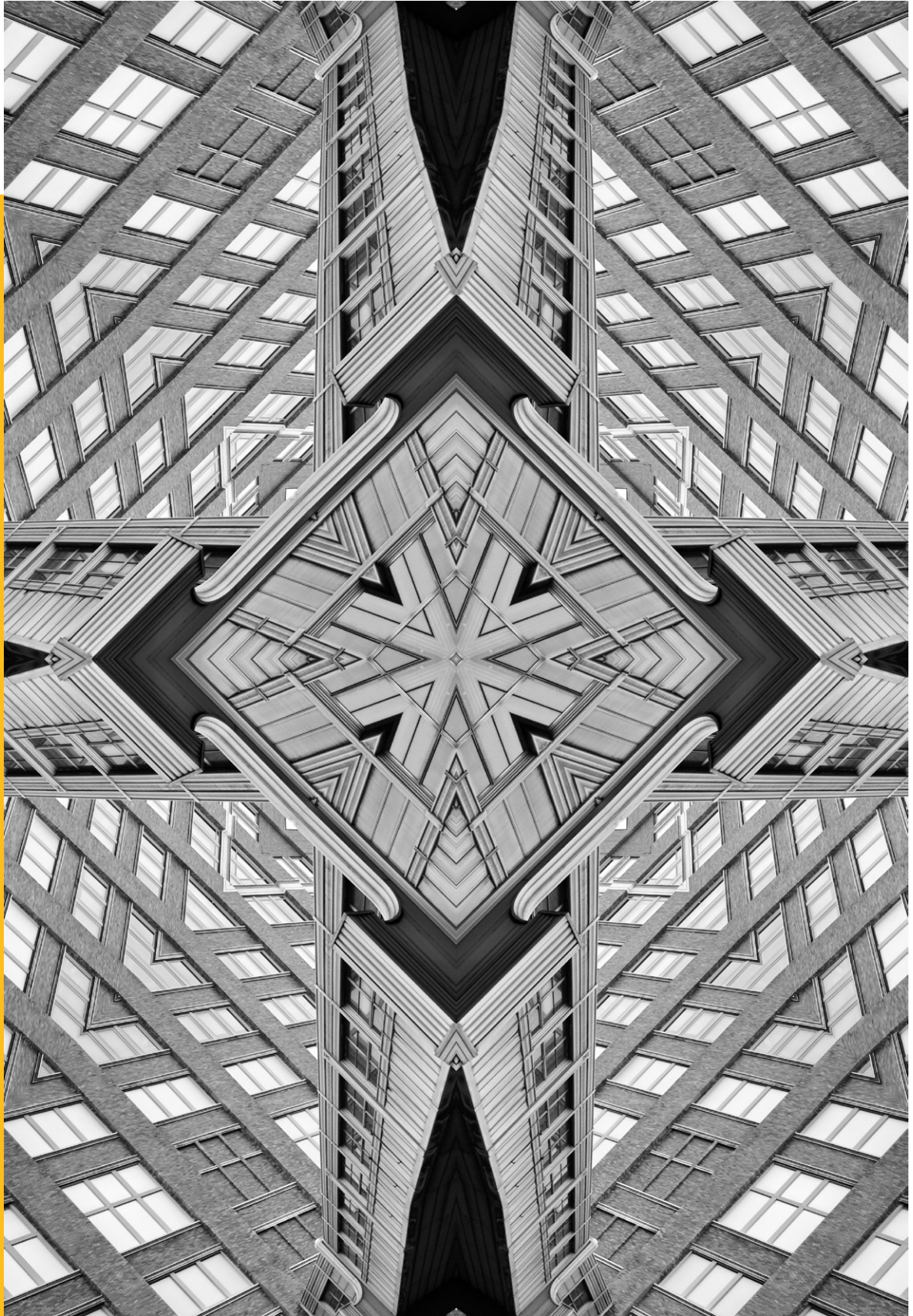


Occasional Paper



ISSUE NO. 390 FEBRUARY 2023

© 2023 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.

Amid Changing Nature and Character of War, the Need for Tech-Oriented Military Commanders for India

Akshat Upadhyay

Abstract

It has historically been assumed that while the nature of war remains the same—i.e., violence inflicted on the adversary to bend them to one's will—the character of warfare changes with technology, organisation, politics and culture. This notion has changed. Over the past decade, the nature of war has also changed, with increased use of non-contact and non-kinetic modes of warfare expanding the battlefield spatially and temporally. Defined periods of war and peace have been substituted by a competition continuum where adversaries aim less for destruction and more for disruption. Dual-use technologies that are cheap and diffused, have been key in this shift. In the changed milieu, it is imperative for the Indian armed forces to cultivate a class of technology-capable commanders who not only understand the latest technologies but also have the creative bandwidth to utilise them for innovative counters against adversaries.

The Changing Nature and Character of War

Theorists attempting to categorise changes in warfighting over time, refer to ‘generations’ of warfare.¹ The first generation emphasised massed manpower and line-of-column tactics; the second involved machine guns and indirect fire; the third introduced manoeuvre and combined-arms warfare; and the fourth involved non-state adversaries. The current fifth generation is characterised by non-kinetic military actions such as disinformation, cyber-attacks and social engineering, as well as the use of artificial intelligence (AI) and autonomous systems.²

There is an inherent assumption, related to the etymology of the word ‘generation’, that each one leaves behind the previous warfighting techniques and modes. Events of the previous decade, however, have shown that these generations bleed into each other. The Armenia-Azerbaijan conflict, Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF),^a and the ongoing Russia-Ukraine conflict have reinforced this view. Attrition warfare has combined with counterinsurgency operations, the use of technologies such as unmanned systems and combat biometrics, and cyber-attacks and disinformation to create a chaotic ‘battlefield’. The past several years have also shown that the relationship between warfighting and the achievement of political objectives has become tenuous. It may not be possible to totally achieve military objectives such as attrition of the adversary’s war-waging potential or occupation of territory, and in turn, they are inadequate for achieving the desired political objectives. Cooperation and conflict are almost co-existing with each other. The case of the US and China, India and China, and other dyads reinforces this notion.

As a result, two parallel ways of waging warfare are being conceptualised: non-contact and non-kinetic. Non-contact warfare comprises the use of long-range vectors such as rockets and missiles, electromagnetic (EM) spectrum, unmanned aerial systems (UAS) and cyber-attacks; meanwhile, non-kinetic operations include the use of disinformation through social media, export controls, propaganda, and cyber-attacks.^b These methods all use technology, specifically based on the collection, collation and analysis of data, advanced semiconductors, AI, and encrypted communication.

a Operation Enduring Freedom (OEF) was launched in the aftermath of the 11 September 2001 attacks against the United States. This was a name given both to the operations in Afghanistan (2001-2021) and the larger global war on terrorism (2001-2013) though some security scholars contend that it is still going on. Operation Iraqi Freedom (OIF) (2003-2011) was initiated as a conventional war campaign by the US military against the regime of Saddam Hussein on the charges of the regime possessing weapons of mass destruction but was later converted into a counter-insurgency campaign in the aftermath of Saddam’s downfall. The Armenian-Azerbaijan conflict was fought by the armed forces of both countries over the disputed territory of Nagorno-Karabakh and started in May 2021.

b Cyber attacks are common to the two because they can impact both the physical and virtual domains.

The Changing Nature and Character of War

Today entire societies are at risk from the increasing weaponisation of erstwhile civilian domains—i.e., trade, interpersonal communication, cognition,³ and economic interdependence.⁴ The risks also emanate from the pervasive nature of data-dominant technologies and the absence of well-defined battlefields. Indeed, the nature of warfare has not *changed* so much as it has become *diffused*. Violence has moved from the physical domain to become more structural, targeting the cognitive vulnerabilities of a state, including political decision-making processes, while exploiting fault lines within the country and fomenting mistrust between the government and the citizenry. Dealing with these changes requires military commanders who are equipped with knowledge of technology and who can recognise that future challenges may not always be solved using old templates. These commanders should have the mental flexibility and capacity to nurture effective junior leadership and create innovative warfighting solutions based on a nuanced understanding of the latest technologies. This will include doctrinal, organisational and most importantly, cognitive changes within the military leadership.

The context is that India is surrounded by two neighbouring and potentially collusive adversaries with revisionist tendencies. It also faces non-traditional challenges in the security domain, including climate change, disinformation, unstable supply chains, and terrorism. Some security scholars are of the view that India's ultimate aim may be to function as the 'third pole' in a transitory international system with the United States and China.⁵ While this is not a declared position, it is an emergent one visible in India's actions on the world stage: it protects its national interests while assisting other countries in healthcare, education, food grains, security, and digital governance. This position faces challenges for which the armed forces are bound to play a crucial role.

Much of the military threat is undergirded by technologies, especially data-dominant ones such as AI and cyberattacks; manipulation of the electromagnetic (EM) spectrum; long- and short-range missiles, and unmanned systems; and space-based intelligence, surveillance and reconnaissance (ISR) systems. It has never been more critical to fill the ranks with military personnel who not only have a grasp of emerging and niche technologies but also possess the creative bandwidth to make use of them for innovative solutions to counter adversaries. Additionally, structural changes are required within the Indian Armed Forces to make them better prepared for ongoing and future periods of conflict. This is particularly important given that the nature of emerging technologies puts flat, decentralised and modular organisations in the best position to take advantage of these technological innovations. The successful conduct of future warfare will hinge on rapid communication, near-instant decision-making, concerted

The Changing Nature and Character of War

application of firepower without necessitating the physical aggregation of military forces, the use of non-kinetic tools, and precision-targeting. All these attributes require a relatively flat organisation where the generation of options and decision-making is done—amid the presumed denial of communication—in an accelerated time frame, apart from being theatre-specific (modular) and autonomous (decentralised).

Are the Indian Armed Forces ready for this change? In terms of technology utilisation, the three services are not homogenous. While the Navy and Air Force are far more technologically oriented due to their nature—dealing with weapon systems and platforms—the Army is today attempting to induct technologies within its folds. Analysing the future battlefield and the requirement of attendant changes in the conceptual, doctrinal and operational domain through the prism of the Indian Armed Forces, this paper will offer suggestions for a new outlook towards warfighting.

“The nature of warfare has not *changed* so much as it has become *diffused*. Violence has moved from the physical domain to become more structural.”

The Use of Technologies in Warfare

The first concept requiring clarification is ‘war’ itself. There is a near-unanimous consensus that ‘war’ refers to the use of violence by a state to attain certain political objectives. There are, however, certain qualifications to this simple definition. This image of ‘conventional’ or classical war, is a “mental and theoretical juxtaposition of two unrelated events—Westphalian pre-nation-state war between kingdoms and; the globe-spanning First and Second World wars fought between nations—which have mingled with each other to create a static image of a catastrophic act that is extremely violent and comprises a universally structured and hierarchical model.”⁶ The gap between such wars is called ‘peace’.⁷

This conceptual model of war prevails in most militaries, including that of India. In this model, there is a clear distinction between war and peace, where war, at least theoretically has an initiation and termination phase, at the end of which diplomacy comes into play for bargaining over territory or solving previously entrenched disputes. This is very much a territorial approach influenced by the industrial era where territory forms the crux of fighting and bargaining. This model also involves a series of battlefields—a geographically defined territory where opposing sides clash for domination or occupation. Bean-counting and the use of platforms such as tanks, aircraft, air defence weapons, and mechanised platforms decide the outcome through an attritional mode of fighting. In the attrition mode, key factors include the industrial heft of the opposing sides, the level of professionalism and training of opposing armies, and the political intent of the leadership.

In recent years, a number of political-economic factors limiting the size of armies worldwide⁸ and the ‘precision revolution’⁹ have shrunk the military battlefield, and the rise of the internet of things (IoT) supplemented by 5G communications has expanded the ‘war-zone’. Entire societies are engaged in an ‘invisible’ war of information and influence.¹⁰ A paradigm shift has occurred: War now forms part of a continuum of conflict and confrontation, rather than occurring at a specific day and time—and ending similarly, too—since the physical battlefields have merged with ‘war zones’ in civilian life. The use of conventional platforms such as tanks, manned aircraft and mechanised platforms, needs to be enhanced through the use of advanced ISR, improved communication tools, and coupling with unmanned systems. Combined-arms operations need to now involve not only ground and mechanised forces but also the air, maritime, cyber, cognitive domains and the electromagnetic spectrum. The ongoing Russia-Ukraine war has shown that combined arms operations have become critical in armed conflicts and need to be supplemented by information warfare, unmanned systems, and cyber-attacks.

The Use of Technologies in Warfare

Warfare has now expanded to cover grey-zone operations,^{c,11} multi-domain operations,^{d,12} and New Generation Warfare (NGW).^{e,13} The focus, through the effective use of technological innovations, is to employ non-contact and non-kinetic means to ensure that the opposing side is entangled within its own societal and organisational vulnerabilities rather than focusing on the adversary. While grey-zone operations intend to attain political objectives through operations other than war, and putting the proverbial ball in the opponent's court to force them to either capitulate or risk a larger conflict—multi-domain operations attempt to combine the traditional warfighting domains of land, air and sea with new ones such as space, EM spectrum, cyber and cognition to disable the enemy's critical infrastructure. NGW, which combines a host of kinetic and non-kinetic means of warfighting, is used to subjugate the enemy's will even before the adversary has time to decide on the relevant course of action.

The roots of the grey-zone strategy are in the United States' (US) activities in Latin America in the 1960s, '70s and '80s which included the Contra scandal, and the failed invasion of the Bay of Pigs by Cuban paramilitaries armed by the alleged US deep state.^{f,14} Subsequently, 'Color Revolutions' and the Jasmine Revolution in West Asia have also been considered part of hybrid warfare.^{g,15} Russia views all these actions as part of the American strategy to impose its favourable political solution over weak states without declaring war against them. Similarly, during the initial phase of its operations against Ukraine in 2014, Russia used a sophisticated template against Ukraine,¹⁶ by combining fire assaults, referendums, surveys, cyber-attacks, the use of troll farms, special forces ('little green men') and armed dissidents, along with conventional economic and political coercion to annex Crimea, prevent the overthrow of the pro-Russian Ukrainian president, deliver warnings to the fringe states in the Baltic, and create an imbalance in its erstwhile area of influence.¹⁷ Similar techniques, especially the use of cyber-attacks and influence operations, were

c These are operations short of war or undertaken below the conventional definition of warfare for achieving political objectives.

d Conducting operations in the physical, cognitive and informational domains.

e A Russian-origin strategy that looks at waging war holistically using all coercive instruments at the disposal of the state, including non-military ones.

f The Contras were a collection of right-wing rebel groups in Nicaragua active from 1979 to 1990 who were supported and supplied by the US to counter the Sandinista junta in Nicaragua. The Bay of Pigs invasion was a failed military landing invasion of Cuba by paramilitaries backed by the US which was aimed at overthrowing the regime of Fidel Castro.

g The term 'Colour Revolution' has been used by the media since 2004 to describe a series of anti-regime protest movements initially in post-Soviet Eurasia and later in different parts of the world. The Jasmine Revolution was a popular uprising by youth across a number of Arab states in response to growing inflation, unemployment, muzzled freedom of speech, and degrading conditions of living. It started in Tunisia and later to spread to other countries including Egypt, Yemen, and Saudi Arabia.

The Use of Technologies in Warfare

used against Estonia¹⁸ and Georgia. Without committing the entire might of its armed forces or resorting to physical aggression—something that is prohibited explicitly by international law—Russia was able to impose a political condition that was favourable to it.

The term ‘grey-zone operations’ can be misunderstood. Influenced by the Chinese interpretation of the ‘grey zone’, as captured in its ‘Three Warfares’ strategy,¹⁹ some military analysts attribute certain activities to the Armed Forces which are conducted by other state agencies or branches. However, ‘grey-zone’ operations are not the same as ‘grey’ operations. The Chinese state will have its own taxonomy because it does not distinguish between the Party and the State, and the People’s Liberation Army (PLA) is an armed component of the Chinese Communist Party (CCP) and not the Chinese state. Therefore, they regard public opinion warfare and legal warfare as part of military operations.²⁰

For democracies, there is a clear distinction between political parties and the state structure, with the Armed Forces generally answerable to the Constitution or the Constitutional Head of the nation. This separation of mandate normatively creates constraints around the kind of activities permitted to the Armed Forces. In other words, there is usually a fixed operational mandate for the Armed Forces in terms of areas, responsibilities and influence. The military’s role in democracies the world over has expanded though the primary goal remains conventional operations. Climate change, cyber warfare, influence operations, and other non-traditional security challenges pose a dilemma since they do not involve solutions for which the armed forces are generally equipped or trained. This is where technology becomes crucial. Owing to its inherent dual-use nature, technology is the bridge that connects the armed forces to solutions against non-traditional threats. It is in this context that the role of tech-oriented commanders in the Indian Armed Forces becomes critical, both for introducing these technologies and inculcating a scientific temperament and proclivity to use complex systems.

In their current form, the Indian Armed Forces are armed, trained and equipped for conventional operations and have limited options to respond to grey-zone operations. While the Indian Army has had considerable success in counterinsurgency (CI) and counter-terrorism (CT) operations in the union territories of Jammu and Kashmir (J&K) and the North East regions, the warfighting part is still conducted using conventional weaponry. Domains such as space, information and EM spectrum are deemed peripheral to conventional operations. This creates a dilemma. In certain instances, the conventional combat potential of the Armed Forces fails to provide adequate deterrence against the use of grey-zone operations by the adversary, imposing a decision dilemma. How should they respond to non-kinetic operations using kinetic

The Use of Technologies in Warfare

tools? The Indian Armed Forces, therefore, require tailor-made operations to respond to emergent scenarios which also include non-kinetic operations. The wide spectrum of threats detailed so far require military personnel, especially in the hierarchy to realise that technology-enabled solutions will need to be given primacy in the future battlespace.

This paper is not arguing that conventional platforms be discarded in favour of purely digital solutions; rather, that technology and its attributes need to be at the centre of planning for future operations. This entails a cognitive process that starts with the acknowledgement of vulnerabilities and capabilities and the gap between them, a keen understanding of the latest technologies and their potential, and finally, the context in which they can be utilised. A leader well-versed in technology also recognises the need for a specialised cadre of technically proficient officers and soldiers who can provide technical solutions, which can then be amalgamated into bigger solutions through coordination and integration. Finally, a tech-capable commander creates the bridge between emerging technologies, conventional capabilities, and a changing context under which war has to be waged.

While commenting on the role of emerging technologies, it is pertinent to recognise that traditional warfighting has not ended, though its importance in conflict termination has reduced. Information operations will dominate every stage of the conduct of kinetic operations (initiation, conduct and termination) since they have the potential to create instability in the target country. The US assassination of Iranian General Qasem Soleimani in 2020²¹ and Iran's retaliation by targeting an American base in Iraq using missiles,²² are examples of kinetic operations manifesting an information effect. Both the countries' leaderships could convey their resolve to their respective domestic audience without going to war with each other. Indian commanders need to look at technological solutions to take the fight to the enemy, by focusing on its will to fight, not just on military victories on the battlefield but also on the cognitive and information domains.

“Owing to its inherent dual-use nature, technology is the bridge that connects the armed forces to solutions against non-traditional threats.”

The Military Uses of Technologies

Technology is generally defined as the application of scientific knowledge to the practical aims of human life or to the change and manipulation of the human environment.²³ This is why ‘science’ and ‘technology’ are spoken about in tandem—i.e., S&T. Nurturing an innovative technological ecosystem requires a robust scientific base, both in practice and temperament. In contemporary times, when military leaders and analysts refer to ‘technology’, they refer to a host of technologies, specifically computing and miniaturisation for information operations, ISR, joint and autonomous fires and battlefield transparency (BFT), propulsion and communication for unmanned systems, and robotics and metallurgy for airframes and chassis. ‘Emerging technologies’, meanwhile, are a set of technologies that are identified by radical novelty, relatively fast growth, coherence over time, prominent impact across several sectors, and uncertainty and ambiguity about utility.²⁴ These would include AI, 5G communications, quantum computing, blockchain, computer vision, bioengineering, and modular nuclear energy. While these have myriad uses in the civilian domain, their utility for the military is still evolving. The success of their military use will depend on factors such as scalability, commercial viability, cost of R&D, technical complexity or ease of use, and compatibility.

The Indian Armed Forces have a long history of fighting both conventional and sub-conventional wars. The use of technologies by non-state and proxy actors—such as trafficking arms, counterfeit currency and illicit drugs using unmanned aerial vehicles (UAVs),²⁵ and attacking airbases—²⁶ is a relatively recent phenomenon. Social media platforms and encrypted applications have also begun to be used for radicalisation activities and for conducting attacks against security forces and civilians by allowing for coordination in real-time.²⁷ This has the potential to divert the forces from their primary aim of conducting counterinsurgency operations in areas such as Kashmir, while creating further instability in an already fragile societal landscape.

Pakistan, for example, has an indigenous drone industry that manufactures cheap drones used to drop illicit drugs and counterfeit currency across the border in India.²⁸ While the Pakistan Army continues to adhere to a ceasefire along the Line of Control (LOC), it has used influence operations in Europe and North America, fanning propaganda and disinformation against India.²⁹ China provided Pakistan with specific platforms and technologies such as advanced drones (CH-4B), submarines, air defence (AD) systems and frigates and fighter aircraft, apart from digital technologies such as AI and EW capabilities.³⁰ The Pakistan Air Force has also established a Centre of AI and Computing (CENTAIC) with Chinese support.³¹ On the LAC, China has developed significant techno-military capabilities that have been documented by the media.³² China has also waged information warfare against India³³ and has allegedly conducted cyber-attacks against civilian facilities.³⁴

The Military Uses of Technologies

All these activities point to a hybrid scenario where India will face multiple conventional and unconventional threats in the medium- to long-term future. Key in acting on these threats is a well-known and oft-used philosophy in the Armed Forces across the world—i.e., the Observe-Orient-Decide-Act (OODA) loop created by Pentagon consultant John Boyd. Since the Indian commanders are adequately trained and aware of the nuances of the OODA loop, it becomes an ideal model for conceptualising how technology can be used for empowering the commanders. In examining the loop, one can also examine how it can be modified or even done away with when dealing with new threats.

OODA Loop

The OODA loop is the go-to paradigm for certain militaries in the world, including India's.³⁵ The concept itself is straightforward: When facing an adversary, an individual fighter goes through a sequential process that starts with the observation of a threat; orienting oneself to react to the threat; deciding the course of action out of several options; and finally, acting on the threat. In a simple case scenario of two opposing individuals, the one who goes through their OODA loop faster will emerge as the winner. The simplicity of this concept lends its use in bigger and higher decision-making scenarios—at the operational and even strategic levels.

The first step—i.e., Observe, is the most crucial and one which all users of technology should be capable of. It is necessary to recognise the threat before proceeding with the desired course of action. Unmanned systems for perimeter patrolling, AI-based image and motion detection systems, multiple ground-based infrared (IR), acoustics, light detection and ranging (LIDAR) sensors and satellite imagery, combined with conventional radars and human intelligence (HUMINT) will be responsible for the physical domain. These need to be fed into a data mining, aggregation and fusion software for generating options for the next stage. AI-based cyber monitoring systems will be required for the cyber domain, while in-house designed algorithms will scan for probable disinformation and fake news proliferation. The Observe part should therefore have three components for the three war domains: a comprehensive plug-and-play module that combines inputs from all sensors, devices and HUMINT for the physical domain; cyber monitoring systems for the cyber domain; disinformation monitoring systems for the cognitive domain.

The second part, i.e., Orient—has a far more expansive interpretation at the operational, strategic and national security levels and also the most critical: How is observation translated into a threat scenario? This requires the development

The Military Uses of Technologies

of a perspective through which the data from the first phase is filtered and contextualised such as culture, organisation, and threat perception. In terms of technology, it can be achieved by creating suitable algorithms. These will require training data which has been adequately labelled, cleaned and standardised. Therefore, the OODA loop has to be modified. Since the variety of threats may require coordination with other departments and agencies of the government apart from private players, this stage should instead be called ‘Coordinate and Orient’.

The third part i.e., Decide is where multiple courses of action are generated for the decision-maker. A robust decision support system (DSS) is therefore necessary at this stage. AI-based systems combine inputs from sensors and HUMINT and generate options for the decision-maker. The Decide phase needs to be supplemented by an additional Integrate phase as it is here that the relevant instruments in various domains will be integrated. The fourth and final stage is Act, which now needs to be replaced with Delegate. After the Delegate phase, there will be multiple actions occurring at the tactical levels. This is where the need for tech-capable commanders is most critical. Since the tempo of operations and decisions required may saturate the cognitive capacities of the commanders, it is necessary to decide which parts can be automated, which should be delegated, and finally, where human intervention is necessary. The transition from Delegate to Act will require two qualities: enabling autonomous actions and excellent professional military education (PME) which emphasises questioning established paradigms and devising unique solutions. Tech-capable commanders, through their understanding of technologies and their contextual utility, can empower their command and ensure that the Indian Armed Forces are able to conduct operations in the competition continuum.

“The success of the military use of emerging tech will depend on scalability, viability, R&D cost, ease of use, and compatibility.”

The Military Uses of Technologies

Technological leadership

Understanding technology is part of the puzzle of preparing for and fighting future wars. Acknowledging and implementing the structural changes brought by technology is a different ball game altogether. Who is (are) more qualified to oversee transformational changes in a military organisation? This question is at the root of determining what ‘good leadership’ means for the Armed Forces today. To be fair, leading soldiers in battle, issuing instructions and directives, facilitating two-way communication, and tolerating and eventually assimilating dissent—are all tasks of leadership. Generalship or tech-capable leadership at the operational or strategic level involves providing a free space for junior leaders to act at the tactical level.

This is a delicate game of centralisation and decentralisation in tandem. Centralisation is required for converting political objectives to military ones, ensuring the provision of adequate resources and technology, understanding the nature of the threat, and providing the broad intent and direction under which the warfighting has to be done. These requirements have become more critical in dealing with the continuum of competition where the lines between war and peace have become blurred. Decentralisation is required for conducting campaigns at the lower levels. For example, influence operation campaigns are region-specific, at the very least, and require decentralisation for successful conduct. Similarly, climate change effects will manifest in different ways across India’s varied topography. It is the local commanders on the ground, equipped with the latest technology and authority to coordinate with other agencies, who will be able to make calibrated decisions.

This recalls the question: Who is (are) more qualified to oversee transformational changes in a military organisation? Given that it is assumed that a military ‘has’ power, there is less focus on *how* it generates power, how that relates to battle effectiveness and finally, which of the individual or combination of factors leads to an outcome favourable to a particular organisation. Is it battle procedures, weapons, techniques, quality of personnel, organisation, or something else?

The litmus test of military leadership lies in deciding on and creating optimal force structures that can function effectively for a sustained time period in ensuring that the Armed Forces remain effective instruments for achieving national interests. Since national interests are dynamic, military leadership has to play a critical part. Should that leadership be a generalist or skewed towards the technocrat? Again, this is a subjective view but at the highest level, the leadership needs to be a generalist with a special cadre or corps of officers

The Military Uses of Technologies

and rank-and-file who are experts in their domain. This generalist leadership, however, has to undergo periodic military education capsules and orientation so that it is in touch with the latest technologies and geopolitics. With warfare now hinging on information warfare (IW), AI, machine learning (ML), quantum computing and other niche technologies, a class of professionals in domains such as linguistics, cryptography, geology and data science needs to be nurtured and incentivised to remain.

This is where the role of military education, cross-postings, and civil-military interactions for enhancing jointness and inculcating a more mature military leadership cognisant of emerging challenges comes into play. Many academic studies on military innovation and technology transfers have stressed the fact that separate pathways need to be created for selected officers, based on their professional acumen, innovativeness, or technological proficiency to incubate a culture of military innovation and ensure that technologies and doctrinal changes are scaled up and made available to the cutting edge.³⁶ Competent officers have to be nurtured by the leadership from an early stage, based on skills rather than hierarchical structures and conventions.

The conventional military way of responding to threats is training—repeating step-by-step ways of responding to challenges that follow a template. This would have worked till the ‘80s and even the ‘90s. In an era, however, when even the nature of the threat is ambiguous, relying solely on training may not be adequate. Military education, therefore, has to inculcate an attitude of logic and reasoning, by questioning inherent assumptions. Personnel must ask *Why*, rather than *How*. It is only in responding to the *Why* that innovative solutions can be devised. The age of large-scale manoeuvres is passé and ‘command’ per se has morphed into managing new-age technology-driven warfare. How must leadership evolve? The model today is Competition (decisive victory uncertain) rather than Confrontation (conventional warfighting paradigm).

“The litmus test of military leadership lies in deciding on and creating optimal force structures that can function effectively for a sustained time period.”

Handling New-Age Warfare

War has become less concentrated and more spread in terms of space and time. Erstwhile purely civilian domains such as agriculture, trade, finance, and resource sharing, have been securitised and weaponised. Induction of technology means the involvement of more civilians—much more than the current model of interaction with agencies such as the Defence Research and Development Organisation (DRDO) or the Directorate General of Quality Assurance (DGQA)—in the workings of the military, and in turn, coordinating with them becomes a more complex task. Examples include issues of data standardisation, cyber security, and autonomy in unmanned systems. The re-classification of information needs to be a priority. In all three services, most information is classified, creating challenges for civilian startups for AI solutions since the training of algorithms requires real-time data rather than the one generated synthetically. For example, if a certain AI algorithm needs to be trained to identify differences between consecutive real-time satellite maps of a certain area, it needs to be trained on the same rather than depending on training or synthetic data.

The current rules do not allow a seamless transfer of information between the military and civilian domains. With the privatisation of geospatial intelligence,³⁷ space startups,³⁸ and the proliferation of open-source intelligence (OSINT),³⁹ there is a need to rethink what is considered confidential and what is not. Increasing use of technology within the armed forces also requires closer coordination between them and their civilian counterparts—in academia, think tanks, industry, and other ministries. This achieves a two-fold aim: amortisation of the cost of using the technology across the military and civilian fields, especially for technologies and platforms with possible dual purposes such as unmanned systems, AI and data management systems; and ensuring impetus to indigenisation through optimisation of commonalities between the two domains. The establishment of industry groups and consortiums is one of the examples through which this can be achieved.

“Erstwhile purely civilian domains such as agriculture, trade, and resource sharing, have been securitised.”

Lessons from the Russia-Ukraine War

The ongoing conflict between Russia and Ukraine provides certain lessons in the use and importance of weapons platforms and technologies that may prove useful in the Indian context and thus frame the debate on how these can be absorbed by tech-capable commanders for future wars.

The era of long slogs

The conflict has provoked a classic dilemma: Is the era of long slogs back or not? The ongoing conflict demonstrates the futility of conventional combat in achieving political aims. Seen from the perspective of the West, small unit tactics, high-technology and defensive weapons such as anti-tank guided missiles (ATGMs) have led to an effective Ukrainian fightback against superior Russian forces.⁴⁰ These have been supplemented by emerging forms of intelligence, surveillance, target acquisition and reconnaissance (ISTAR) such as UAVs, private satellite constellations such as Starlink⁴¹ and the use of AI tools of companies like Palantir⁴² and Clearview.⁴³

The second phase of the fight, however—a likely Ukrainian offensive in the spring of 2023—requires the use of offensive weapons such as tanks, a key reason for dissonance within NATO and with the US.⁴⁴ Additionally, Russia is reported to have used drone swarms in targeting Ukrainian civilian and telecommunications infrastructure.⁴⁵ The aim is to destroy civilian morale and stop the use of IW by the Ukrainians. The conflict again proves that the line between the military and civilian has been erased and technology remains the bridge between the two.

Need for civilian teams

Certain civilian teams can be embedded with leading formations for testing their prototypes in real-time, similar to the Bayraktar model.⁴⁶ The necessary level of tactical coordination between the soldiers and the civilian experts requires educated and technologically proficient soldiers. By selecting soldiers for fighting future warfare, especially in the light of the Agniveer scheme, which affords the country a once-in-a-lifetime opportunity to create a technically proficient army, tech-oriented commanders can lead the way.

‘Contested equalities’

The conflict between Russia and Ukraine can also be termed as “contested equalities” wherein the Russian Armed Forces are in confrontation with NATO, through the proxy of Ukraine. Most armies in the West, following their Fulda

Lessons from the Russia-Ukraine War

Gap moment^h have mentally prepared themselves for asymmetric warfare,⁴⁷ conventionally and unconventionally. The Ukrainian battleground places Russian forces in direct opposition with American and Western Europe's industrial capacity, along with an assortment of capabilities and platforms. The Ukrainian soldiers have to contend with weapons systems from Eastern Europe similar to their Russian adversaries, German armoured personnel carriers, American drones, and French artillery guns, among others.

The requirement of incorporating different systems during wartime with differing technologies under a common command and control system requires flexibility at the junior level, with broad operational guidance and standardisation norms effected at the political-strategic level. This means that the requirement for techno-leadership is greatly increased. As the Indian Armed Forces scale up their capability in terms of platforms and technologies, the top leaders in the Indian military need to focus on certain foundational issues: issuance of standardisation metrics for all services for emerging technologies in concert with relevant partners; ensuring civilian-military integration for selected technologies so that companies can experiment and fail or succeed fast and finally; and creating relatively modular and flexible organisations.

Effective use of disruptive tech

Disruptive technology used conventionally fails to disrupt or work efficiently. Technologies are meant to flatten—i.e., destroy silos and demolish hierarchies. Using them in the same layered manner renders them ineffective. To obviate this difficulty, tech-capable commanders must understand the nuances of the technologies in detail so that novel uses can be generated. One of the ways is regular interactions with academia and think tanks. At the same time, junior leader innovation should be encouraged and initiatives by the Department of Defence Production (DDP) like iDEX4Fauji⁴⁸ should be given more impetus. Laboratories of government institutes and startups can be provided to these soldiers so they can incubate their ideas and if found feasible, given possible support for further scaling. Techno-commanders can facilitate this transformation.

^h The Fulda Gap moment is a mindset that is symbolised by plans by NATO during the Cold War for conventional warfare with the then-Soviet Union. Fulda Gap represented the shortest route between the East-West German border to the Rhine river and where maximum forces of both blocs were concentrated.

War and politics

The relationship between war and politics in terms of achieving desired political objectives is not as watertight as it used to be pre-Second World War. The advent of nuclear weapons led to the use of proxy wars, information warfare and precision weaponry to increase the intensity and reach of warfare to cover all instruments of state. The mentality of fire-and-carpet bombing—which considered the civilian population fair game—was extended to the emerging domains of warfare. This meant that more and more domains became weaponised.


What is happening today is a spinoff from the same strategic reality. Since outright victory is not possible—despite what one may say about warfare and what is happening in the Russia-Ukrainian conflict—actors tend to gain one-upmanship in small bursts of intense conflicts using both kinetic and non-kinetic tools. The losing side recoups its losses to prepare for the next round, looking for both partners and capabilities. In effect, the preponderance of conventional weapon platforms in the conflict has underscored the futility of conventional warfare as an effective tool for achieving the political-military goals of a state. What we see today is an era of all-pervasive competition. Tech-oriented commanders need to understand this new reality and ensure that relevant capabilities are built up, scaled and utilised in increasingly short bursts of competition.

One model is: Leadership 1.0 (one-way command, loudspeaker-style leadership, charge of the light brigade) -> Leadership 2.0 (2-way discussion, dissent) -> Leadership 3.0 (managing conflicts, managing new era soldiers and technology)

Challenges are going to be unfamiliar; senior generals need to understand and acknowledge that they might not be able or aware of emerging challenges, new technologies and newer adversaries. They need to understand, respect and assimilate the expertise of others, including juniors and civilians. There will be 24/7 operations not of the vintage era but with different requirements. The ubiquity of smartphones and the ‘PubG syndrome’ⁱ are likely to impact junior leaders and tech-capable commanders need to be ready to mitigate the challenges of technology.

ⁱ ‘PubG Syndrome’ is a more specific form of a growing addiction to video games which threatens to divorce the players from real life and adversely affect their cognitive, social and intellectual capabilities.

Today's military strategies are designed to create an optimum environment for politics to play out. Unlike in earlier eras, a 'strategic pause' is the best that one can achieve, as even the United States learnt first against Iran, and then the Taliban. The Indian defence establishment, therefore, needs to utilise and leverage emerging technologies to create cognitive dissonance in the adversary ranks, while generating adequate situational awareness if it is being targeted, and take defensive measures.

The focus should be on revising the hierarchical models within the forces which prevent rapid and decisive actions commensurate with the speed of the war being fought. The OODA loop needs to be reconfigured and a new system of PME that emphasises autonomous decision-making needs to be inculcated. Systemic, cultural and organisational changes coupled with technological ones need to be brought in an urgent time frame for Indian armed forces to dominate the competition continuum. The need for tech-capable commanders—officers who understand the changed environment, the expansion of warfighting to civilian domains, the nature and implications of digital technologies and who encourage and even cultivate a nature of dissent—has never been felt more acutely. 

Lt Col Akshat Upadhyay is a serving army officer. He is the author of *Coercive Diplomacy Against Pakistan (2018)*. He is a Research Fellow at MP-IDSA.

- 1 William S Lind, *Maneuver Warfare Handbook* (New York: Avalon Publishing, 1985), pp. 13.
- 2 Daniel H. Abbott, ed., *The Handbook of 5GW: A Fifth Generation of War?* (Ann Arbor: Nimble Books LLC, 2021).
- 3 Tzu-Chieh Hung and Tzu-Wei Hung, “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars,” *Journal of Global Security Studies* 7 (2022): 1-18.
- 4 Henry Farrell and Abraham L Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” *International Security* 44 (2019): 42-79.
- 5 Lt Gen PR Shankar (Retd), “The US-led global order is tottering. It is India’s time to shine as a balancing ‘third pole’,” *The Print*, November 14, 2022, <https://theprint.in/opinion/the-us-led-global-order-is-tottering-it-is-indias-time-to-shine-as-a-balancing-third-pole/1214758/>
- 6 Akshat Upadhyay, *Fighting Future Wars: Preparing India for Conflicts in the 21st Century*, New Delhi, Observer Research Foundation (ORF), 2022, <https://www.orfonline.org/research/fighting-future-wars/>
- 7 Donald Stoker and Craig Whiteside, “Blurred Lines: Gray - Zone Conflict and Hybrid War - Two Failures of American Strategic Thinking,” *Naval War College Review* 73 (2020): 1-18
- 8 Mick Ryan, “The West needs to boost its industrial capacity fast,” *Engelsberg Ideas*, November 24, 2022, <https://engelsbergideas.com/notebook/the-west-needs-to-boost-its-industrial-capacity-fast/>
- 9 David Zimmerman, “The Precision Revolution: GPS and the Future of Aerial Warfare,” review of *The Precision Revolution: GPS and the Future of Aerial Warfare*, by Michael Russell Rip and James M Hasik, Naval Institute Press, October 2004.
- 10 Huib Modderkolk, *There’s a War Going On But No One Can See It* (London: Bloomsbury Publishing, 2021), pp. 2.
- 11 Javier Jordan, “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict,” *Journal of Strategic Security* 14 (2020): 1-24.
- 12 US Army Training and Doctrine Command (TRADOC), *The U.S. Army in Multi-Domain Operations 2028*, by US TRADOC, Fort Eustis Virginia: 2018, https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028
- 13 Jānis Bērziņš, “The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria,” *The Journal of Slavic Military Studies* 33 (2020): 355-380.
- 14 Noam Chomsky, *American Power and the New Mandarins* (New Delhi: Penguin Books India, 2003), pp. 61.

- 15 Ofer Friedman, "On the Gerasimov Doctrine: Why the West Fails to Beat Russia to the Punch," *Prism* 8, no. 2 (2019), https://www.researchgate.net/publication/350632161_On_the_Gerasimov_Doctrine_Why_the_West_Fails_to_Beat_Russia_to_the_Punch
- 16 David E Sanger, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age* (New Delhi: Amaryllis, 2019), pp. 168.
- 17 David Carment and Dani Belo, *War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare*, Alberta, Canada, Canadian Global Affairs Institute, 2018, https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare
- 18 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011), <https://www.jstor.org/stable/26463926>
- 19 Geoffrey Till, *Grey Zone Operations: The Rules of the Game*, Singapore, Rajaratnam School of International Studies, 2022, <https://www.rsis.edu.sg/rsis-publication/idss/ip22023-grey-zone-operations-the-rules-of-the-game/#.Y8YQ-xBzMK>
- 20 Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks*, January 30, 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>
- 21 "Qasem Soleimani: US strike on Iran general was unlawful, UN expert says," *BBC*, July 09, 2020, <https://www.bbc.com/news/world-middle-east-53345885>
- 22 Amina Ismail and John Davison, "Iran attacks Iraq's Erbil with missiles in warning to U.S., allies," *Reuters*, March 14, 2022, <https://www.reuters.com/world/middle-east/multiple-rockets-fall-erbil-northern-iraq-state-media-2022-03-12/>
- 23 Britannica, "Technology," *Encyclopaedia Britannica*, <https://www.britannica.com/technology/technology>.
- 24 Daniele Rotolo, Diana Hicks and Ben Martin, "What is an emerging technology?," *Research Policy* 44, no. 10 (2015), https://econpapers.repec.org/article/eerespol/v_3a44_3ay_3a2015_3ai_3a10_3ap_3a1827-1843.htm
- 25 Vikas Vasudeva, "Captured 22 drones smuggling weapons, drugs across border in 2022: BSF," *The Hindu*, January 01, 2023, <https://www.thehindu.com/news/national/captured-22-drones-smuggling-weapons-drugs-across-border-in-2022-bsf/article66324442.ece>
- 26 Kamaljit Kaur Sandhu, "In a first, drones used to drop explosives on Jammu air base," *India Today*, June 27, 2021, <https://www.indiatoday.in/india/story/air-force-station-jammu-blast-drone-attack-suspected-1819895-2021-06-27>
- 27 "Terror groups in Pakistan switch to new messaging apps," *Times of India*, January 24, 2021, <https://timesofindia.indiatimes.com/india/terror-groups-in-pakistan-switch-to-new-messaging-apps/articleshow/80433381.cms>

- 28 Lt Gen VK Saxena (retd), *Pak UAV Capability - Poised for a Revamp*, New Delhi, Vivekananda International Foundation (VIF), 2019, <https://www.vifindia.org/article/2019/january/28/pak-uav-capability-poised-for-a-revamp>
- 29 Vaasu Sharma, "Information warfare : The Pakistan angle," *WION News*, August 29, 2022, <https://www.wionews.com/opinions/information-warfare-the-pakistan-angle-511155>
- 30 Gabriel Dominguez, "Pakistan receives five CH-4 UAVs from China," *Janes*, January 27, 2021, <https://www.janes.com/defence-news/news-detail/pakistan-receives-five-ch-4-uavs-from-china>
- 31 Pravin Sawhney, *The Last War: How AI Will Shape India's final showdown with China*, (New Delhi: Aleph Book Company, 2022), pp. 34.
- 32 "It is going on unabated': Army chief on infrastructure development by China along LAC," *Times of India*, November 12, 2022, <https://timesofindia.indiatimes.com/india/it-is-going-on-unabated-army-chief-on-infrastructure-development-by-china-along-lac/articleshow/95477242.cms>
- 33 Law and Society Alliance, *Mapping Chinese Footprints and Influence Operations in India*, New Delhi, Law and Society Alliance, 2021, <https://defence.capital/2021/09/04/law-and-society-alliance-study-report-exposes-communist-chinas-overt-covert-influence-operations-in-india/>
- 34 Kirti Bhargava, "Recent Cyber Attacks With Alleged Chinese Involvement That Targeted India's Critical Infrastructure," *India Today*, December 02, 2022, <https://www.outlookindia.com/national/recent-cyber-attacks-with-alleged-chinese-involvement-that-targeted-india-s-critical-infrastructure-news-241897>
- 35 Frans PB Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, (Oxfordshire: Routledge, 2015), pp. 10.
- 36 Moritz Weiss, "How to become a first mover? Mechanisms of military innovation and the development of drones," *European Journal of International Security* 3, no. 2 (2017), <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/how-to-become-a-first-mover-mechanisms-of-military-innovation-and-the-development-of-drones/F019C614AC1B902F63C413717123201C>
- 37 Juergen Dold and Jessica Groopman, "The future of geospatial intelligence," *Geospatial Information Science* 20, no. 2 (2017), <https://www.tandfonline.com/doi/full/10.1080/10095020.2017.1337318>
- 38 Sidney N Nakahodo and Steven Gonzalez, "Creating Startups with NASA Technology," *New Space* 8, no. 3 (2020), <https://www.liebertpub.com/doi/abs/10.1089/space.2020.0002>
- 39 Libor Benes, "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm," *Journal of Strategic Security* 6, no. 5 (2013), <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1298&context=jss>

- 40 Lt Gen HS Panag (Retd), “Ukraine-Russia shows us the future of war with high-end ATGMs, drones. India has to step up,” *The Print*, September 22, 2022, <https://theprint.in/opinion/ukraine-russia-shows-us-the-future-of-war-with-high-end-atgms-drones-india-has-to-step-up/1137854/>
- 41 “How Elon Musk’s satellites have saved Ukraine and changed warfare,” *The Economist*, January 05, 2023, <https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare>
- 42 David Ignatius, “How the algorithm tipped the balance in Ukraine,” *Washington Post*, December 19, 2022, <https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/>
- 43 Paresh Dave and Jeffrey Dastin, “Exclusive: Ukraine has started using Clearview AI’s facial recognition during war,” *Reuters*, March 15, 2022, <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>
- 44 Adam Pasick, “Pressure mounts on Germany,” *The New York Times*, January 23, 2023, <https://www.nytimes.com/2023/01/23/briefing/pressure-mounts-on-germany.html>
- 45 Isabel Coles, “Ukraine Begins 2023 Under Attack From Russian Drone Swarm,” *The Wall Street Journal*, January 01, 2023, <https://www.wsj.com/articles/ukraine-begins-2023-under-attack-from-russian-drone-swarm-11672576538>
- 46 “UAV, ammo sales to carry Turkish defense exports to new highs,” *Daily Sabah*, December 20, 2022, <https://www.dailysabah.com/business/defense/uav-ammo-sales-to-carry-turkish-defense-exports-to-new-highs>
- 47 Richard Simpkin, *Race to the Swift: Thoughts on Twenty-First Century Warfare*, (New Delhi: Natraj Publishers, 2012), pp. 102.
- 48 Innovations for Defence Excellence, “IDEX FOR FAUJI,” Department of Defence Production, Ministry of Defence, <https://idex.gov.in/idex4fauji>

Images used in this paper are from Getty Images/Busà Photography.



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