generally preferred by militaries across world, because they provide a “...quasi-permanent Earth Observation, thus favouring them for military... surveillance missions.”⁹

While they have higher temporal resolution, their spatial resolution in the form of immediate Field of View (iFoV) is limited. Although, a TSAT architecture consisting of exclusively geostationary satellites is also vulnerable to counterspace measures such as kinetic attacks by Direct Ascent Anti-Satellites (D-ASATs) given their fixed orbital paths, targeting satellites in the GEO is not as easy as even China’s DN-2 D-ASAT will take some five hours to reach and strike their targets in GEO, which are in an orbit of 36,000 kilometers (kms) over the earth, giving the defender sufficient time to conduct evasive manoeuvres.¹⁰ However, here too, there are trade-offs in that an operational satellite in GEO executing an evasive action against a D-ASAT is likely to consume fuel on board, reducing the orbital shelf life of the spacecraft. Half the weight of a satellite consists of fuel and this vulnerability still remains a universal problem for any spacefaring country.

Further, GEOSATs are few in number and the loss of even one of them can adversely impact military communications and operations. Unlike GEOSATs, SmSats in a multi-orbit constellation offer some measure of insurance in that they are more easily replaceable with India’s Small Satellite Launch Vehicle (SSLV)¹¹ and offer a multi-layered and variegated capability to the Indian armed forces. SmSats in LEO also have the advantage of lower latency because they are in 500- to 1,500-km orbits, making their transmission time of data and voice communications are lower.¹² Proximity to the Earth also means they can communicate better

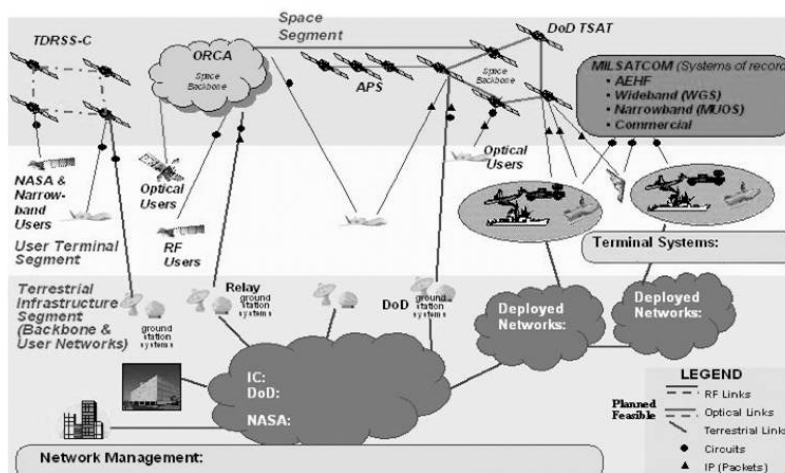
with fixed and rotary wing aircraft and require very small Satellite Communications (SATCOMs) terminals, unlike GEOSATS.¹³ SmSats possess low Size, Weight and Power (SWaP), enabling the use of light terminals and lower power consumption. They can transmit data in real time, enables quicker Command and Control (C2),¹⁴ and provide Beyond Line of Sight (BLOS) communications¹⁵ as well as voice and text communications that is less than 2 seconds as is the case with Iridium satellites.¹⁶

Table 1: Features of TSAT Architecture

1. High-capacity packet services in space.
2. The space backbone transmits data with multi-gigabits per second.
3. Enables circuit-based to packet-based switching. It is also capable of using hybrid mix of switching technologies, which include optical, Radio Frequency (RF) and packet switching.
4. Allows a high rate of transmission of data or circuit switching across space, airborne and terrestrial terminals.
5. Wide usage of commercially available technologies and established Internet Protocols. It also deploys Internet Protocol Version 6 (IPv6).
6. Modulation and coding are dynamic in a TSAT system. The air and space-borne ISR missions will require and secure high data rates. This is crucial in any tactical environment. Mobile units will get high bandwidth, for effective joint operations, and the system promises to support a variety of users.
7. Highly automated and allows for better network planning and management.
8. Generally, TSAT is a well-protected with a secure communications network.
9. Being a Tier 1 provider of data for global coverage TSAT links must be endowed with low probability for intercept and anti-jam capabilities for strategic missions and effective prosecution of net-centric operations.

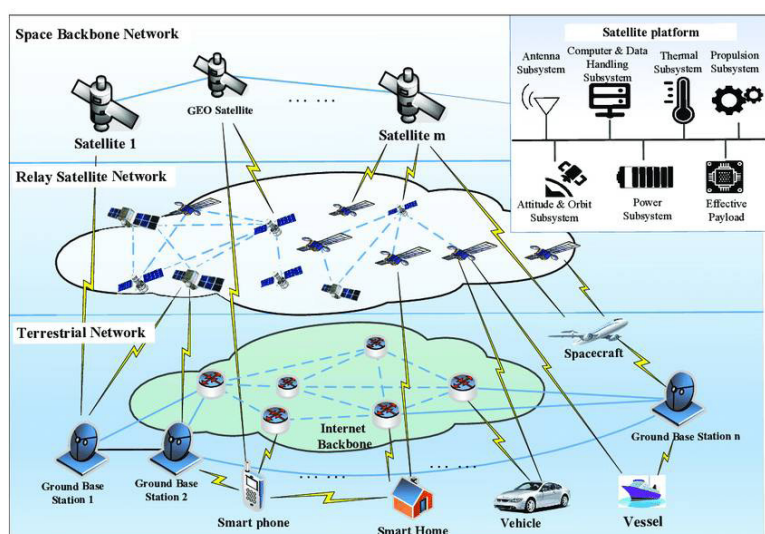
Source: Jeff Pulliam, Yadunath Zambre, Ani Karmarkar, Vineet Mehta, Joe Touch, Josh Haines and Matthew Everett, “TSAT Network Architecture, p. 7, <https://www.strayalpha.com/pubs/milcom2008-tsat-netarch.pdf>

Figure 1: TSAT Architecture



Source: Major (USAF) Maurice M. McKinney, “Transformational Satellite (TSAT) Communications Systems: Falling Short on Delivering Advanced Capabilities and Bandwidth to Ground-Based Users”, Wright Flyer Paper, No. 27, Air Command and Staff College, Air University Press, Maxwell Air Force Base, Alabama, July 2007, p. 5.

Figure 2: Typical SGIIN Architecture



Source: Daojing He, Xuru Li, Sammy Chan, Jiahao Gao and Mohsen Guizani, “Security Analysis of Space-Based Wireless Network”, IEEE Network, January/February, 2019, p. 37

The Indian Space Research Organisation (ISRO) is currently developing the Indian Data Relay Satellite System (IDRSS) satellites for better in-orbit crew communication as part of its Gaganyaan mission, which is India's human spaceflight mission.¹⁷ IDRSS will also enable communications between space and ground stations. Since orbiting spacecraft do not have a clear path of visibility to the Earth to transfer data or information, data relay spacecraft will help with the passage of information.¹⁸ This is as important for the Indian warfighter as it is for Indian astronauts, as it enhances communications and battlespace awareness.

Within India, there is recognition from the civilian space scientific community, if not the armed services, about the imperative for a TDRS capability. Indeed, ISRO scientists have addressed the significance of TDRS capabilities in terms of multi-orbit communications, Telemetry, Tracking and Command (TTC) capabilities, end-to-end use in LEO obviating ground stations, laser-based communications enabling high data rate transmission and protected communication and the data security that TDRS spacecraft offer.¹⁹ China has launched and operationalised its own TDRS satellites with the first Tianlian -1 launched in 2008, and the second, more advanced second-generation satellite Tianlian- 2 (02), and finally the Tianlian- 2 (03) in July 2022 in support of the under development Tiangong space station.²⁰

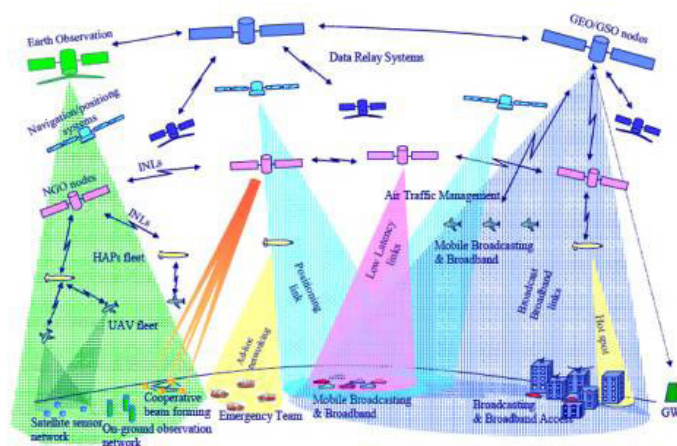
However, the TDRS capabilities in a form that meets the needs of the Indian armed forces is still not planned, nor have India's strategic and military planners demonstrated any visible enthusiasm or vision to develop a comparable system such as China's SGIIN. The latter is likely to feature six GEO-based satellites forming the space backbone, which should include data relay satellites, connected by inter-satellite links to possibly MEO-based satellites and a planned 60 hybrid spacecraft and 60 broadband satellites that are LEO-based once launched and operationalised.²¹

Most likely the latest version of an American space information network, whose architecture could feature a mix of geostationary, Medium Earth Orbit (MEO) and LEO satellites. A prospective European space-ground network dubbed the Integrated Space Infrastructure for Global Communications (ISICOM) would be similar in architecture to a future Chinese SGIIN and potentially an Indian SGIIN as shown in figure 3. Decoys can also be deployed in GEO and MEO to deceive India's adversaries, when it decides to build a three or multi-orbit SGIIN.²² Nevertheless, spacecraft in LEO will have to be an indispensable part of it.²³

LEO spacecraft communications are faster through space, because speed of light is faster through space than it is through fiber optic cables as light travels 31 percent slower through the latter.²⁴ Communication routes are more direct or have a straight path of transmission and transmission delay or latency is low due to the spacecraft' low altitude at 500 kms.

Whereas with fiber optic cables point to point transmission is constrained by geographic factors such as mountains, national borders, the sea and the density of population.²⁵

Figure 3: Proposed European Integrated Space Infrastructure for Global Communications (ISICOM)

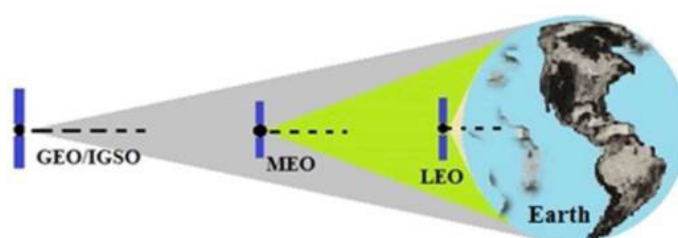


Source: Zhenhua Liu, Chuanwen Lin and Gang Chen, “Development and Trend of Space based Information Network”, *Journal of Physics: Conference Series*, Vol. 1544, 2020, p. 3.

Ultimately every orbit and spacecraft located in it, has its strengths and weaknesses. Indeed, multi-orbit satellites are the only way for India to create redundancy and complementarity and remain the best way, if not to neutralise then at least to limit damage by the counterspace capabilities²⁶ of China and Pakistan. While SmSats may have advantages in terms of launch costs, high revisit rates and sheer numbers making them difficult to destroy, their optical and transmission power is low.²⁷ An LEO-based constellation running into thousands of satellites networked to communicate with each other as well as with ground stations are a strength for LEO-based SmSats. However, an exclusive investment by India in LEO-based communications and Intelligence, Surveillance and Reconnaissance (ISR) satellites geared to meeting the requirements of an SGIIN capability will render it vulnerable to cyber-attacks which is among their chief weaknesses. SmSats in LEO are likely to increase the surface of (cyber) attack for any would-be or cyber-capable adversary, because there are numerous points for entry in a spacecraft.²⁸ This contrasts with a GEO satellite, which follows a bent-pipe principle by relaying communication to a single-user terminal and vice versa, which is at fixed position and transmits a signal back to a ground station to a network that is linked.²⁹

As one former officer who headed the Directorate General of Information Systems (DGIS) for the Indian Army (IA) observed about a prospective Indian SGIIN capability: “It should be hack-proof and have redundancy.”³⁰ This is especially vital given the increasingly higher engagement rate of the cyber-space nexus, as seen for instance in the cyber-attacks on Viasat and SpaceX’s Starlink satellites during the Russian invasion of Ukraine in February 2022.³¹ Encryption is one way to make satellites hack-resistant, especially in LEO, deployed as part of a future Indian SGIIN. However, increased encryption means commensurately high costs.³² The choice is between the higher risk of relaying data rapidly, which increases the chance of a cyber-attack as opposed to cyber-proofing LEO-based SmSats. When it comes to nuclear Command, Control and Communications (NC3),³³ India may be compelled to opt for cyber attack-resistant capabilities, especially in the nuclear domain, if not for conventional missions. They are also vulnerable to at least temporary damage in the form of non-kinetic measures such as jamming and microwave weapon attacks, if not to D-ASATs.³⁴

Figure 3: Field of View (FOVs) from Different Orbits



Source: Mathew Mowthorpe, “Space resilience and the importance of multiple orbits”, *The Space Review*, January 2, 2023, <https://www.thespacereview.com/article/4504/1>

Without SmSats and LEO constellation, an Indian space-borne information network will be unattainable, but GEO-based satellites will still be necessary to ensure resilience. Coverage will be based on the size and architecture of the satellite constellation and the number of terrestrial stations. An Indian SGIIN capability will need to be a multi-orbit constellation. Making up a segment of a prospective Indian integrated space-borne information network will be TDRS spacecraft in MEO. The LEO segment of the network could be similar in size, if not smaller, to China’s Hongyan and Hongyun constellations. A larger number of SmSats based in LEO will perform ISR missions and communications functions networked with MEO and GEO satellites. China already possesses data relay satellites, albeit primarily geared to supporting its Tiangong space station, and is in

the process of launching its own Guowang LEO constellation. The SGIIN would enable China to use a taut space-ground information network, augmenting its military’s situational awareness across domains. The Indian armed services significantly trail other spacefaring countries in conceiving an SGIIN-type satellite constellation. For all three Indian armed forces, the adoption and integration of IPv6 is still a work in progress.³⁵ Greater urgency is necessary to adopt IPv6. Most critically, Indian policymakers need to demonstrate clarity of vision by stepping up and financially supporting all the service branches of the Indian military to secure an SGIIN capability.

On Autonomous Weapons, Don't Fall for Technological Determinism

Militaries across the world, including India's, are of the view that disruptive technologies are changing the face of warfare.³⁶ In a webinar in June 2021, then Indian Army Chief Gen. Manoj Mukund Naravane acknowledged the autonomous role of technology in shaping future conflicts: "it may not be inaccurate to infer that technology itself is emerging as a core capability."³⁷ Naravane suggested that earlier modes of warfare fought with "large platforms" such as tanks, artillery, fighter aircraft and capital ships will be "rendered relatively less significant."³⁸ Among these disruptive technologies, lethal autonomous weapons (LAWS) have been the most prominent. The LAWS combine self-mobility, self-direction and

self-determination. It is only in the last domain of self-determination that weapons are in the landscape of a fully autonomous system. So far, LAWS have made their presence felt on the battlefield largely through what military parlance calls unmanned aerial combat vehicles (UCAVs) or drones. The Indian military decision-makers believe that "drones will be increasingly used in all sorts of combat in the future, both by the state and non-state actors" and therefore needs to be factored in all "future plans" for military action.³⁹ Such emphasis on technology, particularly on Unmanned weapon systems, has led to a belief that weapons of war have been "overtaken by disruptive technology."⁴⁰

Autonomous systems offer significant advantages over conventional weapon systems manned by humans.⁴¹ First, autonomous systems provide an edge in decision-making and reaction time, reducing one's own decision-making loop and allowing greater intervention in the adversary's decision-making cycle. Second, LAWS reduce some important elements from the friction and fog of war, whether concerning human fatigue, confusion and limitations of the human mind in understanding a fluid situation. Lastly, unmanned systems, even when allowing militaries to be more risk-acceptant and prone to the use of force, help control the escalation ladder by reducing domestic reputational costs. Loss of unmanned systems does not invoke pressures to retaliate as in the case of loss of manned systems.

However, LAWS do have its downsides. First, they can make war less political. Risk reduction can unwittingly motivate the initiation of wars but also reduce public interest in understanding the causes and consequences of war. Second and more importantly, autonomous weapons raise the question of political and military responsibility for the conduct of warfare, both at the tactical and strategic levels.

Yet, the question confronting the Indian military is far more fundamental: do autonomous systems change only the character of war or do they transform the nature of war? In so far as war is politics by other means, the nature of war endures. However, autonomous systems have caused two crucial changes in the character of war.⁴² First, they are rapidly "out-ranging" the enemy not only through their capability to target adversaries at long distances but by eliminating the need for physical contact. Second, they are reducing the decision time between sensing the enemy and its effective targeting.⁴³

Given the changes in the character of war, where do the Indian military planners locate the usefulness of LAWS in attaining India's military goals vis-à-vis its adversaries, and by extension its political objectives? Several factors are significant in apprehending possible answers to this puzzle. First, unlike the West which has used unmanned aerial systems to target distant terrorist groups with little direct contact with the adversary, the Indian military finds itself in immediate contact with its two main adversaries across a large yet unsettled border. Second, the Western experience is also misleading because of the asymmetry in the technological capabilities of the hostiles. Taliban and al-Qaeda have hardly had the technological capabilities to counter American drone warfare.⁴⁴

In a contested battlefield where the adversary possesses significant area-denial and anti-aircraft missile capabilities, the use of drones for offensive actions would be at a premium. Third, even in cases where drones have helped the cause of offensive action against conventional militaries such as the 2021 Armenia-Azerbaijan conflict, the air-defence and electronic warfare capability of the Armenian military were highly suspect.⁴⁵ The success of Azerbaijan's military campaign against drones was a result of, partly, Armenia's decrepit air-defence systems and also of its military's failure in following normal procedures of combined arms manoeuvre and camouflage.

Similarly, the havoc unleashed by Ukraine's use of drones during the initial assault by the Russian military to annex Kyiv was primarily caused by the latter's shabby tactical preparations and failure to implement combined arms manoeuvres. The "Russian problems" in establishing air superiority and logistical support, absence of short-range air defences, lack of counter-drone or electronic warfare and basic core competency of combined capabilities of armour and infantry were largely responsible for Ukraine's drone success.⁴⁶ Even

then, the Ukrainian drone use was more useful for harassment akin to guerrilla warfare. Ukraine had to rely on conventional military tactics and platforms for engendering a defensive stalemate. Russia's use of Iranian suicide drones during the latter phase of the war bordered on revenge-taking and terrorism rather than an intrinsic element of its military strategy.

The experience on the use of unmanned aerial weapon systems in warfare, therefore, has been highly limited, in scenarios of extreme capability difference between adversaries, avenues where they can be availed for asymmetric warfare for harassing enemy combatants or simply for provoking terror against unarmed civilians. First, conventional armies, brought up on conventional war-fighting techniques, need to adjust to cheap and precise targeting solutions against both them and the adversary by UCAVs. Loitering munitions, with maximum autonomy of self-determination to execute kills, are the most lethal of these systems. Second, excessive use of drones can help harass enemy forces, saturate air defences, attack key nodes of the enemy's networked systems and even terrorise civilians. UCAVs are, therefore, more force multipliers rather than independent vectors for projecting military power.

It is highly unlikely that the traditional role of the military in warfare will be usurped by LAWS. The requirement of all military operations—whether offensive, defensive or relating to low-intensity operations on land and sea—is fundamentally about control of territory and populations, as the Indian Military’s Joint Doctrine postulates.⁴⁷ Only human control is the ultimate arbiter of defeat and victory. Nevertheless, they will perform significant military roles. It is proven by now that unmanned systems will play a crucial role in Intelligence, Surveillance and Reconnaissance (ISR) and act as advanced nodes for networked warfare.⁴⁸ Yet, UCAVs have yet to achieve the physical agility, speed and payload capabilities of manned fighter aircraft and propeller-driven UCAVs are less effective in contested war zones particularly when air defences are highly saturated.⁴⁹ Most of India’s UCAVs are still propeller-driven and will be operating in highly defended airspace against both Pakistan and China.

Under this scenario, how should India employ and deploy its UCAVs vis-à-vis both Pakistan and China? Loitering munitions and swarm drones therefore will be the most promising avenues for India’s force projection on both the India-Pakistan and China-India borders. First, these assets can help target key nodes across the Line of Actual

Control, particularly Chinese air defences, key logistical bases and air support systems. Both Harops and Harpy loitering munitions under India’s possession provide New Delhi with such capabilities. The ongoing development of indigenous systems such as ALS-50 by Tata Advanced Systems Limited (TASL), as well as other efforts by Economic Explosives Limited (EEL) and Zmotion Autonomous Systems (ZMAS) will add further momentum to building India’s arsenal.

Second, the build-up to the Chinese encroachment on Indian territory which resulted in the 2020 Galwan crisis underscored the need for better ISR capabilities along the LAC.⁵⁰ The gaps in ISR capability continue to inflict Indian military preparedness. It was only through US technical means and the exchange of ISR information through the Pentagon that the Indian Army was able to deter another Chinese encroachment in Arunachal Pradesh in December 2022.⁵¹ Given the length and terrain of the contested border, UAVs can play a pivotal role. India’s existing ISR capabilities depend upon Searchers and Herons, which have limitations especially in terms of their operating ranges because of the lack of satellite communication links. Even the synthetic aperture radars carried by these systems are of low quality.

Third, autonomous systems must be fully integrated with conventional war-fighting assets. Without fully networked sensors and shooters, the Indian military cannot fully exploit the advantages offered by autonomous systems. Not only physical assets but autonomous systems need to be figured into the entire spectrum of the command-and-control system, which requires synthesis at both organisational and doctrinal levels. Organisationally, for a long period of time, unmanned aerial systems were operated by the Artillery. Only recently, these systems have been handed over to Army Aviation.⁵² More importantly, across battle theatres, an issue is how these assets are distributed and who decides for their allocation against what targets. Force structuring of India's UCAVs will become a critical factor.⁵³ With all services—the Army, Air Force and Navy—aiming to incorporate unmanned aerial systems in their force capabilities, it will be critical to how these systems are distributed between services and their interoperability in both Air-Land battle space along India's borders and Air-Sea battle space in India's maritime operations.⁵⁴

The Indian Army has yet to come out with an integrated doctrine to operationalise the deployment of LAWS in its warfighting thought process. In fact, none of the services so far have dedicated specific doctrinal thought over the use of drones in their military strategy. Even when the Joint Doctrine of the Indian Armed Forces

specifically mentions Space, Cyber, and Special Operations as distinct domains requiring greater jointness and integration, autonomous weapons and robotics remain an understudied concept.⁵⁵ Compare this lack of doctrinal clarity with countries such as Turkey which have developed specific doctrines and concepts on Robotics warfighting.⁵⁶ LAWS also require a battery of highly skilled and trained operators.⁵⁷ India's joint training doctrine released by the Integrated Defence Staff in November 2017 does indicate greater synergy in training across services.⁵⁸ It is imperative for the Indian military to develop joint training mechanisms and institutions to train the next generation of India's drone warriors.

The advent of autonomous weapons has only changed the character of war. Successful militaries would need to incorporate the advantages offered by these systems into their core competencies, whether projecting firepower, gathering intelligence or bringing greater efficiency in logistics.⁵⁹ Most importantly, the tactical supremacy of combined arms manoeuvre will continue to define future battle space. The Indian military should not consider autonomous weapons as an independent vector of force projection, only their better assimilation in traditional warfighting strategy and core competencies.

India's Defence Preparedness on Artificial Intelligence

At the 11th edition of the Indian Defence Expo in Lucknow in 2020, Army Chief Gen. M. M. Naravane, while recognising the unpredictability and indeterminable factors of future wars stated that technology will be key.⁶⁰ Indeed, Artificial Intelligence (AI) with its ability to analyse large datasets, discern the strategic environment, detect objects, weigh risks, and provide real-time intelligence—is playing a critical role in determining the defence preparedness of militaries globally by supporting on-spot assessments and decision-making capabilities.

Since 2014, the Indian government has pivoted towards adopting a technology-driven approach and significantly invested in the modernising of military and defence equipment to further India's defence preparedness.⁶¹ This move is consequential for India as it shares sensitive borders from Kashmir in the North to Sikkim in the East with Pakistan and China. While one adversary is supplying arms and ammunition to its terror networks in Jammu and Kashmir and Punjab using drones,⁶² the other is providing low-cost drones to support delivery and is challenging territorial integrity from the other side of the border.

In addition to developing and acquiring offensive AI capabilities including Lethal Autonomous Weapon Systems, India is utilising AI's potential to perform tasks like collecting and analysing data to monitor threats, detecting personnel and objects, anticipating logistical requirements, devising cost-effective approaches to missions, planning the future course of action, and stimulating human intelligence. Shortly after recognising technological modernisation as a priority as part of the national defence documents in 2017, the Indian Department of Defence Production (DDP) set up a multi-stakeholder task force with N. Chandrasekaran as the head to study the strategic implications of AI to provide military superiority.⁶³ The MoD set up a high-level Defence Artificial Intelligence Council (DAIC) under the stewardship of Defence Minister Rajnath Singh and Defence AI Project Agency under the Chairmanship of Secretary DDP in 2019 to provide guidance to develop an operating framework and drive policy-level changes for AI adoption in the Indian military; the council was allocated an annual budget of INR 1,000 crore.⁶⁴ The Defence Research and Development Organization's Centre for AI and Robotics is also providing support in developing AI-based signals intelligence solutions to enhance the intelligence collection and analysis capabilities of the armed forces.⁶⁵

With ambitions of becoming a global hub for AI as emphasised by Prime Minister Modi, India is leveraging its uniquely evolved IT ecosystem and Defence Public Sector Undertakings to develop and design AI systems to support core defence operations.⁶⁶ In early 2022, the Indian Navy hosted a workshop on leveraging AI in critical mission areas and launched the Centre of Excellence at INS Valsura on Big Data.⁶⁷ The Navy personnel are undergoing AI training at IIT campuses and Navy training schools. In July 2022, the Department of Defence Production at the MoD hosted AiDef or the first ever 'Artificial Intelligence in Defence' exhibition and symposium to display the accomplishments of DPSUs, research organisations, industry and domestic startups under the guidance of DAIC in the last three years.⁶⁸ In a report following the event, MoD documented 75 prominent use cases in the advanced stage of deployment.⁶⁹ The Indian military is working on about 100 more use cases which are in the early stages of development.

In addition to the autonomous offensive systems deployed across the Navy, Air and Land, there are three deployment trends of AI systems by the Indian military:⁷⁰

A) Intelligence, Surveillance, and Reconnaissance (ISR). ISR provides the base for all military operations as it equips the decision-makers with better situational awareness across domains by collecting, analysing and sharing information to make accurate and timely decisions. For instance, one of the AI systems currently used by the Indian military includes Drone Feed Analysis which conducts AI-enabled analysis on objects retrieved by drones and builds a database to identify patterns in enemy operations and predict the future course of action by adversaries using deep learning. It is being used to monitor counter-terrorism operations, illegal immigration movements, and border surveillance.

Seeker Monitoring and Analysis System, a self-contained system with facial recognition, surveillance, monitoring and analysis system, and Proactive Real-time Intelligence and Surveillance Monitoring System also assist in threat identification by monitoring multiple real-time feeds of disturbed areas, Line of Control, Line of Actual Control and generating alerts for suspicious movements. Similar tools to track vehicles (Project V-logger), intruders using intrusion detection systems (Sarvatra Pehchaan), human detection and facial recognition rail-mounted robots (Silent Sentry) among others are also being deployed at the Northern and Western Borders of India for real-time threat

monitoring.⁷¹ Additionally, to understand and collect information from adversaries, Natural Language Processing-based wearable language translation devices are also being developed with low weights, less latency and high battery life, for example, to translate from Mandarin to English.

B) Supply chain management and logistics. AI-based solutions to support military logistics ensure efficient transportation of soldiers, ammunition and equipment.⁷² Moreover, automating predictive capabilities for regular maintenance by alerting technicians assists in avoiding possible failure of components or equipment on the battlefield. For instance, PRO-HM+ enables the prediction of equipment failure by using AI to monitor flight patterns and the health of aircraft components.

C) Cyber operations. Non-kinetic methods of maintaining strategic deterrence including AI-enabled information operations assist in the generation and distribution of disinformation campaigns, political influence operations, and deep fakes. AI-enabled cyber-attacks can also be used for offensive and defensive purposes, such as network jamming, scanning vulnerabilities, intrusion detection, and prediction of cyber-attacks.

Despite India's strides in military AI adoption, the country is still in the nascent stages when compared to economies like the United States, China, and European Union. As part of a panel at AiDef 2022, Lt. Gen. Shantanu Dayal, Deputy Chief of Army Staff, also emphasised limitations in India's approach, saying, "The scope of artificial intelligence is vast. And if I did say, what we have done till now is very rudimentary or very basic of what the scope or potential of AI in the Indian Army can be."⁷³ Defence preparedness is not just about AI adoption but also updating existing policies, strategies, and tactics to ensure the integration of the technology across the three branches of the Indian military. On the occasion of 75th Army Day on 15 January 2023, the Defence Minister highlighted the gaps and requested the armed forces to "develop adaptation capabilities according to time" to secure India from all sides.⁷⁴

"Rapidity is the essence of war," Sun Tzu said in *The Art of War*, the Chinese military treatise that dates back to the 5th century.⁷⁵ This treatise has guided China's rapid integration of emerging technologies including AI, in its military modernising efforts. Under President Xi Jinping's leadership, China has

prioritised military modernisation and adopted the Next Generation Artificial Intelligence Development Plan to shift the People's Liberation Army's capabilities from informatised war to intelligentised warfare capability.⁷⁶ AI is the foundation layer on which China is strengthening and scaling up cross-domain deterrence across cyber, nuclear, and space domains. As such, the military-civil diffusion of AI development and adoption is an inherent part of China's national strategy as expanded under the China's Military-Civil Fusion plan of 2014. While the military AI applications are similar to the ones adopted by India, for instance, to facilitate decision-making, situational awareness on the battlefield, conduct multi-domain operations, and promote training, the velocity, volume and variety of adoption are significantly more advanced in China. Beijing has successfully leveraged its huge talent pool, collaborative efforts among industry and academia, and access to the vast pool of data resources to make significant advances in defence preparedness.

On the other hand, Pakistan has made few investments in AI. It launched the Presidential Initiative for Artificial Intelligence & Computing in 2018 which is one of the four initiatives to promote research, education and business in AI.⁷⁷ The other initiatives include the launch of the Centre of Artificial Intelligence and Computing at Rawalpindi, the National Center of AI, and the Department of Robotics and Intelligent Machine Learning at the National University of Science and Technology.⁷⁸ China is keen on assisting Pakistan in building its digital infrastructure and integrating its military AI systems. With the Digital Silk Road project under the Belt Road Forum 2019, Beijing is laying optic undersea cables and infrastructure for 5G wireless networks in Pakistan as part of the China-Pakistan Economic Corridor.⁷⁹ China is also providing training support on AI to Pakistan's military personnel.

With the recognition that AI can significantly tilt the scales of modern warfare, India has leveraged partnerships with economies in the advanced stages of utilising AI to further defence preparedness including the United States, Australia, Japan, and France in the recent years.⁸⁰ India is also improving its AI ecosystem to cement self-reliance as customisation of AI tools and data sovereignty is equally critical. The government has reserved

orders up to INR 100 crore on yearly basis for domestic Micro, Small & Medium enterprises (MSMEs) in Defence Acquisition Procedure (DAP) 2020.⁸¹ Innovations for Defence Excellence, an innovation ecosystem was also launched in 2018 to foster technology development and innovation in Defence with start-ups, MSMEs, innovators, academia and R&D institutes by providing them grants and research support.⁸²

While these initiatives are commendable, India must enhance investments at a rapid scale to match the steps with China. In 2023, China increased its defence budget for the eighth consecutive year and its budget is presently almost three times more than India's.⁸³ India must also design strategies to enhance cohesion amongst the three armed services and various Ministries that are working on AI to effectively utilise the AI-ready skill force, large amounts of datasets and address the rising risk of AI-powered cyberattacks and influence operations from China.^{84,85} It must also assign resources to build research on enhancing accuracy and precision in AI outcomes to avoid false negatives and positives at the battlefield.

Cyber Operations in India's Military Strategy

Despite mounting regional instability and a growing awareness of the range of cyber threats it confronts, India has yet to develop a coherent cybersecurity strategy and doctrine. Cyber-attacks by India's adversaries like China and Pakistan have risen as strategic competition intensifies in South Asia and the Indo-Pacific. Both state and non-state actors have been targeting India's critical infrastructures like nuclear plants, energy grids, telecommunication systems, hospitals and financial institutions through cyber-attacks.⁸⁶ There's a growing belief that China and Pakistan are coordinating cyber activities to disrupt and damage India's critical sectors, most recently, during the post-Galwan crisis when Indian security agencies went on high alert.⁸⁷ Though there is scarce evidence to prove that India has conducted cyber operations, officials in the NSA have argued that

such capabilities do exist to “conduct extensive cyber sabotage and cyber warfare.”⁸⁸ Moreover, Oxford Analytica suggests that India-based non-state actors like ‘Dropping Elephant’ have been engaged in conducting cyber operations without sufficient proof that New Delhi assisted in some capacity.⁸⁹

Yet, despite the proliferation of cyber threats and the increased intensity of cyber-attacks against India, debates continue on whether India should integrate offensive cyber capabilities into its military strategy. This section lays out the landscape around offensive cyber operations in India—i.e., attitudes to cyberspace, institutions that govern cyberspace, and the effects on cyber operations—before analysing whether India can adopt an offensive cyber approach.

It argues that the institutional conditions exist for India to adopt and deploy an offensive cyber approach into its military strategy but that outcome hinges on spelling out an adequate and nimble cybersecurity strategy that articulates how the Indian government views cyberspace as a security domain and the measures necessary to deal with threats emanating from that landscape through incumbent tools and capabilities.

Understanding India's institutional architecture of cyber issues could help understand and ascertain the broader framework around which cyber doctrine and cyber capabilities may find a place. Generally, India's approach to cyberspace has been cautious and slow, working gradually and in piecemeal—identifying cyber risks and threats, establishing institutions and policies, and using diplomacy to deflect rules that constrain domestic powers. India's cyber agencies, especially the National Technical Research Organization (NTRO) and the Computer Emergency Response Team (CERT), work closely with partners like the United States to bolster domestic cyber defence and resilience;⁹⁰ cyber diplomatic efforts are led by the Ministry of External Affairs (MEA).⁹¹ CERTs are largely responsible for mitigating cybersecurity threats by coordinating with their CERT counterparts of other countries.⁹² India's cyber response is largely shaped and governed by the 2008 Information Technology Amendment Act

with cyber responsibilities spread across a litany of national and state agencies.⁹³ This fragmentation has constrained India's cyber preparedness and stymied the growth of a partnership between the government and the private sector to identify and root out rising threats and risks online. As a result, the overall cyber approach has largely been defensive and domestic, focusing on fixing internal gaps before venturing to counter foreign threats.

Defensiveness, however, does not appear to have precluded Indian authorities from considering the development of offensive cyber capabilities. In 2016, the deputy National Security Advisor Arvind Gupta mentioned that India “needs to closely analyse the patterns of cyber attacks against us and build suitable response measures including the capability to conduct cyber operations, if required.”⁹⁴ This statement was echoed by Former Minister of State for Defence Shripad Naik who stated in Parliament in 2019 that “sufficient budgetary allocation is being provided for Cyber operations and capability development.”⁹⁵ Yet, the time to shift India's cyber approach and adopt an offensive mindset and posture may have arrived as threats fester and proliferate. To be sure, an offensive cyber strategy does not rule out bolstering domestic preparedness; essentially, this approach allows India to proactively identify and eliminate various cyber threats before they strike Indian targets.

What are offensive cyber operations? These operations are conducted by states using computer activities, digital tools and instruments to disrupt, degrade and destroy cyber threats.⁹⁶ Often, these operations are conducted in partnership with private sector firms with better knowledge of the tools used. Offensive cyber operations vary from using software to disrupt critical physical infrastructures like power grids and ports, to malware that targets dissidents or journalists or ransomware that demands payment to return data. Some cyber operations are designed to seek domestic influence or sabotage an adversary. What might such operations seek to accomplish? Different objectives exist. Offensive cyber operations can help obtain or exploit information on an adversary's network, particularly related to military strategy; to extract network information that could be used to disrupt its functioning later; conduct industrial espionage to gain a competitive advantage; used in conjunction with other military capabilities to soften and penetrate the adversary's defences in certain conflict situations.⁹⁷

So far, there is no concrete evidence that indicates India has integrated offensive cyber operations in its military strategy but the institutional conditions do exist for India to adopt and use an offensive strategy to deter and degrade cyber threats. Generally, states must have the adequate physical infrastructure to adopt an offensive cyber strategy, specifically sufficient intelligence, surveillance and reconnaissance (ISR) capabilities. These

ISR capabilities must be ubiquitous, real-time, persistent and capable of executing a strike when necessary. Currently, India is in the process of transforming its ISR structure which consists of information-gathering satellites, airborne platforms and ground based sensors that facilitate cyber operations.⁹⁸ The 2017 Indian Armed Forces Joint Doctrine signals the presence and relevance of ISR capabilities for conducting effective operations which does suggest that the Indian army could integrate and deploy cyber operations at some point.⁹⁹

Second, states need a cyber institution or agency that manages, runs and executes cyber operations. In 2021, India established the Defense Cyber Agency, which appears to resemble a cyber command that can undertake offensive cyber operations, hack and disrupt networks and mount surveillance operations.¹⁰⁰ Additionally, the National Cyber Coordination Centre (NCCC), launched in 2014, helps synchronise efforts among various government agencies tasked with cyber responsibilities.¹⁰¹

Finally, cyber agencies have to work with the private sector to develop a viable offensive cyber operations structure, given their ability to significantly influence the nature, execution and success of cyber operations.¹⁰² India has a robust and dynamic information technology sector that can support its cyber operations. The country also has strengths in the digital economy that includes a vibrant start-up culture and a large talent base.¹⁰³ The private sector has also moved more quickly than the government in promoting national cyber security, which gives New Delhi a potential advantage.¹⁰⁴


India has the necessary institutional conditions including infrastructure, cyber agency, and private sector expertise to adopt a viable offensive cyber approach. However, it lacks one fundamental aspect that could affect its ability to conduct offensive cyber operations abroad—a pronounced cybersecurity strategy. To be sure, the basic doctrine of the Indian Air Force mentions cyber warfare as “an attractive low cost war-waging model because it has some notable features such as low entry cost” and “can be conducted across the entire range of military and non-military operations to achieve national objectives”; however, it stops short of describing and analysing when such methods are to be used and in what context.¹⁰⁵ Similarly, the 2018 Land Warfare Doctrine suggests that the Indian Army needs to adapt to an era of information warfare and that

cyber conflict will form a terrain where new wars will be fought which necessitates the enhancement of existing cyber warfare capabilities.¹⁰⁶ These documents recognise the importance of cyber operations to military strategy but present an effective roadmap to integrate them.

A reliable and robust cybersecurity strategy is imperative to organise and execute responses to India’s cyber threats. A viable and agile policy framework safeguards India’s cyber strategy, whether offensive or defensive, allocates financing to implement that strategy, including investments in areas like the ISR, and identifies pathways where the private sector can contribute, if necessary. It provides a roadmap to protect and defend cyberspace. A strategy also allows India to adopt the requisite approach and measures to counter and deter rising digital threats. Delays in finalising this strategy effectively leave India vulnerable in an era defined by manifest and mounting cyber risks.

Conclusion

This report underlined how India should approach the emerging technological landscape in space, autonomous weapons, Artificial Intelligence, and cyber warfare in its military capability and strategy. The authors have emphasised why Indian defence planners need to integrate ground-based sensors with space-based assets for networked warfare, why autonomous weapons should be integrated into traditional core competencies of the Indian military, how AI is being leveraged for generating military efficiency, and why India must focus on cyber offensives in its military deterrent. However, emerging technologies are only disruptive to the extent that they will change the character of war: they will increase the speed of its execution, expand the physical distance between adversaries, and provide new avenues for conflict escalation and de-escalation. The nature of war insofar as it singularly prioritises political objectives over the conduct of war, however, will remain intact.

The Indian military should, therefore, understand how the shifts in the character of war unleashed by emerging technologies should aid the conduct of war to achieve political objectives rather than drive war autonomously. Technology, therefore, needs to be better integrated to build capabilities and command and control structures. Integration, rather than mere capabilities, will be the most important variable in availing technology for successful military campaigns, whether defensive or offensive. 

Endnotes

- 1 Zhenhua Liu, Chuanwen Lin and Gang Chen, “Development and Trend of Space based Information Network”, *Journal of Physics: Conference Series*, Vol. 1544, 2020, p. 4.
- 2 Rebbecca Cowen-Hirsh, “10 Years After TSAT: Comsatcom Advancements At the Core of Integrated Architecture”, *Via Satellite*, 26 June, 2018, <https://www.satellitetoday.com/government-military/2018/06/26/10-years-after-tsat-comsatcom-advancements-at-the-core-of-integrated-architecture/>
- 3 “The 13th Five Year Plan: For Economic and Social Development of the Peoples Republic of China – 2016-2020”, National Development and Reform Commission (NDRC), Beijing, 2016, <https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf>
- 4 Andrew Jones, “The coming Chinese megaconstellation revolution”, *Spaceneews*, February 23, 2023, <https://spaceneews.com/the-coming-chinese-megaconstellation-revolution/>
- 5 “TSAT: Essential to Security”, Lexington Institute, Arlington Virginia, August 2007, p. 1, <https://www.lexingtoninstitute.org/wp-content/uploads/TSAT-Essential-to-Security.pdf>
- 6 Jeff Pulliam, Yadunath Zambre, Ani Karmarkar, Vineet Mehta, Joe Touch, Josh Haines and Matthew Everett, “TSAT Network Architecture”, p. 7, <https://www.strayalpha.com/pubs/milcom2008-tsat-netarch.pdf>
- 7 Kai Lin Tay, “Evaluating China’s ‘Space Ground Integrated Information Network’ Project”, *The Diplomat*, May 21, 2021, <https://thediplomat.com/2022/05/evaluating-chinas-space-ground-integrated-information-network-project/>
- 8 Reuben Mann, “SKYTRAC #SatComSeries: The Differences, Strengths, and Weaknesses of LEO and GEO Satellites”, SKYTRAC, April 26, 2022, <https://www.skytrac.ca/resources/magazine/skytrac-satcomseries-the-differences-strengths-and-weaknesses-of-leo-and-geo-satellites/#:~:text=maintenance%20and%20upkeep.,Strengths%20of%20GEO%20Satellites%20Constellations,up%20to%20300%20Mbps%20throughput.>
- 9 M. Mesrine, E. Thomas, S. Garin, P. Blanc, C. Alis, F. Cassaing D. Laubier “High resolution earth observation from geostationary orbit aperture synthesis”, *International Conference on Space Optics – ICSO 2006*, Noordwijk, Netherlands, 27-30 June, 2006, <https://www.spiedigitallibrary.org/conference-proceedings-of-spice/10567/105670B/High-resolution-earth-observation-from-geostationary-orbit-by-optical-aperture/10.1117/12.2308095.full?SSO=1>
- 10 Mathew Mowthorpe, “Space resilience and the importance of multiple orbits”, *The Space Review*, January 2, 2023, <https://www.thespaceview.com/article/4504/1>
- 11 Rajeswari Pillai Rajagopalan, “India’s Space Program: The Commercial Domain”, *TheDiplomat*, May 10, 2019, <https://thediplomat.com/2019/05/indias-space-program-the-commercial-domain/>

- 12 Nandini Sarma, “Small Satellites: Breaking the monopoly of powerful nations in space industry”, *Commentary*, Observer Research Foundation, May 9, 2019, https://www.orfonline.org/research/strengthening-the-c4isr-capabilities-of-indias-armed-forces-the-role-of-small-satellites-67842/#_edn92, Mann, “SKYTRAC # SatComSeries: The Differences, Strengths, and Weaknesses of LEO and GEO Satellites”.
- 13 Mann, “SKYTRAC # SatComSeries: The Differences, Strengths, and Weaknesses of LEO and GEO Satellites”.
- 14 “Command and Control: High Reliability, Low Latency Command and Control (C2)”, <https://www.skytrac.ca/services/command-and-control/>
- 15 “Global Visibility for your Unmanned Flight Operations”, <https://www.skytrac.ca/services/bvlos/>
- 16 “Iridium Voice and Text Communications”, <https://www.skytrac.ca/services/voice-text-and-push-to-talk/>
- 17 Shouvik Das, “Gaganyaan Mission: ISRO to Launch IDRSS Satellites for Seamless Crew Communication”, *news18.com*, January 7, 2020, <https://www.news18.com/news/tech/gaganyaan-mission-isro-to-launch-idrss-satellites-for-seamless-crew-communication-2449535.html>
- 18 “Isro to launch data relay satellites to maintain contact Gaganyaan”, *Business Standard*, April 25, 2020, https://www.business-standard.com/article/current-affairs/isro-to-launch-data-relay-satellites-to-maintain-contact-with-gaganyaan-121042500389_1.html
- 19 Gottimukula Praveen Reddy, Imteyaz Ahmad, Killedar Pankaj Damodar, Anjaneyulu KVVSSSR, “Study of Data Relay Satellite System and its Relevance to Indian Context,” *International Journal of Pure and Applied Mathematics* 118, no. 16 (2018): 1227–1244.
- 20 Andrew Jones, “China launches new communications satellites to support Tiangong space station”, *space.com*, July 14, 2022, <https://www.space.com/china-launches-communications-satellite-tiangong-space-station>
- 21 Tay, “Evaluating China’s ‘Space Ground Integrated Information Network’ Project”.
- 22 Mowthorpe, “Space resilience and the importance of multiple orbits”.
- 23 Author interview with Indian military officer.
- 24 Lin Han, Alvaro Retana, Cedric Westphal and Richard Li, “Large Scale LEO Satellite Networks for the Future Internet; Challenges and Solutions to Addressing and Routing”, *Computer Networks and Communications*, Volume 1 Issue, 2022, p. 34.
- 25 Han et al., “Large Scale LEO Satellite Networks for the Future Internet; Challenges and Solutions to Addressing and Routing”.
- 26 Mowthorpe, “Space resilience and the importance of multiple orbits”.
- 27 Lieutenant Colonel Tim Vasen, “Mega-Constellations: Commercial Small Satellite Constellation in Low Earth Orbit”, *Joint Airspace Power Conference*, June 2020, <https://www.japcc.org/essays/mega-constellations/>
- 28 Shaun Waterman, “Leo Constellations’ Connectivity Offers Risks, And Rewards, Execs Warn”, *Air&Space Forces Magazine*, April 7, 2022, <https://www.airandspaceforces.com/leo-constellations-connectivity-offers-risks-and-rewards-execs-warn/>.

- 29 Mowthorpe, “Space resilience and the importance of multiple orbits”.
- 30 Former Indian Army officer interview with author.
- 31 Robert Lemos, “Space Race: Defenses Emerge as Satellite-Focused Cyberattacks Ramp Up,” *DARKReading*, January 2, 2023, <https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks>
- 32 Mowthorpe, “Space resilience and the importance of multiple orbits”.
- 33 Mowthorpe, “Space resilience and the importance of multiple orbits”.
- 34 Vasen, “Mega-Constellations: Commercial Small Satellite Constellation in Low Earth Orbit”.
- 35 Author interview with Indian Army officer.
- 36 Air Marshal Anil Chopra, “Aviation: The Future is Unmanned,” *USI Journal*, Vol. CXLIX, No. 615, January-March 2019, <https://usiofindia.org/publication/usi-journal/aviation-the-future-is-unmanned/>. Commander Manish Chowdhury, “Emerging Dynamics of Warfare — Role of Artificial Intelligence (AI) and Robotics and how India can exploit it,” Vol. CLI, No. 623, January-March 2021; Lt General VK Ahluwalia, “Imperatives of Transformation: Changing Character of Conflict in the Emerging World Order,” Vol. 12 No. 1 (2019): Summer 2019, <https://ojs.indrastra.com/index.php/clawsjournal/article/view/80>.
- 37 General Manoj Mukund Naravane, “Shifting Domains of Warfare,” *Manekshaw Papers* No. 96, Center for Land Warfare Studies, New Delhi, 2021, <https://www.claws.in/publication/shifting-domains-of-warfare/>.
- 38 Abhishek Bhalla, “Drones future of warfare to take on tanks and artillery: Indian Army chief,” *India Today*, February 11, 2021, <https://www.indiatoday.in/india/story/drones-future-of-warfare-to-take-on-tanks-and-artillery-indian-army-chief-1768343-2021-02-11>.
- 39 Mayank Singh, “‘Need to factor this in our strategy’: Army chief thinks drone warfare will be on the rise,” *The New Indian Express*, July 2, 2021, <https://www.newindianexpress.com/nation/2021/jul/02/need-to-factor-this-in-our-strategy-army-chief-thinks-drone-warfare-will-be-on-the-rise-2324332.html>.
- 40 “Weapons of war overtaken by disruptive technology: Indian Army Chief.” *The Sentinel*, February 11, 2021, <https://www.sentinelassam.com/topheadlines/weapons-of-war-overtaken-by-disruptive-technology-indian-army-chief-524352>
- 41 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (New York: WW Norton, 2018).
- 42 John Govern, “The Importance Of Distance In Modern Warfare,” May 16, 2016, Modern War Institute, <https://mwi.usma.edu/reexamination-distance-modern-warfare/>.
- 43 Benjamin Jensen and Matthew Strohmeyer, “The Changing Character of Combined Arms,” *War on the Rocks*, May 23, 2022, <https://warontherocks.com/2022/05/the-changing-character-of-combined-arms/>.
- 44 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (New York: WW Norton, 2018).

- 45 Col. Neeraj Trivedi, "Armenia-Azerbaijan Conflict: Implications for India," Center for Land Warfare Studies, Vol. 14 No. 1 (2021): Summer 2021, <https://ojs.indrastra.com/index.php/clawsjournal/article/view/123>; Shaan Sheikh and Wes Rembaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," CSIS, December 8, 2020, <https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense>.
- 46 John Kalberg, "Drones Will not Liberate Ukraine – but Tanks Will," June 24, 2022, CEPA, <https://cepa.org/article/drones-will-not-liberate-ukraine-but-tanks-will/>.
- 47 "Joint Doctrine: Indian Armed Forces" Headquarters Integrated Defence Staff, Ministry of Defence, 2017.
- 48 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, (New York: WW Norton, 2018).
- 49 Scharre, *Army of None: Autonomous Weapons and the Future of War*.
- 50 Debalina Ghoshal, "Possessing advanced ISR capabilities is crucial to India's conventional and nuclear deterrence," Force India, March 28, 2023, <https://forceindia.net/aero-india-2019/long-way-go/>.
- 51 Paul D. Shinkman, "U.S. Intel Helped India Rout China in 2022 Border Clash: Sources," US News, March 20, 2023, <https://www.usnews.com/news/world-report/articles/2023-03-20/u-s-intel-helped-india-rout-china-in-2022-border-clash-sources>.
- 52 Suchet Vir Singh, "As drones usher in new era of warfare, India's growing UAV industry begins to take flight," *The Print*, May 23, 2022, <https://theprint.in/defence/as-drones-usher-in-new-era-of-warfare-indias-growing-uav-industry-begins-to-take-flight/962704/>
- 53 Ministry of Defence, "Joint Doctrine: Indian Armed Forces" Headquarters Integrated Defence Staff, 2017
- 54 Ministry of Defence, "Joint Doctrine for Air-Land Operations" Headquarters Integrated Defence Staff, 2010.
- 55 Ministry of Defence, "Joint Doctrine: Indian Armed Forces" Headquarters Integrated Defence Staff, 2017
- 56 Ridvan Bari Urcosta, "The Revolution in Drone Warfare: The Lessons from the Idlib De-Escalation Zone," *Journal of European, Middle Eastern, & African Affairs*, August 31, 2020, <https://www.airuniversity.af.edu/JEMEAA/Display/Article/2329510/the-revolution-in-drone-warfare-the-lessons-from-the-idlib-de-escalation-zone/>, Abhishek Bhalla, "From Surveillance to Combat: Decoding India's drone mission," *India Today*, June 30, 2021, <https://www.indiatoday.in/india/story/decoding-india-drone-mission-surveillance-combat-jammu-attack-1820965-2021-06-30>.
- 57 Brigadier Kulbhushan Bhardawaj, "Emergence of Drone Warfare and Implications for India," *USI Journal*, Vol. CLI, No. 625, July-September 2021, <https://usiofindia.org/publication/usi-journal/emergence-of-drone-warfare-and-implications-for-india/>.
- 58 "Joint Training Doctrine: Indian Armed Forces" Headquarters Integrated Defence Staff, 2017, Ministry of Defence. New Delhi.
- 59 Chirs Stolz, Jeremy Sauer and Michael Kaiser, "Core Competencies For An Army Of Preparation," February 1, 2014, Association of the United States Army, <https://www.ausa.org/articles/core-competencies-army-preparation>.

- 60 Huma Siddiqui, “‘Technology will be a key driver of future wars, Indian Army is on track’: Army Chief Naravane – Exclusive Q&A ahead of DefExpo 2020”, *Financial Express*, February 4, 2020, <https://www.financialexpress.com/defence/technology-will-be-a-key-driver-of-future-wars-indian-army-is-on-track-army-chief-naravane-exclusive-qa-ahead-of-defexpo-2020/1855551/>.
- 61 *The New Age of Defence: Presenting AI preparedness of the Country in Defence*, <https://www.ddpmod.gov.in/sites/default/files/ai.pdf>, Department of Defence Production, Ministry of Defence, Delhi, 2022.
- 62 “Pak Using Drones To Smuggle Weapons, Says Jammu And Kashmir Top Cop”, *NDTV*, October 31, 2022, <https://www.ndtv.com/india-news/pakistan-has-started-new-game-of-smuggling-weapons-drugs-through-drones-j-k-dgp-dilbagh-singh-3476932>
- 63 Pranav Mukul, “Task force set up to study AI application in military”, *The New Indian Express*, February 3, 2018, <https://indianexpress.com/article/technology/tech-news-technology/task-force-set-up-to-study-ai-application-in-military-5049568/>.
- 64 “Raksha Mantri Launches 75 Artificial Intelligence Products/Technologies...”, Ministry of Defence, Government of India, July 11, 2022, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1840740>
- 65 Defence Research & Development Organisation, Centre for Artificial Intelligence and Robotics, <https://www.drdo.gov.in/labs-and-establishments/centre-artificial-intelligence-robotics-cair>.
- 66 Shreya Nandi, “India should soon become a global hub for AI, says PM Modi”, *LiveMint*, October 6, 2020, <https://www.livemint.com/news/india/want-india-to-become-global-hub-for-artificial-intelligence-pm-modi-11601912327145.html>.
- 67 “Indian Navy to incorporate Artificial Intelligence in forthcoming projects”, *IndiaAI*, January 28, 2022, <https://indiaai.gov.in/news/indian-navy-to-incorporate-artificial-intelligence-in-forthcoming-projects>.
- 68 “First Ever ‘Artificial Intelligence in Defence’ exhibition & symposium to be held in New Delhi on July”, July 8, 2022, Ministry of Defence, Government of India, <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1840142>.
- 69 “The New Age of Defence: Presenting AI preparedness of the Country in Defence”, Department of Defence Production, Ministry of Defence, July 11, 2022, https://www.google.com/search?q=The+New+Age+of+Defence%3A+Presenting+AI+preparedness+of+the+Country+in+Defence&source=hp&ei=JO4mZPmTD6qVseMPp-uV6A4&iflsig=AOEireoAAAAAZ-Cb8NKfKo41JK005AQp8ShkJYDd8XFmh&ved=0ahUKEwj5tYK6sIb-AhWqSmwGHad1Be0Q4dUDCAg&uact=5&oq=The+New+Age+of+Defence%3A+Presenting+AI+preparedness+of+the+Country+in+Defence&gs_lcp=Cgdnd3Mtd2l6EANQAFgAYABoAHAAeACAAQCIAQCQAQCgAQKgaAQE&scient=gws-wiz#fpstate=ive&vld=cid:ce91e660,vid:wEc3uxeHoTI
- 70 Harsh V. Pant and Kartik Bommakanti, *Towards the Integration of Emerging Technologies in India’s Armed Forces*, New Delhi, Occasional Paper No. 392, Observer Research Foundation, 2023, <https://www.orfonline.org/research/towards-the-integration-of-emerging-technologies-in-indias-armed-forces/>.

- 71 “Indian Army deploys AI-based system to reduce manual surveillance at borders”, *Hindustan Times*, August 6, 2022, <https://www.hindustantimes.com/technology/indian-army-deploys-ai-based-system-to-reduce-manual-surveillance-at-borders-101659779253991.html>; Rajat Pandit, “Army steps up deployment of AI-powered surveillance systems on borders with China & Pakistan”, *The Times of India*, August 7, 2022, <https://timesofindia.indiatimes.com/india/army-steps-up-deployment-of-ai-powered-surveillance-systems-on-borders-with-china-pakistan/articleshow/93402906.cms>.
- 72 Sanur Sharma, *Artificial Intelligence in Warfare*, New Delhi, Lok Sabha Secretariat, 2022, https://parliamentlibraryindia.nic.in/lcwing/Artificial_Intelligence_in_Welfare.pdf.
- 73 Pritam Bordoloi, “How does the Indian Army want to use AI?”, *Analytics India Magazine*, August 4, 2022, <https://analyticsindiamag.com/how-does-the-indian-army-want-to-use-ai/>.
- 74 “Majority weapons are operated through AI thereby eliminating need of any in-person human presence: Defence Minister Rajnath Singh”, *ANI*, January 15, 2023, <https://www.aninews.in/news/national/general-news/majority-weapons-are-operated-through-ai-thereby-eliminating-need-of-any-in-person-human-presence-defence-minister-rajnath-singh20230115183956/>.
- 75 Sun Tzu, *The Art of War* (Jaico Publishing House; First edition, 2010)
- 76 Jiayu Zhang, *China’s Military Employment of Artificial Intelligence and Its Security Implications*, *The International Affairs Review*, August 16, 2020, <https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap>
- 77 Ahyousha Khan, “Artificial Intelligence in South Asia and Implications for Pakistan”, *Strategic Vision Institute*, October 19, 2020, <https://thesvi.org/artificial-intelligence-in-south-asia-and-implications-for-pakistan/>.
- 78 National University of Sciences & Technology, National Centre for Artificial Intelligence, <https://ncai.nust.edu.pk/>.
- 79 Sonia Naz, *India’s Military Application of AI: Implications for Pakistan*, Lahore, Center for Security, Strategy and Policy Research, 2021, <https://csspr.uol.edu.pk/wp-content/uploads/2021/07/Indias-Application-of-AI-Tech.pdf>.
- 80 “Defence Minister Rajnath Singh to host Defence Ministers’ Conclave in Bengaluru on sidelines of Aero India 2023”, *NewsonAIR*, February 14, 2023, <https://newsonair.com/2023/02/14/defence-minister-rajnath-singh-to-host-defence-ministers-conclave-in-bengaluru-on-sidelines-of-aero-india-2023/>.
- 81 Defence Acquisition Procedure 2020: Atmanirbhar Bharat, 2020, <https://www.mod.gov.in/sites/default/files/DAP2030new.pdf>.
- 82 Ministry of Defence, Government of India, https://mod.gov.in/sites/default/files/pre6_0.pdf.
- 83 “China hikes defence budget for 8th consecutive year with 7.2 per cent increase to USD 225 billion”, *The Economic Times*, March 5, 2023, <https://economictimes.indiatimes.com/news/defence/china-plans-7-2-defence-spending-rise-this-year-faster-than-gdp-target/articleshow/98421749.cms>.

- 84 Ayushi Kar, “Involve Defence Ministry while drafting policies on AI, Big Data for telecommunication”, *The Hindu*, January 1, 2023, <https://www.thehindubusinessline.com/info-tech/involve-defence-ministry-while-drafting-policies-on-ai-big-data-for-telecommunication/article66327157.ece>.
- 85 Sriparna Pathak and Divyanshu Jindal, “China’s AI-powered influence operations at India’s doorstep”, *Hindustan Times*, March 6, 2023, <https://www.hindustantimes.com/ht-insight/chinas-ai-powered-influence-operations-at-india-s-doorstep-101678086529152.html>
- 86 Anupriya Chatterjee, India’s had its worst year of cyberattacks, but 2023 will see govt & firms ramp up defences. *The Print*, December 30, 2022, <https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/>. For a list of cyber-attacks on India, see “Cyber Operations Tracker”, Council on Foreign Relations. <https://www.cfr.org/cyber-operations/>.
- 87 Aditya Bhan and Sameer Patil, “Pakistan emerges as China’s proxy against India,” <https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india/>
- 88 M.K. Narayanan, “The best among limited options,” *The Hindu*, November 1, 2016. <https://www.thehindu.com/opinion/lead/The-best-among-limited-options/article14990381.ece>
- 89 “New players join the race for offensive cyber capabilities”. Oxford Analytica Daily Brief. 20 August. Oxford Analytica. 2018, As of 11 March 2021: https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Egloff_2018_Oxford-Analytica-New-players-join-race-for-offensive-cyber-abilities-.pdf
- 90 For an overview of India’s cyber architecture, see Arindrajit Basu, UNIDIR India’s International Cyber Operations: Tracing National Doctrine and Capabilities, <https://www.unidir.org/cyberdoctrines/India>.
- 91 Basu, UNIDIR India’s International Cyber Operations: Tracing National Doctrine and Capabilities; Also see. Statement delivered by India at the Organisational Session of the Open-Ended Working Group (OEWG) on ‘Developments in the field of Information and Telecommunications in the context of International Security’ 3 June, 2019, Government of India. Ministry of External Affairs, <http://meaindia.nic.in/cdgeneva/?8251?000>
- 92 ‘Developments in the field of Information and Telecommunications in the context of International Security’.
- 93 ‘Developments in the field of Information and Telecommunications in the context of International Security’.
- 94 Arvind Gupta, “Keynote address by Dr Arvind Gupta, Deputy National Security Advisor at the 18th Asian Security Conference on ‘Securing Cyberspace: Asian and International Perspectives.’” Manohar Parrikar Institute for Defence Studies and Analyses, February 10, 2016, New Delhi https://idsa.in/keyspeeches/18asc-securing-cyberspace-asian-and-international-perspectives_deputy-nsa.
- 95 Cyber Warfare Threats. Lok Sabha Starred Question No.138, Government of India. Ministry of Defence, November 27, 2019, <http://164.100.24.220/loksabhaquestions/annex/172/AS138.pdf>.
- 96 Herbert S. Lin, “Offensive cyber operations and the use of force.” *Journal of National Security Law & Policy* Vol. 4, 2010, p. 63.

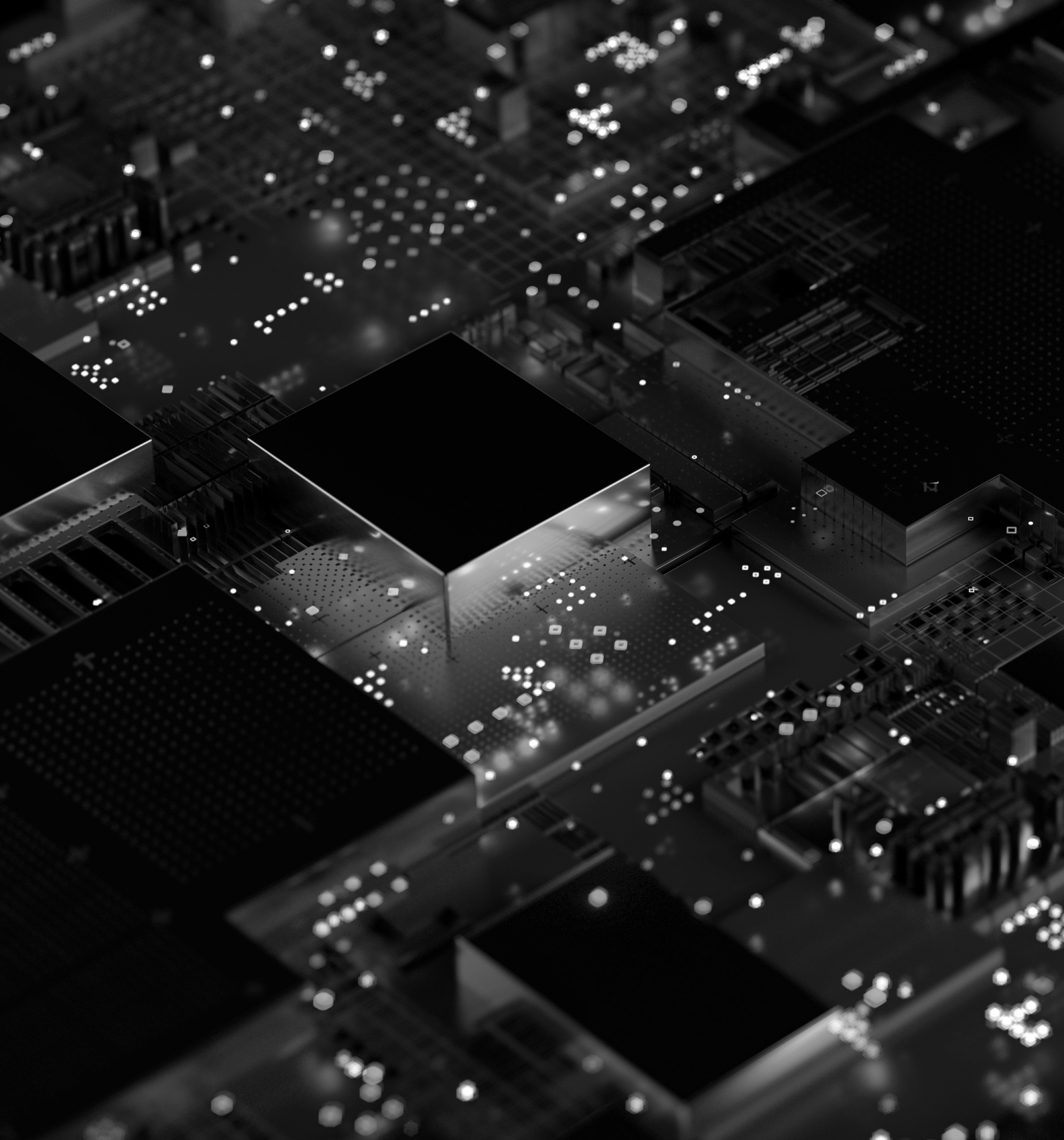
- 97 Max Smeets, “The strategic promise of offensive cyber operations.” *Strategic Studies Quarterly* 12, no. 3 (2018): 90-113.
- 98 Basma Khalil, “India’s ISR Capabilities: Implications for Pakistan”, *Eurasia Review*, April 24, 2020, <https://www.eurasiareview.com/24042020-indias-isr-capabilities-implications-for-pakistan-oped/>
- 99 Basic Doctrine of the Indian Air Force, Indian Air Force, Air Headquarters, New Delhi 2012, <https://www.scribd.com/doc/109721067/Basic-Doctrine-of-Indian-Air-Force-2012-PDF#>
- 100 Arindrajit Basu, *India’s International Cyber Operations: Tracing National Doctrine and Capabilities*, United Nations Institute for Disarmament Research, (UNIDIR), December 16, 2022, <https://www.unidir.org/cyberdoctrines/India>.
- 101 Basu, *India’s International Cyber Operations: Tracing National Doctrine and Capabilities*.
- 102 Herbert Lin and Amy Zegart, “Introduction”, in *Bytes, Bombs, and spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart, (Washington, D.C.: Brookings Institution Press, 2019), pp. 14-15.
- 103 Carol Upadhya, and Aninhalli Rame Vasavi. *In an outpost of the global economy: Work and workers in India’s information technology industry*. Routledge India, 2012.
- 104 Rising Focus on Cybersecurity in India. <https://www.ibef.org/blogs/rising-focus-on-cybersecurity-in-india>; Dharmaraj, Samaya. *India Cybersecurity Industry Grows Significantly Amid Pandemic* <https://opengovasia.com/india-cybersecurity-industry-grows-significantly-amid-pandemic/>
- 105 Basic Doctrine of the Indian Air Force.
- 106 Indian Army. 2018. *Land Warfare Doctrine*, March 11, 2023: <https://www.ssri-j.com/MediaReport/Document/IndianArmyLandWarfareDoctrine2018.pdf>.

About the Authors

Kartik Bommakanti is Senior Fellow at ORF. **Yogesh Joshi and Karthik Nachiappan** are Research Fellows at the Institute of South Asian Studies, NUS. **Shimona Mohan** is a Research Assistant at ORF. **Antara Vats** is a former Junior Fellow at ORF.

Cover image:

Back cover image: Getty Images/Andriy Onufriyenko



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**