THE 'EVERYWHERE BATTLEFIELD': IMPLICATIONS FOR AIR WARFARE IN THE ERA OF MULTI-DOMAIN OPERATIONS AND PAKISTAN'S AERIAL DEFENCE POSTURE

Ezba Walayat Khan[*]

Abstract

The evolving character of war due to technological advancement and integration of the fields has led to the notion of the everywhere battlefield. This paper is a review of how Multi-Domain Operations (MDO) are transforming the way strategic and operational thinking is being addressed by bringing together land, air, naval, cyber, and space capabilities into a unified framework. The main aim of the study is to examine the consequences of MDO to Pakistan, and more specifically Pakistan Air Force leading role in the development of network-centric and cross-domain capabilities. The paper uses the Network-Centric Warfare theory to place the trajectory of Pakistan in the context of global trends, such as the US doctrine of Joint All-Domain Command and Control (JADC2), the Chinese doctrine of Integrated Joint Operations, and lessons of the war between Russia and Ukraine. Methodologically, the study adopts a qualitative approach, combining semi-structured expert interviews with systematic analysis of secondary sources. The study's findings reveal that the effective integration of MDOs during May 2025 war with India provided Pakistan with a concrete operational advantage, highlighting their role in strengthening credible deterrence. Furthermore, the paper highlights challenges such as hybrid threats, and resource limitations, and wraps up with policy suggestions on how Pakistan can sustain current momentum on tri-service synergy, technological innovation, and resilience in operations in the era of multi-domain warfare.

Keywords: MDO, C[4]ISR, Network-Centric Warfare, Everywhere Battlefield, Air Power, Cyber, Space.

Introduction

The realisation that warfare is no longer limited to traditional combat zones or geographically defined battlefields gives rise to the idea of the everywhere battlefield. In the past, wars were fought inside predetermined zones, with militaries facing off against one another. The development of technology, long-range strike capabilities, precision-guided munitions, and cyber operations has enabled states to penetrate deep into adversary territory without physically crossing frontlines, blurring the clear boundaries of the battlefield.[1]

[*]Ezba Walayat Khan is a Research Assistant at the Centre for Aerospace and Security Studies (CASS), Lahore. The author can be reached at ezbawkhan546@gmail.com.

It was evident in the most recent Russia-Ukraine war, the full range of military and civilian infrastructure, from communications networks to financial systems has now been regarded as part of the battlespace.[2] This results in the "everywhere battlefield," depicting a strategic setting in which boundaries are obscure, domains are linked, and conflict transcends both the physical and digital realms.

In the past, air power operated as a separate field, and victory in traditional warfare required control of the air. From the Second World War to the Gulf War, when air superiority permitted operational freedom on land and at sea, the twentieth century supported this reasoning. However, recent conflicts show that domain-specific strategies are no longer enough, giving rise to the concept of Multi-Domain Operations (MDO).[3]

MDO is a conceptual and operational transformation towards the integration of five key domains, including space, cyber, air, land, and navy, into an integrated framework. Satellites in space perform surveillance, communications, and navigation applications that support almost every aspect of modern conflicts.[4] The cyber domain is characterised by electronic signals and data flows travelling at the speed of light and providing opportunities for both offensive and defensive operations.[5] The domain of air is made up of platforms and systems which provide mobility, strike and Situational Awareness (SA), It is also about integration with advanced technologies for quick and precise decision-making.[6] On land, traditional instruments such as tanks, artillery, and ground forces continue to anchor combat power.[7] The naval domain includes the surface vessels, submarines and related assets that can project power and protect sea lines of communication. Together, MDO increases situational awareness for commanders and operators and enables effective and coordinated use of one's assets while denying an equivalent capability to the adversary.[8]

Because of their speed, manoeuvrability, and ability to strike with precision, crewed aircraft were the epitome of air power throughout the 20th century. However, their importance in today's conflict is less about being stand-alone platforms and more about serving as nodes within larger networks of sensors and shooters. This change aligns with the ideas of MDO and the concept of everywhere battlefield, which both argue that air superiority can no longer be guaranteed solely by air assets. The necessity for cross-domain integration is highlighted by the increasing susceptibility of air defences to cyber, space, electronic, and drone threats.[9] This calls for coordinated technological, operational, and doctrinal innovation across all five domains.

This study is framed by the main research question: How is the traditional primacy of air superiority being redefined by the "Everywhere Battlefield", driven by the convergence of kinetic and non-kinetic domains, and how is Pakistan reorienting its air power capabilities to ensure credible deterrence and operational resilience in MDO?

The overarching aim of this research is to map development of warfare from domain-specific conflicts to the integration of land, air, naval, space and cyber domains, in order to define how the integration of domains has come to shape the strategic environment. In particular, the research will be concerned with understanding how the advent of MDO challenges existing air power concepts and redefines operational thinking for states such as Pakistan. It will also assess the vulnerabilities and opportunities that Pakistan's aerial defence posture faces in an era when threats can come from multiple domains at once, from precision-guided munitions and stealth platforms to cyber intrusions and space-based surveillance. The study identifies a gap in existing literature, as most scholarship on MDOs remains Western-centric and provides limited analytical focus on Pakistan's air power capabilities within this framework. Therefore, the study aims to fill the literature gap by bringing attention to the unique geostrategic context of Pakistan, which so far has not received much attention in the overall MDO discourse. Ultimately, the research is aimed at providing policy-driven insights on how Pakistan can adapt its air power development to be resilient, deterrent, and operationally effective in the age of profound transformation in air power.

Network-Centric Warfare Theory

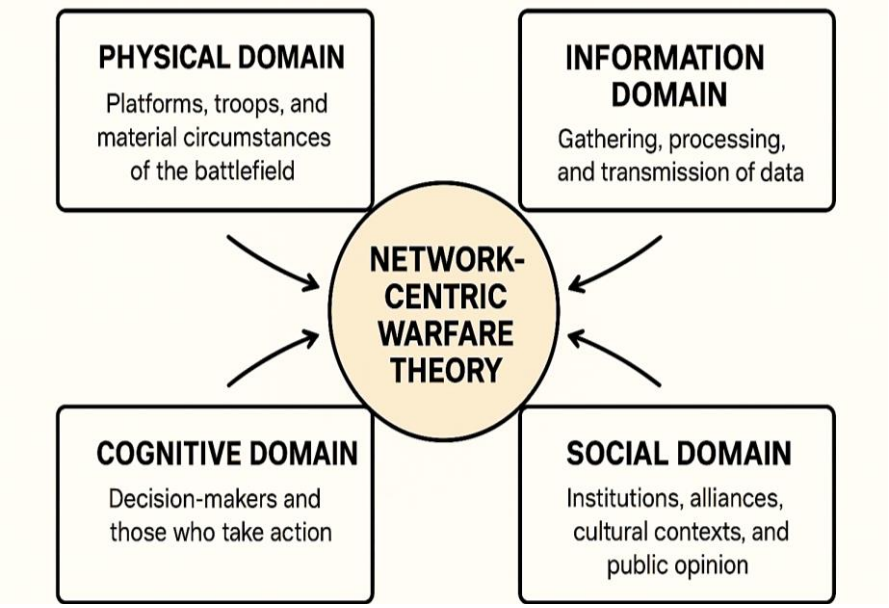
The theory of Network-Centric Warfare (NCW) was developed to translate an information advantage into combat power by networking geographically dispersed sensors, decision-makers, and shooters. The theory was driven by advances in information and communication technology and the need for a more effective, faster, and lethal force.[10] For NCW, Command and Control (C^2) is the essence as it facilitates correct, quick and consensus-based decision-making, allowing resources and assets to be employed in time and space where they matter the most. Additionally, it allows force application with conviction and clarity, making NCW the enabler for data collection, fusion and display in a user-friendly manner.[11]

Unlike the past linear concept of the Air-Land Battle, where the front lines were fixed and zones of control were well defined, NCW is being addressed as an intricate, adaptive system, where connectivity and information are paramount. It focuses on the coordination of various components into a unified network where dispersed forces would act in one way with principles in information superiority, speed of command, and self-synchronisation pointing out that the power to operate effectively is not in a single system but in the coordination of a large number of elements working in a responsive network.[12]

Network-Centric Warfare (NCW) can be interpreted with reference to four domains, which are all intertwined. The physical domain is related to the concrete elements of war such as platforms, troops, and material circumstances of the battlefield. These are evaluated on the basis of lethality and survivability. The information domain relates to the gathering, processing, and transmission of data that enables command and control.

The cognitive domain pertains to those who make decisions and take action, where perception, situational awareness, and judgement influence outcomes. Finally, the social domain encompasses institutions, alliances, cultural contexts, and public opinion, all of which affect compliance and cooperation.[13]

Figure 1: Four Domains of NCW Theory[14]



Source: Author's Compilation

The conceptual basis of NCW provides a framework for understanding how forces can gain an edge in modern, multidomain conflicts. These four domains together illustrate that combat power is no longer a linear function of material strength alone. Rather, it is being influenced more by the quality of connections and the effectiveness of information transfer.[15] NCW recommends coordination of efforts at land, air, sea, cyber and space domains to create synergies. The aim is to place the opponents in simultaneous dilemmas, which is beyond their ability to respond effectively. This indicates a decisive break from linear warfare, where the force was used proportionately and predictably. Within an NCW-informed approach, the results are non-linear and agile, and based on the strategic exploitation of networks to interfere with the decision-making processes of the adversary.[16]

Methodology

The study uses a qualitative methodology with systematic analysis. Semi-structured interviews with subject-matter experts were used to collect primary data to obtain first-hand information about the evolving concept of MDO and its execution in terms of Pakistan's aerial defence posture.

The research design is exploratory and interpretive in nature, aimed at developing the analytical depth of an emerging operational concept. Because of both the sensitive nature of the topic and privacy constraints, limited interviews were conducted with questions that examined issues of balancing indigenous development with external collaboration in the latest technologies, adapting to new challenges posed by emerging threats such as drones and Electronic Warfare (EW), lessons learned in recent conflicts, and the doctrinal and institutional changes required for a multi-domain mindset.

Systematic secondary analysis of defence literature, research articles and policy documents was also undertaken to supplement the primary data, leading to the triangulation of the findings and enhancing the analytical strength. This approach enabled a comprehensive assessment of how the concept of the "Everywhere Battlefield" is shaping air warfare and influencing Pakistan's strategic and operational thinking. While much of the existing literature on MDOs and the technological requirements of the "Everywhere Battlefield" is highly Westernised, Pakistan provides a compelling example of a middle power that has advanced its capabilities through indigenous development and doctrinal innovation. Its achievements in precision targeting, EW, and operational coordination were clearly demonstrated during the May 2025 war with India. The criteria of assessment is built on four interrelated dimensions: doctrinal evolution, interoperability, technological integration and operational effectiveness. These dimensions collectively enable an evaluation of the extent and character of how Pakistan is operationalising and consolidating its multi-domain warfare capabilities within an evolving operational environment.

Multi-Domain Operations: From Theory to Practice

Multi-Domain Operations (MDO) is a paradigm shift in contemporary military thought since it synchronises the capabilities of land, sea, air, space and cyber domains. Instead of being dependent on one domain of isolated pre-eminence, MDO exploits the connectedness of modern warfare to establish cross-domain effects debilitating the decision-making of the adversary and establishing strategic advantage.[17]

Strategic Rationale for MDO

MDO is guided by technological change, shift in geopolitical competition and the emergence of hybrid threats.[18] The classic single domain doctrines are no longer sufficient in a time where threats can reside in the physical and cyber realms as well as where tactical actions can have immediate strategic consequences. Thus, MDOs are based on the necessity of scalable operations and addressing the requirements of modern warfare, when the enemy is operating in various domains simultaneously. The integration of individual capabilities of these domains enhances the speed, accuracy, and flexibility of operations and enables forces to exert offensive pressure against critical enemy targets without compromising defensive postures.[19]

Analysing the vulnerabilities and dependencies of the opponents, MDO provides the commanders with the choice to put pressure at all levels at the same time. This allows the military planners to interconnect and use specific capabilities of each domain as well as to develop and execute plans that complement one another and that are in the national security interest of a country.

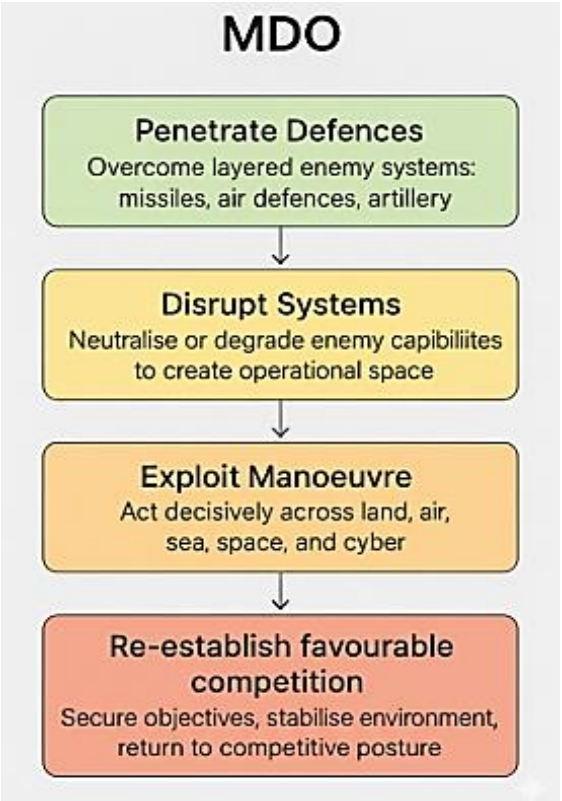
How MDO Is Intended to Work?

The core principle of Multi-Domain Operations (MDO) is to maintain the advantage by being able to compete at all domains under stressful conditions, or even below the threshold of open conflict.[20] This is aimed at discouraging possible enemies by making constant contact and being involved. Nevertheless, in case deterrence falters and conflict arises, the militaries use MDO as follows:

- **Penetrate Adversary Defences**: This entails overcoming developed defensive systems that can encompass precision-strike weapons, anti-ship capabilities, air defence systems, and long-range rockets and artillery. When forces are able to successfully penetrate these layers, they can function more efficiently across domains.
- **Dis-integrate Enemy Systems**: At the point of initial penetration, the target is to disrupt, degrade, or neutralise adversary capabilities. This results in tactical and operational opportunities to achieve goals with comparatively less resistance.
- **Exploit Freedom of Manoeuvre**: When enemy forces are in disarray, other forces can take decisive action to accomplish operational and strategic objectives, along all fronts: land, air, sea, space, and cyber, defeating enemy forces and capturing vital targets.
- **Re-establish Favourable Competition**: Once military success is achieved, the last step is to consolidate gains across all domains, stabilising the operational environment, and resuming a competitive posture under favourable circumstances.[21]

This chain is the core logic of MDO, leveraging integrated capabilities to dominate in conflict and shape the environment in competition to prevent war in the first place as shown in the Figure 2.

Figure 2: MDO's Operational Concept[22]



Source: Author's Compilation

Air Power as an Enabler in Multi-Domain Operations

From its early use in World War I for reconnaissance,[23] air power has developed into a key component of contemporary military strategy, including fighter jets, bombers, unmanned aerial vehicles, and transport aircraft that can carry out a variety of tasks. Its unparalleled speed, reach and flexibility make it possible to quickly deploy troops and equipment over great distances, which is essential for dealing with new threats. Guided munitions on modern aircraft enable the precision strike on enemy infrastructure, thereby minimising collateral damage and efficiently achieving the strategic objective at the same time. The intelligence, surveillance, and reconnaissance capabilities can also assist commanders in making informed decisions and undertaking adaptive operations, having access to real-time information about the enemy position and the situation on the battlefield.[24] Air-to-air combat and air dominance allow forces to act freely and restrict the options of the enemy by controlling the skies. In addition to these operational impacts, there is also a major psychological impact of air power to exert influence through its formidable capabilities and discouraging enemies.[25]

Through these benefits, the air domain is one of the major aspects in Multi-Domain Operations that directly and indirectly support the other domains. Its capabilities in the skies enable it to influence land and sea operations along with the underwater operations, while using cyber, space, and electronic capabilities to further enhance its abilities. Air-to-Air warfare secures control of the skies, whereas air-to-surface operations disrupt the ground and naval forces of the enemy, providing an enabling space to other forces. Historically, air power has been most efficient when it is applied in targeting the centres of gravity of an adversary, and this has consistently shaped the course of military operations.[26]

Technological Catalysts for MDOs

The concept of technological determinism has been prominent in the field of studies of science and technology (STS) in highlighting the importance of how technology shapes institutions and society. Technological determinism states that the future of warfare will predominantly be influenced and shaped by technological developments, which will not only influence the military capabilities but also doctrine, operational concepts, and national security priorities.[27] Historical and modern practices have demonstrated that technology is fundamentally transformative in military contexts. Although the experience, leadership, and strategy remain important factors, technology often becomes decisive, especially in revolution in military affairs (RMAs), in which it becomes the driver of change.[28]

The fast development of military technologies has been one of the greatest contributors of MDO.[29] A baseline of distributed, fast, and data-driven operations across vast and networked battlefields has been made possible by innovative developments in artificial intelligence, autonomous systems, cloud computing, cyberwarfare, and advanced sensing technologies. Military forces can now simultaneously coordinate defensive operations, ISR (intelligence, surveillance, and reconnaissance), and precision strikes using real-time data fusion with 5G and satellite networks. These changes have not only expanded the scope of tactical capability but also shortened decision-making times and made modern warfare more complex.[30]

To exchange real-time information across platforms and domains, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems have become an essential component of MDOs. By combining inputs from sensors, drones, satellites, and manned aircraft into actionable intelligence, advanced data fusion techniques shorten the time for decision-making and improve responsiveness. By improving threat identification, target prioritisation, and predictive analytics, machine learning and Artificial Intelligence (AI) allow commanders to take proactive decisions and guarantee that operations are coordinated across the air, land, and cyber domains.[31] Meanwhile, the outcomes of conflicts are influenced by jamming enemy radars, interfering with communications, and destroying networked command systems, just as much as by conventional kinetic attacks.

Space-based capabilities, especially ISR satellites, are essential for multi-domain integration because they offer secure communications, targeting assistance, and continuous surveillance. Together, these technology enablers form a multi-layered, interconnected system where precision, situational awareness, and integration, rather than just the quantity of platforms used, are critical to operational success.[32]

Unmanned Aerial Vehicles (UAVs): A New Dimension

Unmanned Aerial Vehicles are one of the novel technologies shaping MDO.[33] UAVs that were originally deployed in reconnaissance operations have evolved into multi-purpose platforms, which can be deployed in strike missions, intelligence collection and swarm missions.[34] They are cheap, scalable, and flexible, which is why they are both technologically advanced and a cost-efficient option in the modern era of technology.[35] UAVs encompass a broad spectrum of systems, including High-Altitude Long Endurance (HALE), Medium-Altitude Long Endurance (MALE), and loitering munitions. They are deployed and used depending on the nature of the operational requirements of the mission. UAVs can be used as a source of kinetic applications in uncontested space. Their presence crafts narratives, directs popular awareness and allows continuous surveillance by blurring the distinction between action taken and strategic message.[36] Moreover, drone warfare in recent conflicts has demonstrated weaknesses in the conventional ideas and the necessity to invest in anti-drone and EW capabilities.[37]

Domain Convergence and Operational Complexity

The contemporary battle terrain is increasingly characterised by the overlap of realms. The outer space and cyberspace, which were previously seen as support areas, are now distinct operational domains.[38] Satellites are crucial to navigation, communication and early warning but they are susceptible to jamming and hacking.[39] On the same note, cyber operations may shut down vital infrastructures, interfere with logistics, and disrupt command systems.[40] The need for MDO is further supported by this convergence, since domain-specific, isolated responses are no longer adequate. In a world where no single sphere is safe or uncontested, cross-domain integration is not only advantageous but also necessary for operational success.

Geopolitical Pressures and Strategic Competition

MDO responds to the changing geopolitical competitive environment. Hypersonic weapons, advanced defence capabilities, strategic UAV fleets, and cyber arsenals are among the advanced capabilities that major and middle powers are spending heavily in order to impose their influence. They are used not only during war but also during peacetime to engage in strategic rivalry to shape environments and deter competitors through presence and posture.[41]

Hybrid Threats and Grey-Zone Challenges

The contemporary conflicts take place in the grey area, which is above the level of peaceful competition but below the line of open warfare. States frequently use proxy warfare, political meddling, disinformation, and cyber intrusions. Here, too, UAVs are important because they provide low-cost access to contested areas and plausible deniability. MDO offers a framework for combining traditional and non-traditional tools to combat grey-zone threats. States can preserve strategic stability without instantly escalating conflicts by using it to enable quick, cross-domain reactions to cyberattacks, information operations, or other provocations.[42]

Implementation Challenges and Leadership Demands

Although the idea behind MDO is well justified, it becomes challenging to implement. Silos across institutions, technical incompatibility, and disparate strategic cultures tend to constrain interoperability across services, allies, and domains. Additionally, MDO creates strategic conflicts because of the different priorities of stakeholders. This requires a unified approach by the planners at all levels to achieve intended outcomes. MDO success hinges on military leaders' capacity for innovative thought, decisive action, and constant adaptation, all while staying true to strategic goals. It does not constitute a one-off adjustment; it is a paradigm shift in the conduct of conflict in the 21st century. Integrated, cross-domain operations have become necessary due to the emergence of UAVs, hybrid threats, strategic competition, and technological advancements. MDO offers a unique framework to deal with the intricacy, unpredictability, and interdependence of contemporary warfare.[43] In such a setting, the ability to combine and coordinate effects across domains, faster and more effectively than adversaries, will determine victory rather than dominance in a single domain.

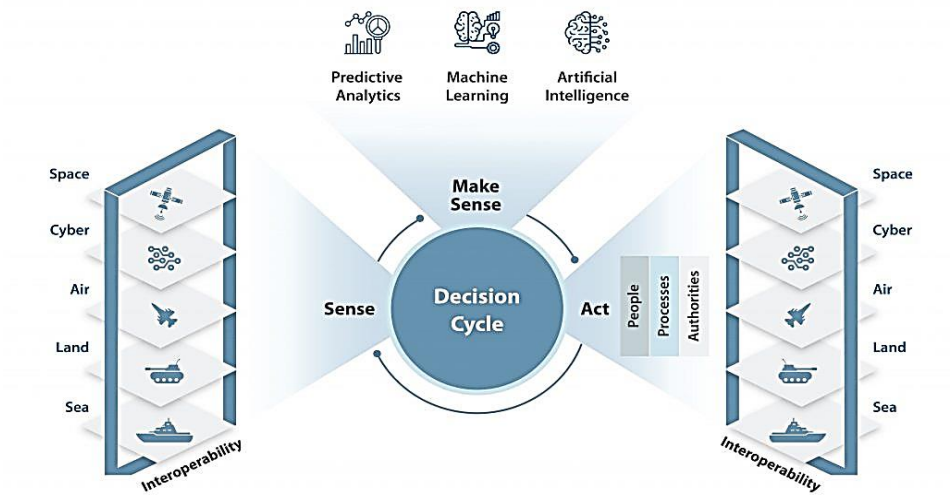
Global Military Trends in MDO

United States: JADC2 Doctrine

The United States has placed Joint All-Domain Command and Control (JADC2) at the centre of its future warfighting strategy. It is intended to ensure decision and information superiority in an era of great power competition. The Department of Defence describes JADC2 as the mechanism to command across land, sea, air, space, cyber, and the electromagnetic spectrum, even in degraded conditions, in order to deter and, if required, defeat adversaries.[44] Although conceived as a global framework, its design is primarily shaped by the need to counter near-peer rivals such as China and Russia while also assuring interoperability with allies and partners in NATO and the Indo-Pacific.[45]

At the operational level, JADC2 is built on a "Sense, Make Sense, Act" model. This involves collecting data from sensors across domains and electromagnetic spectrum, fusing and analysing it into intelligence, and enabling commanders to act at the speed of relevance. The aim is to compress the sensor-to-shooter cycle and maintain decision-making tempo even under contested conditions.

Figure 3: US JADC2 Strategy



Source: The Air Power Journal[46]

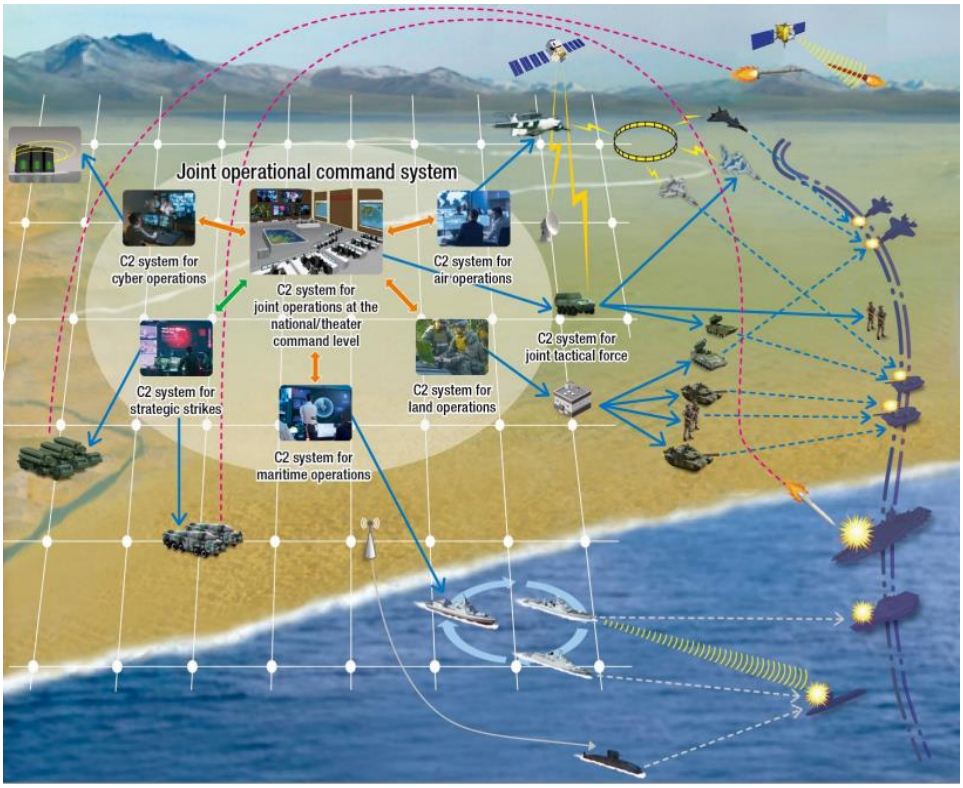
The strategy is organised around five Lines of Effort (LOEs), establishing the JADC2 data enterprise, building the human enterprise, developing the technical enterprise, integrating nuclear command and control, and modernising information sharing with mission partners. These LOEs demonstrate that JADC2 is not merely a technical project but also an institutional and cultural transformation requiring doctrinal and organisational reform.[47]

Six guiding principles shape its implementation, including layered security, resilience in contested electromagnetic environments, and the adoption of common data standards. A Cross-Functional Team involving senior leaders across the Services, Joint Staff, Combatant Commands, and the Office of the Secretary of Defense oversees execution through a formal Implementation Plan. Supporting initiatives like the Advanced Battle Management System of the Air Force, the Project Convergence of the Army, and the Project Overmatch of the Navy contribute to the JADC2 ecosystem, indicating that Washington recognises that the future warfare requires fully integrated MDOs.[48]

China's Integrated Joint Operations

The idea of integrated joint operations has gradually been developed in China since its significant military reform in 2015. The doctrine has a vision of a command structure that will integrate land, air, naval, space, cyber and electromagnetic forces into a unified operation system. It is also applied to new areas like information and cognition, as Beijing conceived that any future conflicts would be resolved in the information space as much as in the physical arena.[49]

Figure 4: Conceptual Representation of China's Integrated Joint Operations



Source: The National Institute for Defense Studies[50]

One of the main aspects of such change was the establishment of the Strategic Support Force (SSF), which incorporated space, cyber, electronic, and information warfare capabilities. Its aim was to offer seamless support to the joint commanders in the form of reconnaissance, communications, EW, and cyber operations. Introducing these features into operational planning, the SSF aimed to ensure that the PLA had an ability to make precision strikes, sustain situational awareness, and disrupt the decision-making of adversaries.[51]

The SSF was disbanded in 2024 and three forces were established under the Central Military Commission, the Aerospace Force, the Cyberspace Force, and Information Support Force (ISF). The ISF has emerged as the backbone of joint integration, tasked with managing networked information systems, ensuring secure data flows, and embedding information support teams alongside air, naval, and ground units. These changes signal a recognition that information dominance is no longer an auxiliary function but a core pillar of joint warfare.[52]

PLA doctrine and force development increasingly emphasise the role of cyber and information operations in the opening phases of conflict. The focus is on targeting adversary command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems in order to paralyse decision-making and establish favourable conditions for air and naval campaigns. This reflects lessons drawn from recent conflicts, where the integration of space-based ISR, unmanned systems, and electronic interference has proven decisive in shaping operational tempo. [53] Collectively, these developments reveal a PLA focused on achieving multi-domain synergy, with information warfare and cyber power positioned as central enablers of future joint campaigns.

Russia-Ukraine: Actions and Key Lessons

The Russia-Ukraine conflict has served as a testing ground for multi-domain operations, revealing both the opportunities and vulnerabilities inherent in modern warfare. Russia has relied heavily on large-scale missile strikes, loitering munitions, and layered EW to suppress Ukrainian air defences and disrupt command networks. Its extensive use of GPS jamming and electromagnetic interference has not only complicated Ukrainian operations but has also spilled over into neighbouring regions, highlighting how control of the electromagnetic spectrum has become a theatre-wide instrument of coercion.[54]

Ukraine has responded by integrating a diverse mix of conventional and unconventional assets. Unmanned aerial systems, ranging from improvised quadcopters to advanced strike drones, have been employed for surveillance, targeting, and direct attack. These systems have been combined with precision artillery provided by international partners to achieve rapid, localised effects against Russian positions. A critical enabler of Ukrainian resilience has been the use of commercial satellite services, which have ensured continuity of command and control when traditional military infrastructure was degraded. This improvisational approach has emphasised the importance of flexibility, redundancy, and the ability to rapidly adapt technology for battlefield use.[55]

Several lessons emerge for future multi-domain operations. First, electromagnetic spectrum dominance is as vital as control of the air or land, requiring states to invest in hardened communications and alternative navigation methods.

Second, the cost-exchange ratio of drones against high-end air-defence systems highlights the need for layered and distributed defence rather than exclusive reliance on strategic interceptors. Third, the role of commercial space and digital infrastructure have blurred the line between civilian and military domains, raising new questions of vulnerability and regulation. Finally, the conflict illustrates that speed, agility, and decentralised decision-making can offset material disadvantages, reinforcing the premium on adaptive doctrine and training in contested environments.

Pakistan's Path to Multi-Domain Operations

Strategic Necessity for MDOs

Airpower is a critical component of the Pakistan defence strategy that offers speed, range, and the means of controlling the vertical aspect of the battlefield. It protects the national airspace and allows land and marine forces to work efficiently. Air-delivered intelligence, surveillance and precision strike are increasingly becoming important to ground troops to achieve their missions, whereas air cover, anti-ship strike and airborne early warning are increasingly important to naval forces to secure sea lanes and discourage incursions. Airpower is not supportive in the strategic environment of Pakistan, but determining the operational liberation of all other environments, which is the heart of multi-domain integration.

In the South Asian context, Pakistan faces a numerically superior adversary in India. Traditional approaches based on conventional balance of power or force size are insufficient to ensure security. Multi-Domain Operations (MDO) offer a strategic framework to achieve capability overmatch by leveraging technology, doctrine, and integration rather than focusing on sheer numbers. For Pakistan, MDO is a strategic imperative to offset asymmetry, achieve qualitative parity, and maintain credible deterrence. By embracing this approach, Pakistan can convert constraints in resources into operational advantages and ensure its forces can respond rapidly and effectively across air, land, maritime, cyber, and space domains.[56]

PAF Initiatives and Modernisation

In 2010, the PAF initiated a shift towards MDOs, which was characterised by intended doctrinal, technological, and structural changes that focused on leaving behind platform-centric air power in favour of integrated use of air, land, sea, space and cyberspace.[57] In the following years, the focus of these activities involved networking sensors and shooters, hardening command and control structures, increasing electronic and cyber capabilities, and internalising operational experience in order to facilitate cross-domain convergence. The PAF has institutionalised MDO by incorporating air, cyber, space and EW capabilities to create a strong cohesive system of operations. This strategy does not merely mean possession of individual platforms, but to create a doctrine and a force structure, which serves as a force multiplier.

The modernisation programme is an amalgamation of indigenous development with a strategic alliance with China allowing the access to high-tech fighters like the J-10C and JF-17 Block III, air defence systems such as HQ-9B. These platforms with long-range precision weaponry, AESA radars and networked connectivity enable the Pakistani pilots to control the fights and blend into a networked combat cloud.[58] PAF training plays an exemplary role as it is crucial to ensure that the personnel are familiar with complex systems and are capable of working accurately and confidently in the conditions of real-time inter-domain fights.

Phases of Development

Three stages of development can be used to understand the way the PAF has gone to this posture. The initial period (1957-1967) was marked by the induction of competent aircraft like the F-86 Sabre and F-104 Starfighter that formed the base of Pakistan to gain tactical and strategic air superiority during conflicts with India. The second (1979-1989) phase is characterised by the emergence of force multipliers such as the F-16, sophisticated radar and weapons with beyond-visual-range capabilities, which greatly upgraded both the strike and defensive capabilities.

The third and decisive phase, which started in 2021, saw the complete transition of Pakistan to the multi-domain phase. When Air Chief Marshal Zaheer Ahmed Baber Sidhu took over as Chief of the Air Staff in 2021, he expedited the ongoing shift of the PAF to multi-domain warfare by focusing capability development on the new operational demands and indigenisation. His vision provided coherence and momentum to the evolving processes, turned conceptual foundations into operational systems and integrated multi-domain thinking into the fabric of force development, training and command systems. Understanding that air power could no longer exist in isolation, persistent investments were channelled into cyber operations, EW, space, air defence and unmanned systems, combined together with centralised command and control system. These efforts were further augmented with the creation of a Multi-domain Operations Centre (MDOC) and the National ISR and Air Operations Centre (NIIAOC), enabling the real time fusion of sensors, shooters and decision-making across domains, and contributing to a more modern force structure and organisational design.

It was also a period of rapid operationalisation of J-10C fighters, the introduction of PL-15 long-range missiles, CM-400 hypersonic strike complex, HQ-9BE High-to-Medium Air Defence (HIMAD) systems and advanced UAVs, all of which were integrated into a redefined doctrinal structure. Collectively, these reestablished the first-look, first-shoot capability of Pakistan and enabled the PAF to engage as a next-generation force based on speed, integration, and adaptability.[59]

PAF's Network-Centric Approach

The foundation of the network-centric approach of Pakistan is Command and Control, which combines radars, early warning sensors, shooters and decision-makers into a Common Operating Picture (COP) to allow quick, accurate and coordinated reaction across all areas. The main centre of this network that provides situational awareness and cohesion in operations is the Air Defence Operations Centre (ADOC) and the Air Operations Centre (AOC) located at the heart of it to plan, coordinate and execute air operations. This has been enhanced with the use of mobile C2 nodes, sophisticated radar systems and AI-based Decision Support Tools (DSTs) like the Next Generation Mobile Mission Control Centre (NG-MMCC), which has increased mobility, resilience and secure communications, and demonstrated the MDO principle of digital fusion.[60]

Institutionalising Multi-Domain Capabilities

To be able to function in harmony with air operations, the PAF also formally incorporated cyber, space, and EW capabilities. PAF has established individual cyber, space, EW, and UAV commands, which result in cumulative effects and defeat opponents despite an advantage in numbers. Pakistan can achieve plausible deterrence and operational superiority in a multi-domain space through networked operations, strengthened by training, advanced sensors, precision shooters and secure communications. Moreover, efforts are being made to integrate AI, exemplified by initiatives such as the Centre for Artificial Intelligence and Computing (CENTAIC).[61] In the coming years, Pakistan's indigenous UAV development is expected to play an increasingly significant role in shaping existing capabilities.[62]

Marka-e-Haq: A Case Study in Multi-Domain Warfare

Initial Engagement: The Night of 6-7 May

The conflict started on the evening of May 6-7, when India tried to take advantage of the element of surprise by using airborne BrahMos missiles and SCALP to launch standoff strikes while purposefully avoiding physical border incursions. India was supposed to be in charge of the timing, location, and intensity of this strategy. But for Pakistan, the window for engagement was very small, just five to seven minutes. To ensure that all sensors and shooters worked in unison, the nation responded using a centralised command network. When Pakistan's integrated kill chain turned the attack into a defensive scramble, India's offensive momentum swiftly vanished.

Execution of Multi-Domain Integration

Pakistan activated its multi-domain framework after Indian missiles were fired. While cyber operations cut off command links and slowed decision-making, EW assets jammed radars and interfered with communications.

In the meantime, space-based assistance caused disorder in enemy lines by disrupting situational awareness. Indian pilots were unable to receive support from ground control or airborne early warning and were left unprotected. In one hour, the fighters of Pakistan, especially J-10Cs with PL-15 missiles, took the initiative and shot down seven Indian planes, Rafales, Mirages, MiG-29s, and a Su-30. This, almost a 120-aircraft night encounter, was among the greatest beyond-visual-range battles ever fought.[63] The PAF effectively implemented MDOs combined with disciplined training and mastery of the platform, marking the first practical aerial demonstration of MDO.[64]

Drone Employment and Escalatory Dynamics

The Indian response after these failures changed gears on 8 May when it launched drone swarms to suppress and destroy Pakistani air defences. Pakistan responded by a mixture of EW and kinetic attacks, which were able to neutralise 88 drones without putting their most important assets at risk. India tried to take it a step further by launching more BrahMos missiles on 9 May and placing unmanned systems on Pakistani airbases. Although these attacks came close to a number of bases, they had minimal impact, which resulted in the very slight destruction of infrastructure.[65]

Operation Bunyan ul Marsoos: Pakistan's Counteroffensive

India, encouraged by war-fuelling rhetoric in its media, proceeded with provocative military activities, in spite of repeated warnings by Islamabad. Pakistan considered the attacks a serious threat to its sovereignty after intercepting BrahMos supersonic missiles that were directed against its military bases by India. In retaliation, the Pakistan Army quickly went on the offence. In response, on 10 May it initiated Operation Bunyan-ul-Marsoos, a joint operation by air and ground troops to restore deterrence and protect national security.[66] This combined operation dealt a counter blow by attacking several Indian targets of high value such as airbases, depots, S-400 batteries and command centres.[67] At the same time, cyber units in Pakistan launched a massive attack, disabling the Indian power grid, and crippling major networks. India had considerable IT resources and foreign assistance, but it failed to penetrate the defences of Pakistan. Protective systems like geofencing and cloud shielding helped with operational continuity but thousands of Indian digital assets were disrupted as a result of cyber operations.[68]

Lessons from War

The war proved that many of India's perceived technological capabilities including Rafale fighters, S-400 systems and BrahMos missiles could be neutralised through well-coordinated multi-domain operations. It also emphasised the use of drones, often regarded as a secondary asset, can have a decisive impact in the contested airspace. Most importantly,

Marka-e-Haq demonstrated that modern warfare is not characterised by platforms but the capacity to combine capabilities in the air, cyber, space, and electromagnetic environment to generate the cumulative effects. Marka-e-Haq was a breakthrough in the aerial defence posture of Pakistan. It showed that strategic dominance is not gained by numerical superiority but rather by integration, flexibility and precision. The performance of Pakistan demonstrated a shift from platform-focused to system-centric operations, connecting all relevant domains. The lesson that Pakistan can learn is that it has to put long-term investment in the doctrine, indigenous technology, and the expertise to make sure that future conflicts can be approached with the same level of adaptability and multi-domain perspective.[69]

Tri-Service Integration in MDO: Prospects and Challenges

Pakistan's Army, Navy, and Air Force have historically operated in silos, developing separate force structures, procurement priorities, and operational concepts. This service-centric approach has limited full interoperability and constrained the emergence of a coherent strategy. Command and control remain largely service-specific, and while institutional mechanisms exist, operational integration across services has been limited.[70]

However, recent operational experiences, notably Marka-e-Haq in April-May 2025, demonstrate the growing prospects for multi-domain coordination. During these operations, the PAF conducted Marka-e-Haq and executed precision strikes under the doctrine of proportionality and escalation control, while naval assets were repositioned pre-emptively to secure key sea lines of communication and project deterrence along the western seaboard. Simultaneously, the Army structures coordinated ground-based coverage of missiles and EW support, contributing to the strength of the air defence grid. These operations highlight that the tri-services are capable of collaborating effectively in an emergency situation, signalling the potential for more integrated multi-domain operations. Concurrently, they also indicate areas in which the coordination can be reinforced further, especially in real-time synchronisation and joint operational planning.[71]

Historically, there were joint exercises which were undertaken on an annual or biannual basis, and the main purpose was to ensure efficiency and operational preparedness.[72] In modern multi-domain operations, however, there is now a need to plan these exercises around MDO concepts, with land, air, sea, cyber, and space domains being integrated to reflect the pace, complexity and interconnectedness of the current conflict conditions. Moreover, the air domain remains central to tri-service integration, serving as both an independent strategic instrument and the enabler of cross-domain operations. The intelligence gathering capacities, the speed of targeting, and EW all form the foundation of the operational cohesion of the armed forces of Pakistan, coordinating joint actions of the military forces are timely and effective even in the most complicated scenarios.

Recommendations

Drawing on operational insights from the May 2025 war with India, particularly in airpower and MDOs, the following recommendations are proposed to guide Pakistan's future strategic planning.

- **Establish an Integrated Command System**: An integrated command system must be institutionalised to synchronise planning, capability development, and operations across the Army, Navy, and Air Force, incorporating multi-domain elements. This would enable joint prioritisation of platforms, sensors, and C2 networks, validate joint doctrines, enhance interoperability, and improve situational awareness across services, while maintaining each service's unique operational strengths and addressing hybrid and grey-zone threats.
- **Institutionalise Tri-Service Strategic Foresight and Adaptive Training**: A coordinated training programme must be developed across the tri-Service to build awareness of the enduring nature of war and its evolving character, including hybrid, cyber and information-based threats. Through joint scenario-based exercises, the services can develop anticipatory planning skills and a shared understanding of multi-domain operations, enhancing responsiveness and cohesion across all domains.
- **Network-Centric Integration of Emerging Technologies**: The PAF has already taken the lead in institutionalising advanced technologies such as AI, autonomous systems, and space-based ISR, but this integration must extend across the Army and Navy. Applying the principles of Network-Centric Warfare (NCW) would network dispersed sensors, decision-makers and shooters into a unified system, enabling faster decisions, shared awareness, and cooperative effects. Embedding this approach across all services would turn technological progress into actionable combat power, strengthening agility and cohesion in Pakistan's future MDO posture.
- **Roadmap for Technological Development**: Grounded in the logic of technological determinism, Pakistan must recognise that technological advancements are key to shaping the future of MDOs. A phased approach can be pursued in parallel through indigenous efforts and external partnerships: first acquiring and securing critical systems, then adapting and upgrading them through technological adaptation, and ultimately moving towards innovation. Sustained investment in research and development (R&D) should underpin this process to ensure long-term technological self-reliance.

Conclusion

The evolution of warfare into the multi-domain era compels Pakistan to sustain and further consolidate its trajectory of jointness and technological integration.

The May 2025 war demonstrated that decisive outcomes are achieved through the coordinated employment of all services within a unified operational framework. When harmonised, their distinctive capabilities generate effects that multiply rather than merely add to one another, producing a force greater than the sum of its parts.

Pakistan has already made significant progress in the form of doctrinal reforms, joint training, and the development of network-enabled operations. The challenge now remains to institutionalise these efforts with enduring practice to ensure that interoperability becomes institutionalised at all levels of command. This would entail building a common culture of trust, aligning command frameworks and continued modernisation of doctrine, technology and human resources.

Through this direction, Pakistan will be able to make sure that its deterrence posture is not only credible, but also resilient, aided by the synergistic combination of land, sea, air, cyber, and space capabilities. In the future, multi-domain effectiveness will be crucial in a strategic environment that is influenced by hybrid threats, regional tensions, and constant technological dynamism. The future of national security, thus, lies in ensuring the already attained momentum is turned into a long-term and highly integrated culture of tri-service synergy; that way, Pakistan will be able to remain adaptive and effective in the era of the everywhere battlefield.

References

[1] Héloïse Fayet and Leo PÉRIA-PEIGNÉ, *Deep Precision Strikes: A New Tool for Strategic Competition*, 2024.

[2] Ruben Stewart, 'The Shifting Battlefield: Technology, Tactics, and the Risk of Blurring Lines in Warfare', *Humanitarian Law & Policy Blog*, 22 May 2025, https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/.

[3] Albert Palazzo, *When Joint Is Not Enough, Is Multi-Domain the Answer*, 2016, https://archive.smallwarsjournal.com/jrnl/art/when-joint-is-not-enough-is-multi-domain-the-answer.

[4] Lt Col Heiner Grest and Lt Col Henry Heren, *Space Operations - Joint Air Power Competence Centre*, 16 January 2021, https://www.japcc.org/chapters/c-uas-space-operations/.

[5] Col William J. Poirier and Maj James Lotspeich, *Air Force Cyber Warfare: Now and the Future*, 2013.

[6] Ali Mustopo, Rudy AG Gultom, and Oktaheroe Ramsi, 'Air Defense Transformation: Strategy in the Context of Multi-Domain Operations', *ResearchGate*, ahead of print, 21 August 2025, https://doi.org/10.55927/fjas.v4i7.237.

[7] David E. Johnson, *The Importance of Land Warfare: This Kind of War Redux*, 2018.

[8] JAPCC, *Multi-Domain Operations and Challenges to Air Power - Joint Air Power Competence Centre*, 27 June 2019, https://www.japcc.org/essays/multi-domain-operations-and-challenges-to-air-power/.

[9] Didier Tisseyre, 'Cyber and Military Action in the Air and in Space', 2019, https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=120&cidcahier=1183.

[10] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority.:* (Fort Belvoir, VA: Defense Technical Information Center, 2000), https://doi.org/10.21236/ADA406255.

[11] Pk Mallick, '(PDF) NETWORK CENTRIC WARFARE', ResearchGate, 2020, https://www.researchgate.net/publication/344737587_NETWORK_CENTRIC_WARFARE.

[12] NATO, 'Multi-Domain Operations and Digital Transformation: Enabling Converged Effects in the Modern Battlespace - NATO's ACT', 2025, https://www.act.nato.int/article/mdo-dt-enabling-converging-effects/.

[13] M. Matheswaran, *NETWORK-CENTRIC WARFARE AND ITS STRATEGIC IMPLICATIONS*, 2007, https://capsindia.org/wp-content/uploads/2022/10/M.-Matheswaran.pdf.

[14] *Author's Compilation.*, 2025.

[15] Matheswaran, *NETWORK-CENTRIC WARFARE AND ITS STRATEGIC IMPLICATIONS*.

[16] Aviation and Defense Market Reports, *Network-Centric Warfare: The Future Of Modern Conflict*, 2 June 2025, https://aviationanddefensemarketreports.com/network-centric-warfare-the-future-of-modern-conflict/.

[17] Radovan Vasicek and Ondřej Kačmařík, 'The Multi-Domain Approach to Military Operations and Its Challenges to Intelligence and Intelligence, Surveillance, Reconnaissance', *ResearchGate*, ahead of print, 2024, https://doi.org/10.3849/cndcgs.2024.357.

[18] Mihael Plevnik and Pavel Vuk, 'Navigating the Uncertainty of the Modern Environment: Multi-Domain Operations for the Defence of Small States', *European Security* 0, no. 0 (2025): 1–28, https://doi.org/10.1080/09662839.2025.2540955.

[19] Maj. Jesse L. Skates, *Multi-Domain Operations at Division and Below*, 2020, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Skates-Multi-Domain-Ops-1.pdf.

[20] Ludovico Caprio et al., *NATO Multi-Domain Operations: Challengesfor the European Land Forces* (2024), https://finabel.org/wp-content/uploads/2024/08/FFT-NATO-final.pdf.

[21] Congressional Research Service, *Defense Primer: Army Multi-Domain Operations (MDO)* (2024), https://sgp.fas.org/crs/natsec/IF11409.pdf.

[22] *Author's Compilation.*

[23] Dave Roos, 'How Airplanes Were Used in World War I | HISTORY', 2022, https://www.history.com/articles/world-war-i-aviation-airplanes.

[24] Lt Col Francesco Esposito, *Precision-Guided Munitions of the Future - Joint Air Power Competence Centre*, 10 December 2019, https://www.japcc.org/articles/precision-guided-munitions-of-the-future/.

[25] Lynn Dsouza, 'The Role of Air Power in Modern Military Strategy', 2024, https://www.linkedin.com/pulse/role-air-power-modern-military-strategy-espiridi-zsdaf.

[26] lJános Csengeri, *Some Elements of Multi-Domain Operations Regarding Air Power*, 2022, https://stumejournals.com/journals/confsec/2022/1/11.full.pdf.

[27] Air Cdre Haider Raza, Director Emerging Technologies, Centre for Aerospace & Security Studies, Islamabad, 'Interview by the Author', 2025.

[28] Steven A. Walton, 'Technological Determinism(s) and the Study of War', *ResearchGate*, ahead of print, 2019, https://doi.org/10.1163/22134603-00701003.

[29] Lt Col Gaurav Kumar Singh, *Technology-Driven-Multi-Domain-Operations-MDO-for-Joint-Warfighting*, 2024, https://cenjows.in/wp-content/uploads/2024/10/6-Technology-Driven-Multi-Domain-Operations-MDO-for-Joint-Warfighting-by-Lt-Col-Gaurav-Kumar-Singh.pdf.

[30] VIAVI, *Mission-Ready 5G From Lab to Battlefield* (2025), https://www.viavisolutions.com/en-us/literature/mission-ready-5g-lab-battlefield-brochures-en.pdf.

[31] Aviation and Defense Market Reports, *C4ISR Systems : Navigating the Future of C4ISR Insights*, 22 April 2024, https://aviationanddefensemarketreports.com/c4isr-systems-nsights-navigating-the-future-of-command-control-communications-computers-intelligence-surveillance-and-reconnaissance/.

[32] Isabella T. Grant, 'Space And Electronic Warfare Reimagined', *TDHJ.Org*, 19 May 2025, https://tdhj.org/blog/post/space-electronic-warfare/.
[33] UAV Navigation, 'Multi-Domain Operations and UAVs', 2022, https://www.uavnavigation.com/company/blog/multi-domain-operations-and-uavs.
[34] Matilde Gamba, 'Above the Battlefield: The Threat of UAVs in the Hands of VNAs', *GNET*, 24 June 2025, https://gnet-research.org/2025/06/24/above-the-battlefield-the-threat-of-uavs-in-the-hands-of-vnas/.
[35] Syed Agha Hassnain Mohsan et al., 'Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review', *Drones* 6, no. 6 (June 2022): 147, https://doi.org/10.3390/drones6060147.
[36] Air Cdre Imran, Programme Director, PUF, 'Interview by the Author', 2025.
[37] Air Cdre Haider Raza, Director Emerging Technologies, Centre for Aerospace & Security Studies, Islamabad, 'Interview by the Author'.
[38] John J. Klein, *Space and Cyber Warfare as One*, 31 October 2024, https://www.csis.org/analysis/space-and-cyber-warfare-one.
[39] Xiangjun Li et al., 'Overview of Jamming Technology for Satellite Navigation', *Machines* 11, no. 7 (July 2023): 768, https://doi.org/10.3390/machines11070768.
[40] Muharman Lubis et al., 'Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience', *Sensors* 25, no. 15 (January 2025): 4545, https://doi.org/10.3390/s25154545.
[41] Tyler Wesley, 'Multi-Domain Operations and Lessons from NSC 68 in the Competitive Space: A Framework for NATO and Western Democracies for Defence Against Russia', *The RUSI Journal* 165, no. 4 (September 2020): 22–31, https://doi.org/10.1080/03071847.2020.1811140.
[42] Samit D'Cunha, Tristan Ferraro, and Tilman Rodenhäuser, '"Hybrid Threats", "Grey Zones", "Competition", and "Proxies": When Is It Actually War?', 2025, https://blogs.icrc.org/law-and-policy/2025/01/16/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/.
[43] Robert Shawlinski, James Perdue, and SGM Clayton dos Santos, 'The Importance of Leadership in Multidomain Operations • The Havok Journal', 2024, https://havokjournal.com/culture/military/the-importance-of-leadership-in-multidomain-operations/.
[44] Department of Defense, *Summary of the Joint All-Domain Command and Control Strategy* (2022), https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.
[45] Timothy Marler et al., *What Is JADC2, and How Does It Relate to Training? An Air Force Perspective on Joint All Domain Command and Control* (RAND Corporation, 2022), https://doi.org/10.7249/PEA985-1.
[46] Tim Ryan, 'JADC2: The Role for Space | The Air Power Journal', *Shift Paradigm.*, 20 May 2023, https://theairpowerjournal.com/joint-all-domain-command-and-control-the-role-for-space/.
[47] Chip Downing, 'JADC2: Enabling the Data-Centric Enterprise', 2023, https://www.rti.com/blog/jadc2-enabling-the-data-centric-enterprise.
[48] Department of Defense, *Summary of the Joint All-Domain Command and Control Strategy*.
[49] Sugiura Yasuyuki, *The PLA's Pursuit of Enhanced Joint Operations Capabilities*, 2022.
[50] Yasuyuki.
[51] John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, 2018, https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1006&context=china-strategic-perspectives.
[52] Meia Nouwens, 'China's New Information Support Force', IISS, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/.
[53] US Department of Defense, *Military and Security Developments Involving the People's Republic of China 2024*, 2024, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.
[54] Oleksandr Stashevskyi and Frank Bajak, 'Deadly Secret: Electronic Warfare Shapes Russia-Ukraine War | AP News', 2022, https://apnews.com/article/russia-ukraine-kyiv-technology-90d760f01105b9aaf1886427dbfba917.
[55] Thibault Spirlet, 'Russia Really Wants to Stop Ukraine Using Elon Musk's Starlink Satellites', Business Insider, 2024, https://www.businessinsider.com/russia-stop-ukraine-using-elon-musk-starlink-satellites-2024-1.
[56] CASS Lahore, *Dominating the Skies: Strategic Use of the Air Medium in Modern Conflicts* (2025), https://casslhr.com/psr/dominating-the-skies-strategic-use-of-air-medium-in-modern-conflicts/.
[57] Syed Ali Hamid, 'From Humble Wings to Strategic Supremacy', August 2025, https://tribune.com.pk/story/2562902/from-humble-wings-to-strategic-supremacy.
[58] CASS Lahore, *Dominating the Skies: Strategic Use of the Air Medium in Modern Conflicts*.
[59] CASS Lahore.
[60] Muhammad Khan, 'PAF's Central Nervous System – Second To None', 2024, https://secondtonone.com.pk/2024/05/17/pafs-central-nervous-system/.
[61] S. Khalil, *CENTAIC's Transformation Under PAF NASTP – Second To None*, 10 May 2024, https://secondtonone.com.pk/2024/05/10/centaics-transformation-under-paf-nastp/.
[62] Air Cdre Imran, Programme Director, PUF, 'Interview by the Author'.
[63] CASS Lahore, *Dominating the Skies: Strategic Use of the Air Medium in Modern Conflicts*.
[64] Dawn, 'Pakistan Successfully Emerged as "Regional Stabiliser" Following "Marka-i-Haq", Says PAF Chief', https://www.dawn.com/news/1958756.
[65] CASS Lahore, *Dominating the Skies: Strategic Use of the Air Medium in Modern Conflicts*.

[66] The Nation, 'Pakistan Launches "Operation Bunyan Ul Marsoos" against India after Multiple Provocations', The Nation, 10 May 2025, https://www.nation.com.pk/10-May-2025/pakistan-launches-counter-offensive-against-india-after-multiple-provocations.

[67] Aik News, 'Operation Bunyan-Un-Marsus: 5. BrahMos Sites, Airbases in India Face Heavy Damage in Counter-Strike', https://www.aiknewshd.tv/250510001 8-operation-bunyanunmarsus-pakistan-destroys-indian-airbases-missile-depots-s400-system.

[68] CASS Lahore, *Artificial Intelligence, Electronic Warfare & Cyber Warfare, and Unmanned Aerial Systems: A New Paradigm of Next-Generation Aerial War* (2025), https://casslhr.com/psr/artificial-intelligence-electronic-cyber-warfare-and-unmanned-aerial-systems-a-new-paradigm-of-next-generation-aerial-war/.

[69] CASS Lahore, *Dominating the Skies: Strategic Use of the Air Medium in Modern Conflicts*.

[70] CASS Lahore, *Military Interoperability Amid the Changing Character of War: Transforming Pakistan's Defence in the Modern Conflict Environment* (2025), https://casslhr.com/psr/military-interoperability-amid-the-changing-character-of-war-transforming-pakistans-defence-in-the-modern-conflict-environment/.

[71] CASS Lahore.

[72] PAKDEFENSE, *PAKISTAN NAVY Biennially TRI-SERVICES Strategic War Games Shamsheer-e-Bahr IX Kicks Off In Karachi*, 8 August 2023, https://www.pakdefense.com/blog/pakistan-navy/pakistan-navy-biennially-tri-services-strategic-war-games-shamsheer-e-bahr-ix-kicks-off-in-karachi/.