INTEGRATED APPLICATION OF FIREPOWER: ACHIEVING CROSS-DOMAIN SYNERGY IN HI-TECH CULTURE

VIKRANT DESHPANDE

What application of firepower was at the vanguard of the Russia-Ukraine conflict? Traditional logic dictates that it would be an air-to-surface missile like the Kh-31 P or Kinzhal or may be the surface-to-surface vectors like the Grad or Iskander.

However, as confirmed by Microsoft, the first attack was by a cyber weapon called "Foxblade"[1]. The attack targetted the cyber systems, thereby limiting the nation's ability to respond to subsequent kinetic attacks. This is the new world of Multi-Domain Operations and Grey Zone Warfare.

The contemporary conflicts drive home the great Prussian General Carl von Clausewitz's deduction that war is a chameleon, changing its colours as per the situation. In today's turbulent times, grey zone warfare-induced "plausible deniability" and multi-domain operations are *de rigueur* and drive home the need to adapt to changing paradigms.

Wing Commender **Vikrant Deshpande** is an officer of the Logistics Branch of the Indian Air Force, currently posted at Air Headquarters, New Delhi. He is a graduate of the Warfare and Aerospace Strategy Programme.

1. Brad Smith, "Microsoft: Defending Ukraine: Early Lessons from the Cyber War", https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/, June 22, 2022. Accessed on March 6, 2024.

Firepower refers to the destructive capability of a weapon system and fires is the employment of weapon systems to create a particular effect on the target. Traditionally, execution of firepower or fires includes surface-to-surface, air-to-surface, surface-to-air, air-to-air and sub-surface-to-surface.

Application of firepower has evolved over millennia, adapting to new technologies as and when fielded. The paper begins with: what is integrated application of firepower? How has it evolved historically to the present. Next, it delves into the present operating environment and its new domains of warfighting. Following which, the focus shifts to what is cross-domain synergy. And since, "the future is faster than we think," to borrow from Diamandis and Kotler, the paper treads into ways and means to achieve objectives in the high technology culture of today.

Two caveats apply to this paper. The information quoted is open source with no reference to any classified information, nor to tactics, techniques and procedures currently in vogue. The paper will analyse the continental domain with a focus on the evolving times and trends.

Firepower refers to the destructive capability of a weapon system and fires is the employment of weapon systems to create a particular effect on the target. Traditionally, execution of firepower or fires includes surface-to-surface, air-to-surface, surface-to-air, air-to-air and sub-surface-to-surface. Fires are executed in the three domains of land, sea and air by the armies, navies and air forces of the world.

Uses of firepower, including line of sight from the small arms of the infantry, tanks of armoured warfare and guns/rockets of aircraft are classified as direct fires. While fires from mortars, artillery weapons like cannons, rockets and missiles at longer distances and fires from bombs and missiles by fighter aircraft are classified as indirect fires, being non- line of sight employment.

Since time immemorial, warfighting was conducted in the continental domain and, with the advent of ships, included the maritime domain also.

The Italian War of Independence in 1848-49, witnessed the employment of air-to-surface fires for the first time, by the Austrians who used balloons to drop bombs on the Italians[2]. The invention of airplanes, led to the execution of coordinated air operations, in the Italian-Turkish War of 1911[3]. From then onwards, warfighting evolved from fighting battles in single domains to multiple ones. The next evolution was integrating the three domains of warfighting to achieve synergy and desired end states.

Integration denotes combining parts into a whole or, in military parlance, joining diverse elements of firepower into a single warfighting machine in order to achieve objectives. Integration of fires in time, space and force creates synergistic effects.

This paradigm shift brought about integration of fires in its wake. Integration denotes combining parts into a whole or, in military parlance, joining diverse elements of firepower into a single warfighting machine in order to achieve objectives. Integration of fires in time, space and force creates synergistic effects that are greater than the total of the individual ones prosecuted independently. This resonates with the principle of selection and maintenance of aim and economy of effort, and brings about greater efficiency and effectiveness in operations.

There exist multiple examples of successful joint operations with integration of firepower. In the first half of World War II, the German operational art of *blitzkrieg* integrated the German air and land forces; Operation Weseruebung, the Norway invasion, integrated the German Navy into the campaign to achieve decisive victories[4]. While in the second half of World War II, Operation Overlord witnessed 1,60,000 Allied soldiers carrying out amphibious operations on the beaches of Normandy, France, on

2. "History of Aerial Warfare: Wikipedia", https://en.wikipedia.org/wiki/History_of_aerial_warfare. Accessed on March 6, 2024.
3. Ibid.
4. "1930s German Doctrine: A Manifestation of Operational Art", https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/ MilitaryReview_20150630_art013.pdf,Tal Tovy. Accessed on March 7, 2024.

June 6, 1944. It integrated 7,000 naval vessels and 11,000 aircraft to achieve success.[5]

The 42 days of Operation Desert Storm in 1991 represented a contemporary example of joint planning and integrated application of firepower, with centralised planning and control followed by decentralised execution. Air power was effectively employed at the forefront to minimise casualties and collaterals before the ground offensive was launched. Air power was utilised to not only to gain control of the air but also to attack strategic targets, enemy lines of communications and fielded formations on the ground[6].

Thirty-three years since Operation Desert Storm, technology has grown in leaps and bounds, and the operating environment of today is totally different from the days of yore. It was prescient on the part of the North Atlantic Treaty Organisation (NATO) when it correctly envisaged[7] that the present and future battlespace would be characterised by the 5 Cs—congested, cluttered, contested, connected and constrained, especially in the urbanised area of operations.

The advent of radars, computer hardware and software, internet and social media, hyper connectivity by optical fibres and global positioning systems, mobiles and their applications, and cognitive influence by social media have created new domains of warfighting which are electromagnetic, cyber, informational, space, and cognitive.

Fires, kinetic or non-kinetic can also be executed in these contemporary domains to produce effects and achieve ends.

Having covered the operating environment of today, the next stage is the application of fires based on the effects generated. Cross-domain fires are defined by fires executed in one domain which lead to effects in a different domain while multi-domain fires are those that converge effects from two or more domains against a target system[8]. The logical evolution of warfighting

5. Dr. Silvano Wueschner, USAF Air University, "Key to Success: Allied Air Power at Normandy", https://www.airuniversity.af.edu/News/Display/Article/1859844/key-to-success-allied-airpower-at-normandy/, May 29, 2019. Accessed on March 7, 2024.
6. John Andreas Olsen, *History of Air Warfare* (Lincoln, Nebraska: Potomac Books, 2010) p. 238.
7. NATO- Allied Joint Doctrine for Joint Targeting, AJP-3.9, November 21, p. 25.
8. ADP 3-19 Fires, US Army Doctrine Publication, p. 11.

is achieving cross-domain synergy in the execution of fires in order to create effects by synchronisation across time, space and forces.

The French use of balloons for Intelligence, Surveillance, Reconnaissance (ISR) in the battle of Fleurus in 1794 against Austria to achieve objectives on land is a classic case of cross-domain synergy in the application of firepower.[9]

The Bekaa Valley campaign of 1982 by the Israeli Air Force is an example of multi-domain fires by utilising Remotely Piloted Aircraft (RPA) for Intelligence, Surveillance, Reconnaissance (ISR) and jammers for electronic warfare followed by hard kills to destroy/neutralise enemy Surface-to-Missile (SAM) systems.[10]

Operation Safed Sagar by the Indian Air Force (IAF) during the Kargil conflict of 1999, was yet another implementation of cross-domain synergy when coordinated air operations, by prosecuting targets between 14,000 to 18,000 ft, were pivotal in achieving the desired end state for our country[11].

Fast forward to 2022 and we witness the exploitation of the space, cyber/electromagnetic and cognitive domain in recent conflicts in addition to the traditional domains of air, land and maritime.

Starlink, a constellation of Low Earth Orbit (LEO) satellites, is being extensively used for communication and intelligence sharing by the Ukrainian forces, thereby negating the effects of electronic warfare.[12] The Kropyva app considered as uber for artillery[13], allows mapping an enemy position and transmitting to friendly artillery using Starlinks enabled data communication in order to prosecute fires.

9. "Military Use of Balloons During the Napoleonic Era", https://www.centennialofflight.net/essay/Lighter_than_air/Napoleon's_wars/LTA3.htm. Accessed on March 8, 2023.
10 "The Bekaa Valley War", https://www.airandspaceforces.com/article/0602bekaa/, Rebecca Grant, June 1, 2002. Accessed on March 8, 2024.
11. Benjamin S Lambeth, "Airpower at 18,000 Feet: The IAF in the Kargil War", carnegie-production-assets.s3.amazonaws.com/static/files/kargil.pdf. Accessed on March 8, 2024.
12. "Warfare after Ukraine," *The Economist*, July 8, 2024.
13. Tom Cooper, "Kropyva: Ukrainian Artillery Application", https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a, June 10, 2002, accessed on 08 Mar 24

This is a contemporary example of cross-domain synergy and integrated application of firepower[14].

The well publicised "Ghost of Kyiv," a legend who supposedly has six air-to-air kills in a single day, is a use case of exploiting the cyber domain to create effects in the cognitive domain[15] to not only boost the national morale but also to lower the morale of the opposing nation and its forces as a whole.

Social media, riding on the cyber domain, is being utilised to counter propaganda and garner support from across the world[16]. Applications like "Air Alarm" are being used to support civilian populations during air raids. Mass messaging applications like Telegram are being exploited with channels such as the pro Russian "Rybar" and pro-Ukrainian "stop Russian war bot" in the cyber domain, creating effects in the cognitive space. Information and disinformation fires are being carried out with the objective to influence the cognitive domain of the native population as well as influence other nations and garner their support in material and moral terms.

Electronic Warfare (EW) is also being extensively used to create EW fires thereby neutralising or degrading the performance of Global Positioning System (GPS) guided missiles and artillery shells[17].

In the '5C' operating environment of today, conflict has now forayed six domains: air, land, maritime, space, cyber/electromagnetic and cognitive.

This is in keeping with hybrid or grey zone warfare strategies in which a melange of actors, from state to non-state to private companies, are in the cauldron of the fires.

Against this backdrop of grey zone warfare across multiple domains, we, the Indian armed forces, have our task cut out to fight and win today's wars.

14. "How the Kropyva Combat Control System Helps in the Most Difficult Situations: Fortified Positions Couldn't Save Russian Army", https://en.defence-ua.com/news/ how the_ kropyva_combat_control_system_helps_in_the_most_difficult_situations_fortified_positions_ couldnt_save_russian_army-3646.html, July 23, 2022. Accessed on March 10, 2024.
15. Jared Keller, "'The Ghost of Kyiv' is the First Urban Legend of Russia's Invasion of Ukraine", https://taskandpurpose.com/news/ghost-kyiv/, February 25, 2022. Accessed on March 10, 2024.
16. Drew Harwell, "Instead of Consumer Software, Ukraine's Tech Workers Build Apps of War", https://www.washingtonpost.com/technology/2022/03/24/ukraine-war-apps-russian-invasion/, March 24, 2022. Accessed on March 10, 2024.
17. "Battle of the Beams," *The Economist*, July 8, 2024.

In case of a conflict, the desired political end states conveyed by the Raksha Mantri's (RM's) operational directive are converted into joint military objectives[18].

These are enunciated in the joint operational directive for effective planning and conduct of joint operations with structures, linkages and processes in place at all levels. With the joint planning process, integrated employment of forces is orchestrated, utilising operational art.

This planning is crucial for integration of firepower in both time and space to achieve cross-domain synergy. Critical to the planning process are the functions of intelligence and targeting. This involves identifying and prioritising targets based on the selected course of action and intelligence inputs available to achieve the desired effects by employing appropriate fires. The effects would need to be created in all domains, including air, land, maritime, cyber/electromagnetic, space and cognitive.

At the strategic and operational levels of warfighting, it is in the planning of ISR, targeting, management and exploitation of firepower, air space, electromagnetic spectrum, cyber and space domain that technology will play a crucial role.

And so, now we pivot to the new technologies track and understand what applications of high-tech culture could be exploited by the Indian armed forces and the nation as a whole for integration of firepower to achieve cross-domain synergy.

At the tactical level, call for fires in the Tactical Battle Area (TBA) is a challenging activity in a contested, life-threatening environment. Traditionally, voice communications were used to call on fires by the forces on the ground. However, the inherent limitations of verbal communications in a stressful situation with short timeframes, made the fires difficult to communicate, synchronise and execute. Now, with the advent of portable digital systems to transmit targeting information and required fires using tactical data links in a secure mode, the call for fires has become more effective. The digital systems transmit and receive data in standard formats and help in integrating

18. Joint Doctrine, Indian Armed Forces, ch 5, p. 6.

Digital systems must be robust enough to operate in degraded environments with adverse GPS availability in conditions of electronic warfare and be secure enough to withstand attempts to hacking.

processes across domains. They assist in selecting the most appropriate shooter for achieving the desired effects, prosecute targets with precision, and reduce collateral damage and fratricide, while compressing the timeframe required to execute the fire. The caveat being that the digital systems must be robust enough to operate in degraded environments with adverse GPS availability in conditions of electronic warfare and be secure enough to withstand attempts to hacking. These digital systems are embedded in tablets or smartphone-like form factors, making them highly practical.

This is a game-changer at the tactical edge since not only is the communication secure through encrypted links but also the target data and own position information are reliable, accurate and comprehensible. These eliminate errors due to human factors and helps in integration of firepower and achieving cross-domain synergy with higher accuracy and reduced time-frames[19].

Stepping up the ladder to the operational level, is the Joint All Domain Command and Control (JADC2) or Combined Joint All Domain Command and Control (CJADC2). Going out on a limb, at the very basic, we need a common communication network for all the three Services which is resilient and robust. The next evolution would be to connect the varied types of sensors from all the stakeholders—the air force, army, navy, and space—into a single network. For example the Integrated Air Command and Control System (IACCS) and Akashteer have witnessed a certain level of integration. Traditionally, each of the Services designed and developed its own tactical network or battle management system which is generally not compatible with those of the other Services due to software and design issues. The

19. https://www.afcea.org/signal/resources/content/BATS-D_DACAS_Signal_White_Paper_Final.pdf. Accessed on March 11, 2024.

current operating environment and the future conflicts envisaged would necessitate the decision-making time to be reduced to the bare minimum. So how do we synchronise the sensors and shooters? An analogy is the service provided by Uber/Ola which combines two different applications: one for riders and the second for drivers. Using the customer's and driver's positions, the algorithm makes the optimal match based on distance, travel time, and passengers. The application then seamlessly provides directions for the driver to follow, delivering the passenger to his/her destination. The apps use cellular and Wi-Fi networks to transmit data to match customers and provide navigation services to the drivers[20].

The joint all-domain operations paradigm, would, therefore, provide critical and war-winning information to decision-makers, thereby enabling operations using surprise and the speedy integration of fires across all the domains.

CJADC2 will enable sharing of ISR data across the network with the planners to ensure faster decision-making, with the availability of a common operating picture, including enemy targets, friendly locations and command and control information. Next, it would determine the optimum shooter for the desired effects and communicate orders to execute fires. The objective being "any sensor to best shooter."

The joint all-domain operations paradigm, would, therefore, provide critical and war-winning information to decision-makers, thereby enabling operations using surprise and the speedy integration of fires across all the domains. So the JADC2 architecture would empower commanders to rapidly gain and maintain situational awareness, shorten the Observe, Orient, Direct, Act (OODA) loop, and deliver cross-domain synergy.

Going a step further, the CJADC2 would integrate assets across friendly nations and partners for an even bigger collaborative effort to win against common adversaries.

20. https://crsreports.congress.gov/product/pdf/IF/IF1149%203. Accessed on March 11, 2024.

The leading question to this development would be choosing the data source for the CJADC2. It is a given that data centres are vulnerable to attacks. In any future conflict, the initial non-kinetic strikes are expected on data centres so as to cripple the information systems of the adversary.

This leads to the second application of technology, which is the combat cloud. The American armed forces are moving on to the joint warfighting cloud capability[21]. A contract worth $9 billion has been awarded to commercial cloud service providers—Google, Amazon, Microsoft and Oracle—to acquire commercial cloud services directly[22]. This combat cloud is intended to provide operational capability to the JADC2. It is designed to be accessible to all operating domains and across all classification levels. The resilience in the architecture would allow operations even in degraded or denied environments. This combat cloud capability is designed in two stacks. The first is the tactical edge offerings for the warfighter, with small form factors for better ergonomics and ease of use even in a denied or degraded environment. The second is the operational edge capability which will provide applications and data closer to the user, resulting in lower latency. So even if network loss happens, the edge devices will be able to continue and operate and resynchronise when reconnected. This would enable faster decision-making. The cloud is built to be secure against enemy threats and provide reliable, high-speed throughput with redundancy since the missions will carry on irrespective of the situation.

NATO is building its own multi-domain combat cloud with the aim to merge data from various sources in a secure way and convert that data into actionable information. Similar services and algorithms will be running on cloud servers in headquarters, at forward operating bases, as well as on fighter aircraft, tanks, or ships[23]. The cloud layer contains all the nodes which

21. "J9 Hosting and Compute", https://www.hacc.mil/Portfolio/JWCC%20/. Accessed on March 13, 2024.
22. "The Latest on the Pentagon's Major Cloud Acquisition: The Joint Warfighting Cloud Capability", https://defensescoop.com/radio/joint-war-fighting-cloud-at-pentagon/, December 6, 2023. Accessed on March 13, 2024.
23. Colonel Hubert Saur (Retd), "Multi-Domain Combat Cloud: A Vision for the Future Battlefield", https://www.japcc.org/essays/multi-domain-combat-cloud/. Accessed on March 13, 2024.

churn large amounts of data. The battlefield layer crunches less amount of data but links the cloud and edge. The edge layer contains mostly sensors and shooters. They supply the real-time data to the battlefield and cloud layer with the objective of creating operational level information or intelligence. The aim is to achieve a seamless exchange of trusted information at different layers, leading to information superiority and shortening the OODA loop.

Reliable cloud services in all operating environments would not only empower the warfighter but also allow execution of applications like JADC2 for cross-domain synergy and integration of firepower. No paper on new technologies is complete without the mention of Artificial Intelligence (AI). AI is ubiquitous these days in everyday life. The defence sector is also affected by this new technology, what with the availability of huge amounts of data, computing power and algorithms.

Both the application we witnessed, CJADC2 and multi-domain combat cloud, are underpinned by use of AI for rapid data analysis, shortening the decision-making time and selecting the best shooter or weapon system to engage a target. Creative disruption using AI is foreseen. The US Air Force (USAF) recently hosted a bid on February 29, 2024, to find out new AI and distributed command and control concepts to support JADC2, with a funding of $99 million[24]. They envisage AI to be a key component of future command and control systems and the huge investment is the proof.

Overarching the traditional domains of land, sea and air is the space domain.

Though space is considered a global common, it is increasingly turning into a contested area. In modern day wars, the requirement of space is mission critical since space-based applications are enablers for all other domains of warfighting. Satellites utilised for ISR have an advantage because they are not restricted by geographical boundaries and have freedom of operation. Communications using satellites provide ubiquitous coverage wherever traditional communication methods are not available. Providing

24. "Artificial Intelligence and Next Generation Distributed Command and Control", https://sam.gov/opp/d8eb1d7f980d4c02b080d87747297ee6/view. Accessed on March 15, 2024.

Cyber space is increasingly being targeted by state and non-state actors inimical to national interests. The asymmetric effect of cyber attacks and the anonymity offered make cyber space an attractive option for offensive fires.

early warning of incoming ballistic missiles through space is another crucial utilisation. Space enables information for positioning, navigation and timing through GPS which is important for targeting and execution of fires in all weather conditions, by day or night.

Consequently, it is imperative to ensure access to space for friendly exploitation and, at the same time, deny, degrade or disrupt the use of space by our adversaries in times of conflict.

This alludes to weaponisation of space. As on date, four nations viz India, USA, Russia and China have demonstrated Anti-Satellite (ASAT) weapons capabilities[25].

Slowly, but surely, the weaponisation of space will see an uptick. Considering all these applications, it is essential to factor in the space domain in joint planning, with the objective to achieve cross-domain synergy, using high end technology.

In the interconnected world of today, with optical fibre cables and 5G networks, the cyber domain is crucial for the public infrastructure and commercial as well as military applications for any nation. The flow of data and voice communications is imperative to business and the running of everyday utilities. Hence, cyber space is increasingly being targeted by state and non-state actors inimical to national interests. The asymmetric effect of cyber attacks and the anonymity offered make cyber space an attractive option for offensive fires. Nations could be attacked by non-kinetic cyber fires to cripple critical civil infrastructure or damage military command and control systems. The operators of cyber space are not just the military but also private and government entities. Hence, at the operational level itself,

25. Nathaniel Roman, "Global Status of Anti-Satellite Weaponry and Testing", https://ace-usa.org/blog/research/research-foreignpolicy/global-status-of-anti-satellite-asat-weaponry-and-testing/, January 30, 2024. Accessed on March 15, 2024.

fires in cyber space need to be included in the joint planning process to ensure cross-domain synergy with civil agencies.

Cyber could be channelised to create effects in the cognitive domain which affect the minds of the individual and the society at large. The new state of no war no peace is the playground for cognitive warfare.

In conflicts below the threshold of war, state and non-state actors target the human mind and the entire population of a nation by generating fake news and disinformation campaigns.

It is imperative to guard and defend against cognitive warfare by our adversaries. Defence against cognitive warfare, dovetailed during the planning process at the strategic and operational levels is yet another example of cross-domain synergy.

The objective is to create doubts in the minds of soldiers and citizens, polarise opinions and fragment societies which were otherwise peaceful. Additionally, non-kinetic fires in the cognitive domain could be used to create kinetic effects of inciting violence by propaganda and hate speech[26]. Hence, it is imperative to guard and defend against cognitive warfare by our adversaries. Defence against cognitive warfare, dovetailed during the planning process at the strategic and operational levels is yet another example of cross-domain synergy.

To conclude, the hybrid nature of conflicts taking place in multiple domains, with ever increasing lethality in the operating environment of today, makes it mandatory to integrate the application of firepower and achieve cross-domain synergy by leveraging technology. As seen in recent conflicts, while new domains have evolved, there is a constant need to build capacity, capability and synergy of firepower to win wars.

26. Seumas Miller, "Cognitive Warfare; An Ethical Analysis", https://link.springer.com/article/10.1007/s10676-023-09717-7, September, 2023. Accessed on March 15, 2024.