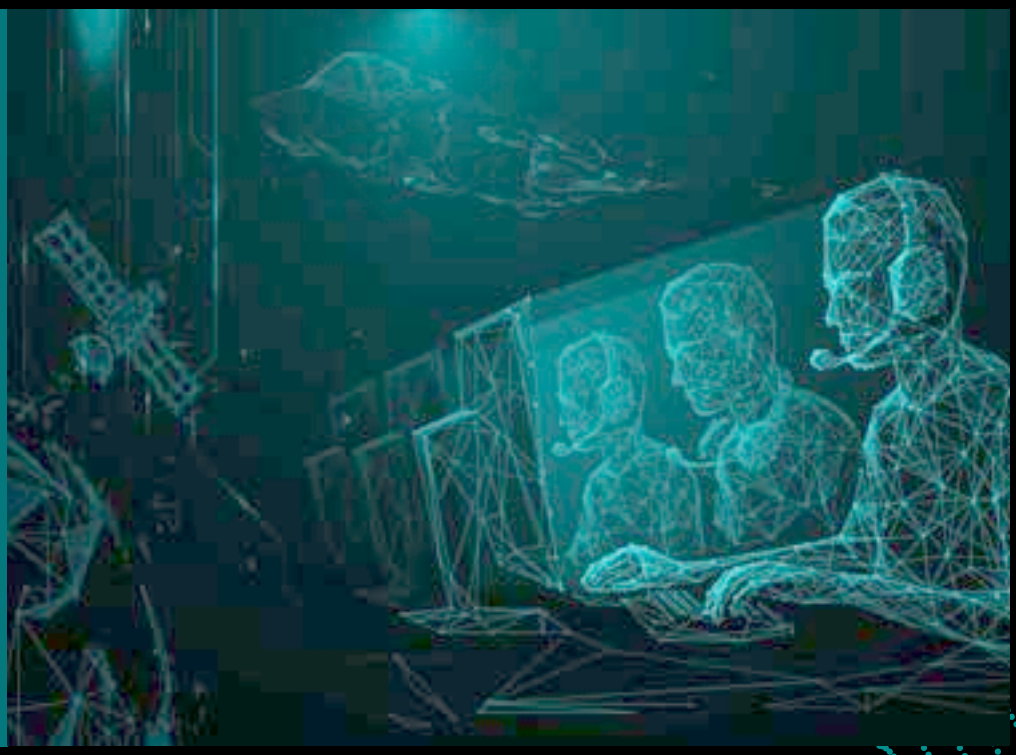
THE
AIR POWER
REPORT

Transitioning to
Multi-Domain Operations



SPPS

Think Ahead.

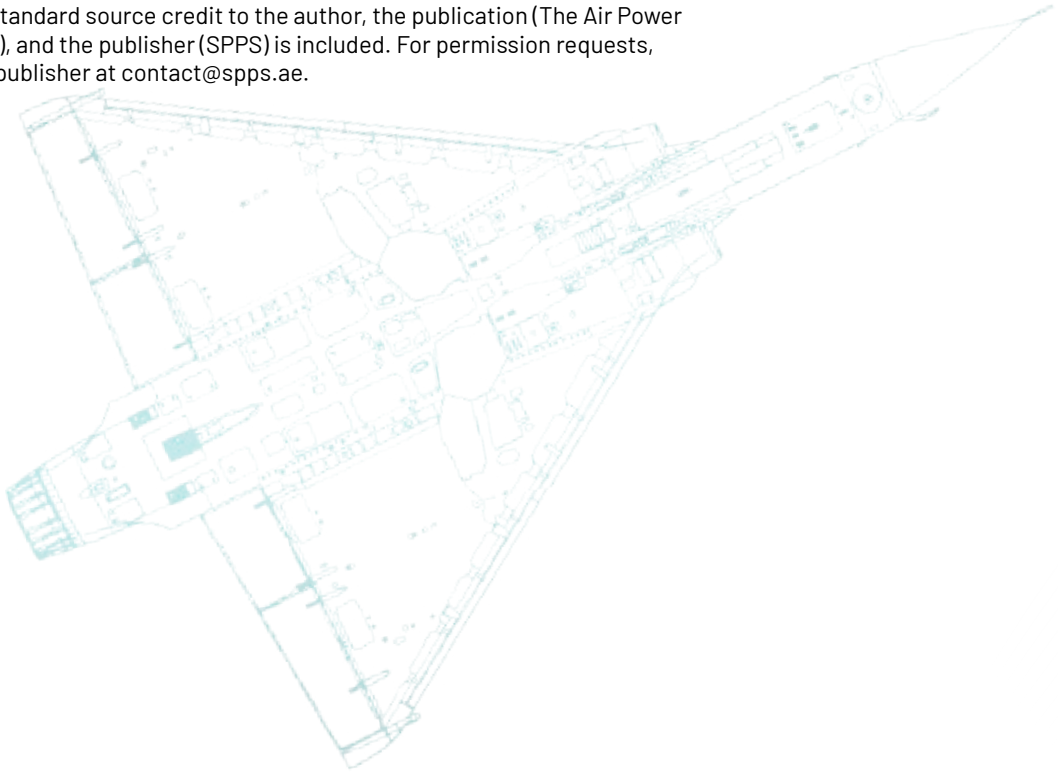
www.spps.ae

This report was published by SPPS in January 2022.

Disclaimer

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. It would be best if you did not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, SPPS, its members, and employees do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else refraining to act in reliance on the information contained in this publication or for any decision based on it.

Release



Overview

Air forces will operate in a multi-polar world characterized by persistent, sub-threshold engagements where a multi-layered and multi-speed battlespace will be stretched across huge distances. The ability to outpace threats in real-time will demand agility from the air force not just in moving assets and personnel but also, crucially, information. Unlocking future operational advantage, therefore, hinges on the ability of air forces to enhance connectivity and integration across force, allied, and partner elements so that information-sharing can occur faster and more widely than ever before. The increasing digitization of military operations has profound implications, particularly for command and control (C2) and battle management (BM). The functional distribution of Air Operations Centers (AOCs) is one game-changing early development in this direction, whereas the emergence of shared digital environments and combat clouds allude to new agile and collaborative operational approaches becoming possible.

Air forces are already critically reliant on the ability to operate across the operational domains, but these are all becoming increasingly cluttered and contested. Multi-domain operations (MDO) provide the lead-in to new operational constructs that will radically improve joint effectiveness. MDO promises to make air forces more adaptive and rapidly transition from synchronization to coordination to unleash multi-domain effects. As MDO fuses the delivery of air power with the space and cyberspace domains, formulating a military space strategy and constituting a dedicated space command are essential preliminary steps toward harnessing the space domain. A shared space capability architecture offers the best pathway for allies and partners to meet future military requirements in space. On the other hand, increasing reliance on cyberspace will introduce new types of threats, and information warfighting will take a place alongside traditional warfighting functions.

The ability to absorb emerging technologies and innovation more broadly will be critical to future joint and coalition warfighting effectiveness. To achieve integrated deterrence holistically, efforts to enhance interoperability must be refocused at the multinational level. Considering interoperability at the design phase of planning future capability is essential, together with adequately aligned doctrine, concept of operations (CONOPS), and tactics, techniques, and procedures (TTPs). However, deepening trust levels between allies and partners will be critical as the role of strategic partnerships underpinned by a new culture of collaboration and information-sharing are imperative. To succeed at MDO and become able to think, fight, and win across the length, breadth, and height of the modern battlespace, air forces will need to fundamentally transform the networks, systems, and processes they use, as well as their ways of working more broadly.

Contents

The Strategic Backdrop 3

The Operational Environment 3

The Transition to Multi-Domain Operations 4

The Digitization of Military Operations 5

The Functional Distribution of Air Operations Centers 6

Command, Control and Battle Management in Multi-Domain Operations 7

Agile and Collaborative Combat 9

Interoperability and Coalition Effectiveness 10

Trust and Information-Sharing 12

The Cyberspace Domain and Information Warfighting 13

Harnessing the Space Domain 15

Building a Military Space Strategy 16

The Dedicated Space Command 17

Absorbing Emerging Technologies and Harnessing Innovation 18

The Way Forward 20

The Strategic Backdrop

Global competition is at a new crossroads as state-based competition once again becomes the norm. The future strategic environment will give rise to new forms of competition as a nexus of adversaries, including non-state actors such as terrorist groups, insurgents, mercenaries, and cybercriminals, align and employ all instruments of power to erode resilience and undermine cohesion between allies and partners. Adversaries will engage in legal and illegal activities across the physical and virtual domains, blurring the distinction between peace and war on the one hand and home and away on the other. Traditional approaches to defense will be fundamentally challenged by threats that may not recognize national borders or subscribe to international norms and practices.

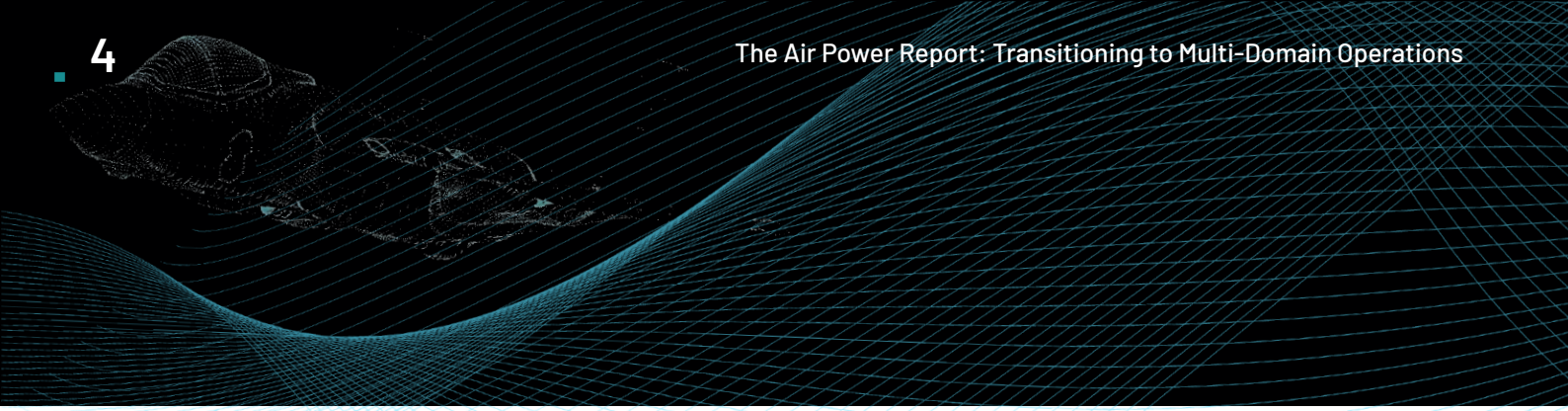
Air forces will operate in a multi-polar world characterized by persistent, sub-threshold engagements where the battlespace is stretched across huge distances. As a service that is continuously active in operations – conducting training and exercises, assurance missions, or in transit – to maintain round-the-clock mission readiness, the future challenge for air forces is especially pronounced. The introduction of a multi-layered and multi-speed battlespace fundamentally disrupts the economics and the character of warfare. In response, air forces need to accelerate change and build the capabilities for a new way of warfare allowing them to be successful in a highly complex and stretched competition continuum in the future – or risk becoming redundant.

The Operational Environment

With adversaries employing advanced network and weapon systems capabilities in dense anti-access/area denial (A2AD) environments, the competition continuum will become highly contested, cluttered, and constrained. The full spectrum of assurance and combat missions performed by air forces will become more convoluted as air operations centers (AOCs), command and control (C2) nodes, and traditional airborne platforms are driven further away from the fight. Consequently, air forces will need new approaches for survivability and delivering effects at the speed of relevance in dense threat environments. Air forces will need to become highly adaptive and able to transition from coordination to synchronization rapidly enough to outpace threats in real-time in high-tempo operational environments with agility not just in moving assets and personnel but also – crucially – information.

"Air forces will need to become highly adaptive and able to transition from coordination to synchronization rapidly enough to outpace threats in real-time in high-tempo operational environments with agility not just in moving assets and personnel but also - crucially - information."

Contemporary threats move too quickly, and connectivity through electronic means is essential since operations can no longer be effectively coordinated at a liaison level. Consider, for example, the relationship between combined air operations centers (CAOCs) and air defense operations centers (ADOCs), which



is not always clearly defined as headquarters may separate operational C2 elements in terms of defensive counter-air and area air defense. Conventional and emerging air and missile threats threaten in different ways, and defense against them may belong to different command authorities. As one threat profile may be too large for a ground commander but also too small for an air combat commander, a seamlessly integrated multi-layered, all-domain operational architecture is necessary for generating shared situational awareness (SA) and ensuring the right shooter is allocated to the respective incoming threat target under the appropriate authority.

The outcomes of future conflicts will be determined in favor of air forces that command information superiority across a competition continuum where the operational domains are fused rather than based on superior weapons systems and standalone capabilities. The unlocking of new operational advantages will hinge on the ability of air forces to enhance connectivity and integration between force elements so that information-sharing can occur faster and more widely than ever before. To enable more robust coordination, command structures and relationships will need to be adapted and even redefined for a new way of warfare. Multi-domain operations (MDO) provide the lead-in for air forces to a new operational command, control, and battle management (C2BM) in the future, which promises to radically improve joint effectiveness in synchronizing force elements and coordinating effects acrossa multi-domain battlespace in ways previously not possible.

The Transition to Multi-Domain Operations (MDO)

The multi-domain operations (MDO) concept is distinct from joint and combined ones in that it proposes the execution of effects-based, synchronized, and tactically-integrated missions across the operational domains, thereby allowing air forces to think, fight, and win across the length, breadth, and height of the modern battlespace. In transitioning to MDO, air forces will need to fundamentally transform the networks, systems, and processes they use and, more broadly, their ways of working. To operate at the speed of relevance, commanders across all levels will need access to robust, continuously updated SA, delivered as a joint common operational picture (COP) to gain a better understanding of the operational environment than adversaries. Additionally, the ability to collect, store, analyze, fuse, distribute, and visualize information from classified and open-source data and intelligence streams for faster decision-making at the lowest levels possible will be vital to operational success.

> ***"In its current configuration, operational C2 remains too manual and incompatible with the tremendous amounts of data and information becoming available as sensors and shooters are merged into a single, master-grid network."***

However, the same wealth of information that can create operational advantages may also overwhelm decision-making processes if it is not adequately filtered and managed.

Beyond simply positioning every sensor integrally into a network and integrating tracked data from multiple sources to share in real-time, it is imperative that data and information streams continuously flowing to commanders are *intelligently* fused and shared so that only data and information that is relevant to a given mission or operational requirement is provisioned. Guarding against the dangers of information burden and cognition overload for commanders and warfighters will be crucial in an age where information is power and can move faster and further than ever but where there is too much data and information to process and absorb. New digital solutions and toolkits are therefore needed, which exploit automation and artificial intelligence (AI) to support information visualization for better understanding and improved decision-making.

The Digitization of Military Operations

Information superiority will be decisive for air forces in converting strategic intent into timely operational and tactical effects orchestrated across the fluid operational domains of the modern battlespace. Toolkits to manage, analyze, fuse, visualize, and, crucially, to better understand massive amounts of information generated from multi-source intelligence streams will redefine operational planning and execution in the years ahead. Air forces will need to harness emerging technologies to shape the digital dimension of the modern warfare environment as a new operational C2 that can support performance at the level the future battlespace demands is evolved. In its current configuration, operational C2 remains too manual and incompatible with the tremendous amounts of data and information becoming available as an increasing number of sensors and shooters are merged into a single master-grid network.

Legacy C2 doctrines, structures, and processes, which can be based on decision-making time cycles of 24 hours, will not suffice against future disruptive threats and the expected pace of operations. No technological advancement can make legacy C2 adequately effective for the anticipated pace of future operations. AI, automation, augmented reality, and quantum technologies present new possibilities for filtering, visualizing, and helping make sense of tremendous amounts of information. Data analytics and fusion engines exploiting big data processing produce new opportunities for individual platforms, capabilities, and decision-makers to integrate into a shared digital environment from a joint and pan-government perspective.

> ***"The development of a shared digital environment between commanders and warfighters will make possible the decentralization of operational C2 and a geographical point-to-point distribution of traditional AOC functions."***

A shared digital environment and the actualization of combat clouds will make it possible for force elements and users in any location to access the same streams of data and information, whether for operational planning or execution, in real-time and at the same rate as those executing missions. Digital toolkits

that are highly adaptable to meet the needs of changing mission requirements will need to become readily available on secure combat clouds and accessible on-demand using military credentials to aid better and faster decision-making across all levels. Developing a shared digital environment between commanders and warfighters will make possible the decentralization of operational C2 and a geographical point-to-point distribution of traditional AOC functions.

The Functional Distribution of AOCs

Distributed AOCs can be understood as being in different places simultaneously, rather than in one place or another, and represent a game-changer for how air forces will operate in the future. AOCs have traditionally been operated by air forces from a single fixed location housing significant infrastructure allowing high volumes of communications to be received and hosting a large number of multi-specialty personnel. Such a centralized model for C2 has served air forces well in the past. However, as the threat landscape evolves, the notion of a single fixed location from where operational C2 is executed makes air operations increasingly vulnerable to adversaries capable of targeting these critical nodes through a range of kinetic and non-kinetic means. The same risks exist in scenarios where natural disasters, fire, or power outages at any centralized location receiving critical communications and providing operational C2 become potential single points of failure.

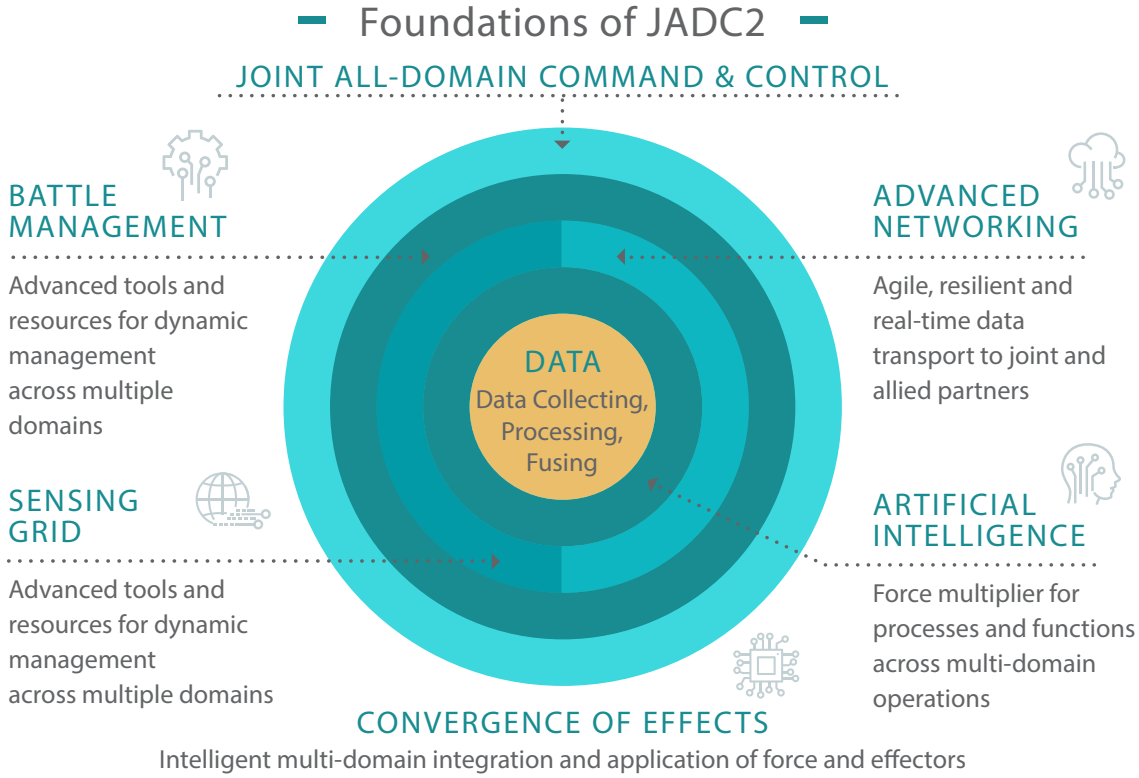
A point-to-point distribution of AOCs delivers better alignment with higher elements of command that may be positioned in different locations and, in coalition scenarios, different regions of the world. Distributed AOCs also make it possible for air forces to connect with a more diverse pool of expertise – routinely needed at more than one place at any given time – to solve complex operational challenges. Air forces will gain decisive advantages from minimizing the need to work off-cycle to get information where and when it is needed and, crucially, build redundancy to become more operationally resilient. As AOC functions are distributed, air forces will be enabled to adapt more quickly to changing demands in dynamic operational scenarios, including any potential loss of critical nodes in the C2 network, thereby making it possible for edge warfighters to continue operating securely with agility.

The most significant force multiplier effect promised by a distributed AOC architecture is making it possible for air forces to seamlessly tie into partner elements and capabilities positioned at different locations. Bringing together allied and partner AOCs positioned across different locations virtually will allow air forces to aggregate available coalition capabilities to leverage the most efficient and lethal mix of air power at any given time and place. The reality and everyday challenges of air forces being individually stressed for resources or personnel can be mitigated by consolidating coalition capabilities to amplify power and deliver integrated deterrence. Air forces will therefore rely less on the individual capabilities of exquisite platforms and more on the strength of a shared capability architecture with integrated operational C2 that radically optimizes sensor/shooter tasking and allocation.

C2BM in MDO

As part of processes to direct tasks and increase the pace of operations by replacing legacy approaches that slow down operational cycles – and therefore reaction times – clear delegations to each level of command must be made to allow the prioritization of decision-making at the lowest level possible. A single commander connected to an agile, adaptive, and assured network that receives data and relays commands should be able to direct the activities of subordinate units exclusively. It will remain essential that orders for the delivery of operational capability can be adequately prioritized. In this regard, a future challenge relates to who commands the commanders – particularly in scenarios where there are apparent pressures for multiple arms of government to be included in the C2 decision-making process. Even where delegated authority remains unchanged, the model for centralized control/decentralized execution and mission command may be challenged, so it will be essential that air forces can update formal relationships and ways of doing business.

> ***"It will remain essential that orders for the delivery of operational capability can be adequately prioritized. In this regard, a future challenge relates to who commands the commanders - particularly in scenarios where there are apparent pressures for multiple arms of government to be included in the C2 decision-making process."***



Open architecture, system-of-systems (SoS) networks designed for high-speed, high-volume data exchanges across a broad and dispersed user base will be essential for provisioning relevant information to the right person where and when needed. Link 16, which provides a common standard for connectivity and interoperability, will remain vital for coalition operations but may not be sufficient even with a holistic modernization program implemented across all users. The rationale for a more powerful operational C2 has driven the development of the joint all-domain command and control (JADC2) construct and Advanced Battle Management System (ABMS) in the United States. JADC2 envisions sensors, shooters, and support platforms across the force being connected to a master grid network so that operational C2 is effectively advanced from a service-centric architecture into a highly flexible, joint all-domain one. The United States Air Force intends to leverage JADC2 for the real-time fusion of data from a myriad of disparate sources, whereas ABMS intends to sense, make sense of and allow commanders to act faster than adversaries by connecting the right sensor to the right shooter.

In a future where no single platform or weapon system will be able to ensure operational success, JADC2 and ABMS aim to systemically mitigate the limitations of individual component systems with the strengths of others. Platforms not plugged into ABMS, or an equivalent battle management (BM) system, will have low survivability and ultimately become redundant. JADC2 and ABMS, which have underpinned combat success for the United States in every wargame scenario for the future, provide a basis for the operational C2 of the future that connects the right sensor to the right shooter. Developing a highly scalable, fully-integrated, and multi-classification network architecture with clearly defined delegations will be vital in achieving information superiority across the air power enterprise, allowing commanders and warfighters to perform more effectively and efficiently. Current networks and systems need to be modernized and adapted to achieve a greater degree of information about the battlespace. However, full network integration presents considerable technical challenges as individual systems do not always speak a common language or interconnect smoothly, particularly in the multinational context involving allied and partner air forces.

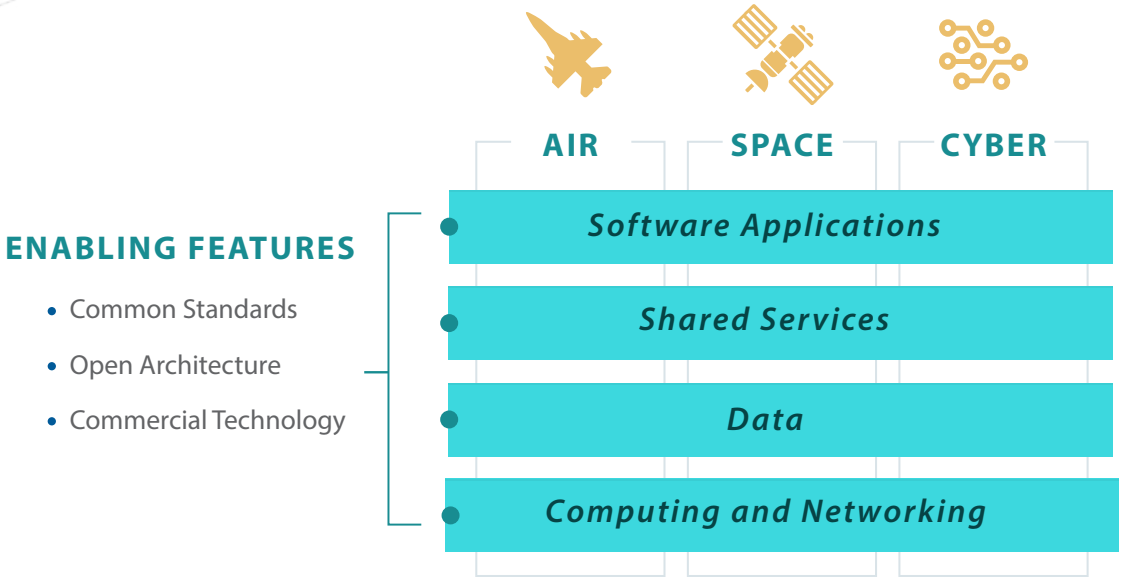
Agile and Collaborative Combat

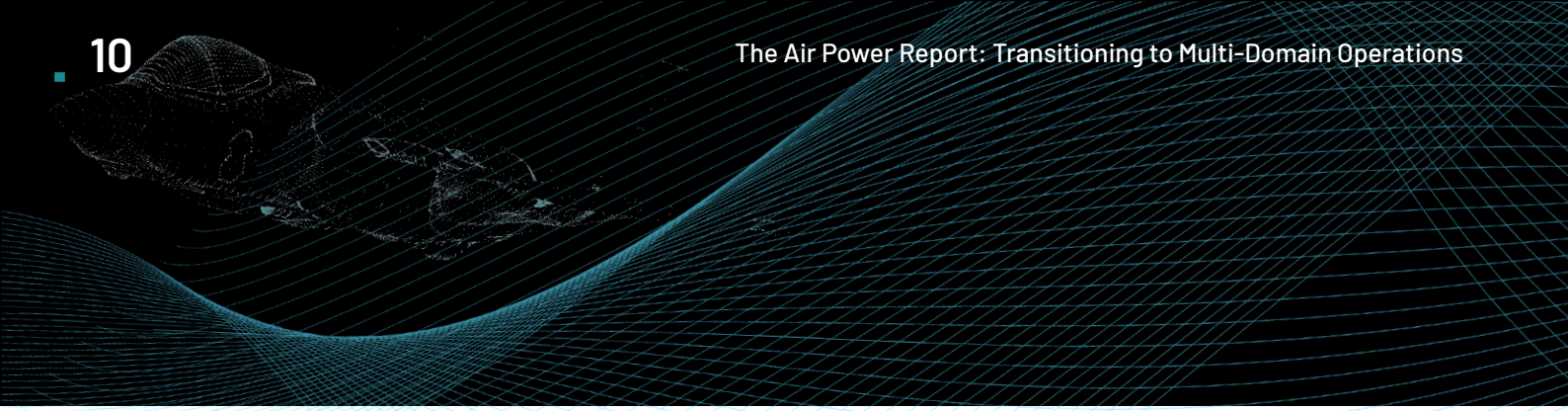
Interoperability is vital in future warfare, and the step towards collaborative combat envisions information exchange across all platforms, not only combat platforms. Going beyond legacy fighters being led by new command-capable fighters, as fifth-generation aircraft make possible, interoperability will need to extend across all platforms, including remotely piloted vehicles (RPVs) and autonomous systems. Interoperability with integrated planning and operational C2 under a robust joint mission command will allow the operational acceleration necessary to overcome adversaries with advanced network capabilities and weapon systems of their own. Adapting legacy systems into a single grid, multi-domain network is the most crucial impending challenge for air forces. A strategic shift must be made to prioritize full network integration and interoperability with the necessary financial resources, time, and personnel.

> **Information superiority can be converted into a decisive combat advantage through rapid exploitation while simultaneously preventing adversaries from the same.**

Integration poses complex challenges, and results can take longer to achieve than expected, as previous national experiences with adopting, adapting, and implementing modifications on Link 16 have demonstrated. Air forces must pressure industry partners to adopt standardization for data protocols and systems engineering more broadly so that interoperability at the level necessary can be achieved effectively and efficiently in the future. At the same time, air forces must break down

Elements of Interoperability in Multi-Domain Operations





parochial ways of thinking, archaic policies for data and information-sharing, and the cultural barriers which prevent them from harnessing the true power of information. There is a new relevance in the military context to the words of former American president Ronald Reagan, who called information the oxygen of the modern age. Information power underpins effective warfighting in the future battlespace. Achieving connectivity between allied and partner assets, resources, and specialist expertise beyond what can be positioned in a single fixed location is imperative for air forces to remain competitive in future combat. Three decades ago, there may have been two or three dozen individuals, comprising commanders and their staff, involved in operational planning, execution, and C2. Today, video teleconferencing and digital applications make point-to-point collaboration and information sharing possible for hundreds of participants positioned across locations and time zones. Obstacles to interoperability with allies and partners will need to be overcome – and bring better alignment between – national cyber security approaches, and their caveats, which are designed to ensure the digital environment is proactively protected and defended. The inherent vulnerabilities of relying on and operating in cyberspace will give information warfighting a place alongside traditional warfighting responsibilities. Simultaneously, the space domain and advances in quantum encryption will help mitigate the impact of advanced cyberspace threats by revolutionizing military communications.

Interoperability and Coalition Effectiveness

Interoperability is the key measure of coalition effectiveness and will determine combat success in future peer competition environments. Transitioning to an all-domain operational strategy with MDO single-handedly without the contribution of allies and partners is not viable. To become truly interoperable from a coalition perspective, a strategic rethink is necessary for how air forces design and plan future capability. Interoperability is generally improvable through adapting existing systems, but it must become an acquisition-level consideration to be strategically advanced. Significant policy-level obstacles to interoperability exist, such as the over-classification of acquisition programs and the transfer of military equipment, systems, and critical components. Such impediments to coalition effectiveness have recently been apparent in coalition warfighting campaigns, prompting the United States to introduce new approaches, such as the Defense Exportability Features Program (DEFP). DEFP intends to create a paradigm shift in how interoperability is prioritized and pursued. In addition, incorporating interoperability consideration into the concept of operations (CONOPS) of initial capability documentation for major acquisition programs will help ensure it is appropriately planned for in the design phase of future programs and strategically built into the acquisition process rather than being programmed in later as an afterthought.

> ***"Air forces must strengthen the conceptual foundations of interoperability at a coalition level through developing shared CONOPS and tactics, techniques, and procedures (TTPs). How air forces train together, collaborate, and cultivate working relationships is key to unlocking operational advantages in future coalition settings."***

The United States is also placing a stronger emphasis on co-developing systems with allies and partners and targeting earlier exportability routes to help improve overall system design and security while simultaneously compressing program development timelines and reducing costs. As no nation or air force can assume it always has the best technology and concepts, importing capabilities when more superior alternatives are available internationally demands better understanding and attention from acquisition leaders. The indigenous development of military systems offers secondary benefits, such as localizing economic benefits, cultivating high-skilled workforces, and in-country job creation, but also may present trade-offs in value for money or systems that do not match the level of performance offered by importable alternatives.

Interoperability equipment at the systems level is vital; however, ensuring interconnectivity between highly interoperable warfighting platforms alone is insufficient. System-level interoperability does not automatically translate into improved coalition effectiveness. Air forces must strengthen the conceptual foundations of interoperability at a coalition level by co-developing shared CONOPS and tactics, techniques, and procedures (TTPs). How air forces train together, collaborate, and cultivate working relationships is critical to unlocking operational advantages in future coalition settings. It takes time to build trust, and interoperability at the operational level – as opposed to the systems level – is built on years of training and working side by side to understand and advance what can be achieved jointly. Searching for trust in times of crisis or expecting to operate at the level and pace of operations required in high-tempo operations is not viable.

Renewed efforts are necessary for air forces to improve coordination and synchronization with sister services, allies, and partners. The pathway toward a more robust shared sensor network and developing the capability to collect, store, process, analyze, fuse, and share information at the right security level begins with bilateral discussions, advances with joint exercises, and are actualized as lessons learned from continuous efforts and interactions are implemented more broadly into training, education and eventually, active operations. Ultimately, the notion of trust, not technological factors, figures most importantly in amplifying power and delivering integrated deterrence from a coalition perspective. Allies and partners can be a source of highly valuable insights. Air forces must be more open to continuously sharing the threat picture with counterparts and sustaining continuous interaction to support continuous improvement collectively.

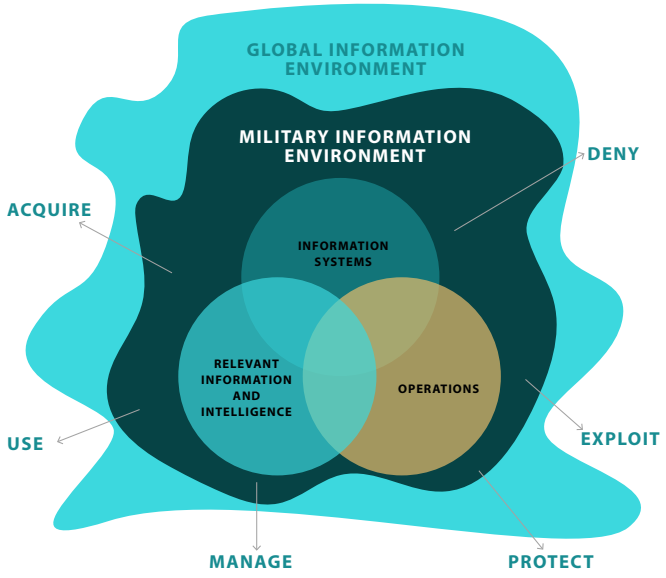
Trust and Information-Sharing

The way information-sharing occurs in an age where information is seen as power but becomes truly powerful only when it is shared is a key measure of effectiveness (MoE)

when gauging trust levels between allies and partners. AI and neural networks will be able to process and analyze tremendous amounts of information that currently takes weeks in real-time. However, how quickly air forces can think and react will hinge on their ability to provide the correct and relevant information at the right classification level to the right person at the right time. Considering the three basic elements of information-sharing (the rationale, in terms of the requirement; the technology and infrastructure, which enable it, and; policies and rules by which it is governed), the rationale is increasingly recognized as legitimate, while the means to enable it are also readily available in most circumstances.

Patriarchally-framed policies and rules relating to information releasability, however, combine with cultural barriers to hinder information-sharing between allies and partners from occurring in a timely and effective manner or frequently, even at all.

The Strategic Environment for IW



"AI and neural networks will be able to process and analyze tremendous amounts of information which currently takes weeks in real-time. However, how quickly air forces can think and react will hinge on their ability to provide correct and relevant information at the right classification level to the right person at the right time."

Archaic information releasability policies and a culture of rigid data ownership combine to restrict the flow of real-time and even historic information to where it is needed. As a result, despite air forces possessing the motivation to work more closely with allies and partners, they tend to remain in lag with the level of information-sharing necessary for more effective warfighting. Obstacles and hindrances to effective information-sharing are attributable to legacy paradigms. However, what worked in the past is not necessarily the most suitable approach for the future. Not all information needs to be shared with everyone at all levels and for all programs, but ensuring the right people have access to the right information is possible through a redesign of information-sharing policies, rules, and classifications that can remove bottlenecks, and hardware and software solutions that lower operational security (OPSEC) risks of industrial-scale information-sharing.

There are valuable lessons to be learned from the successes of the commercial sector in working out solutions to safely improve connectivity and information-sharing at the enterprise level and, crucially, with external partners, resulting in improved productivity and enhanced value for shareholders. Creating new authorities, policies, and information protection procedures is necessary for allowing

information to move safely and seamlessly between the operational domains and across different security classifications in a shared mission partner network. Air forces will need to foster and enforce stronger information and data security alongside establishing a shared data fabric by better aligning technology and processes with joint, allied, and coalition partners. Accessibility to and the security of data networks across the operational domains will be a top priority, where the integrity, trustworthiness, and reliability of information feature as residual concerns.

The Cyberspace Domain and Information Warfighting

Air forces increasingly operate in more complex ways, with the accelerating role for and adoption of digital technologies. With new opportunities, however, also come new risks. The information technology and systems that allow air forces to operate at advanced performance levels also become a type of threat in themselves. Cyberspace is vital for bridging the immense distances across which the modern battlespace is stretched and, as such, will remain a permanent and prominent element of military operations.

Yet the rapid collection, control, and distribution of vast amounts of information give rise to a new type of warfare by generating persistent threats of a pervasive nature that traditional military systems must be better able to fight and defend against. As cyberspace and the electromagnetic spectrum provide the vital terrain for information systems, weapons, and platforms to function today, one of the first considerations for commanders must be to dominate these fluid domains to make them as inhibited and protected as possible against attacks that can introduce area denial issues.

> ***"Militaries broadly need to retrain organizational mindsets and institute standard operating procedures (SOPs) derived from a zero-trust culture so that the information that warfighters are critically reliant on is continuously authenticated and verified across all levels."***

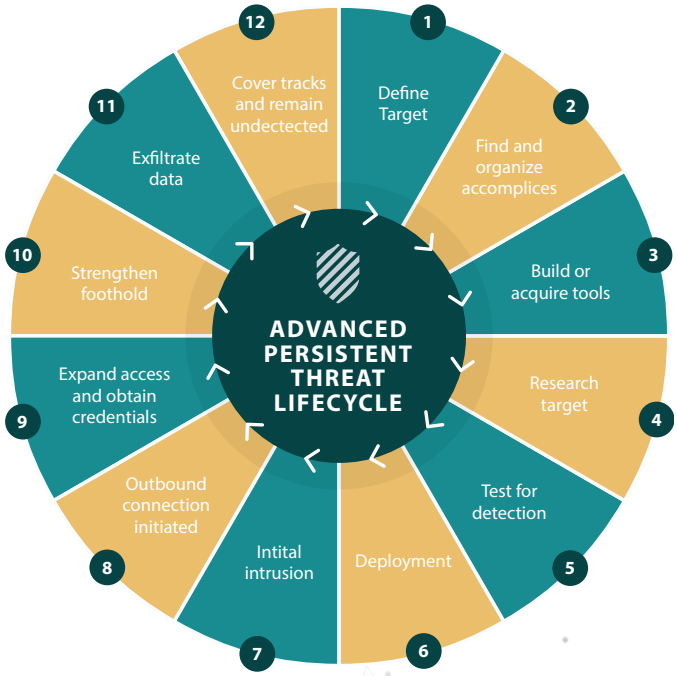
Network protection and defending cyberspace by all means necessary will be imperative for militaries. The nuance is that the future places greater value on data and information resources than the networks which provide the terrain for them. Cryptography modernization will be vital in making possible assured secure communications. However, educating the force on data protection and information security will be a challenge that air forces will need to get right.

Militaries need to retrain organizational mindsets and institute new standard operating procedures (SOPs) derived from a zero-trust culture so that the information that warfighters are critically reliant on is continuously

authenticated and verified across all levels. A primary focus for militaries in cyberspace will remain defending C2 physically and electronically through cybersecurity software and computer network operations.

Information warfighting will inevitably become a core competency alongside traditional warfighting functions. This is despite the lingering uncertainty and complex risks associated with establishing rules of engagement (RoE) in cyberspace. Militaries have observed the 'king of battle' transition from artillery to air power, steadily advancing to become available at any moment and place. Despite serving as the 'go to' capability for fires over the past three decades, it is uncertain whether air power will reign as 'king of battle' over the next three decades or if kinetic capability will go the same way as other legacy capabilities and be replaced by more effective, more precise, and more economical alternatives. Predicting the future is always difficult, yet current trajectories suggest that non-kinetic capabilities will ultimately become 'king of battle,' and fires will transition from hardware to software. Sorties will no longer be needed for effects because computer code and distant clicks will become more destructive than the concussive effects of kinetic weapons.

Advanced Persistent Threat (APT) Lifecycle



Harnessing the Space Domain

With their ability to deliver information down to the lowest levels of command in the fastest and most secure ways, space-enabled datalinks will be essential for force elements to synchronize in highly contested environments. They will allow the observe, orient, decide, and act (OODA) cycle to be radically accelerated and enhance the safety and security of forces before and during operations.

The space domain provides unbeatable reach and persistence for worldwide communications, overhead intelligence, surveillance and reconnaissance (ISR), and the positioning, navigation, and timing (PNT) solutions necessary for maintaining control of airspaces by executing high-tempo operations necessary in the future. Integrating the space domain into MDO will unleash a force

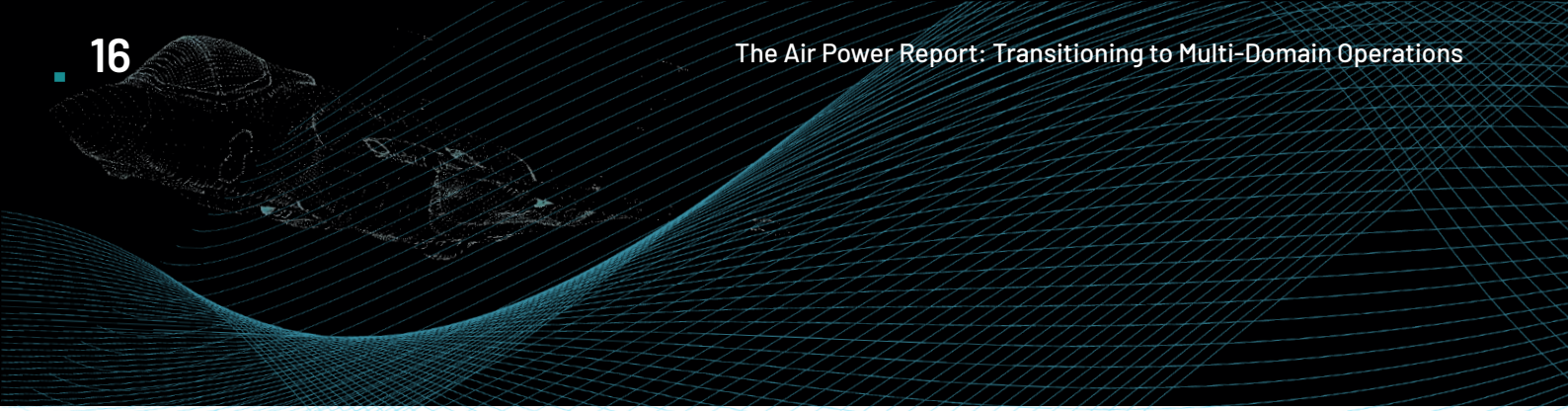
multiplier effect by creating new networks across the operational domains and enabling new mechanisms for distributed joint planning and execution. As traditional ground-based and airborne C2 elements are pushed further away from the fight, the step to the space domain is crucial for spreading connectivity more widely across ground elements and remote carriers, thereby allowing force elements to operate optimally with each other and headquarter elements.

Over the past three decades, satellites have demonstrated an indispensable utility for analyzing communications, localizing target positions, generating accurate coordinates (such as for targeting or aerial drops), and post-strike battle assessment to support planning and execution across the full spectrum of air operations, from warfighting to assurance missions to military operations other than war (MOOTW).

Expanded constellations of geosynchronous satellites will make possible a new form of operational C2 by providing connectivity across all types of manned platforms, RPVs, and autonomous systems, allowing seamlessly integrated operations remotely. As current limiters – namely, computing power, communications bandwidth, and the power generated by solar panels – are overcome, air forces will be presented with revolutionary new prospects via multiple types of new intelligence products and services. In the coming years, it will become possible to harness big data processing, AI, and machine learning (ML) to generate, process, analyze, and filter vast amounts of information onboard satellites and provide automated information services to commanders and warfighters in real-time. Air and space power are woven together, and short of the minimum level of space-based capabilities required, any transition to MDO – which envisions entry across all operational domains but with the space domain arguably at the core – will remain unfulfilled.

Building a Military Space Strategy

The preliminary step to the space domain focuses on developing space situational awareness (SSA), which begins terrestrially with ground-based radar and powerful telescopes before advancing to space-based sensors and enabling capabilities. At the most basic level, SSA must allow air forces to assess launches, monitor the atmospheric re-entry of satellites and launch vehicles, track satellites on orbit, and provide early warning of potential collisions. Building on those preliminary steps, space infrastructure comprising ground stations, space vehicles, and communication links is needed. The delivery of operational effects depends on specialized space staff, operators, and their toolkits, which, considered together, can consume significant financial resources.



Being the service typically tasked with leading the military foray into the space domain, as air forces begin to think about developing a space footprint and operational capabilities, the immediate challenge is to develop programs that can deliver requirements within budgetary constraints and at the speed of relevance.

Air forces need a strategic approach to developing sovereign-controlled space capabilities that will be cost-effective and adequately flexible, allowing for hardware and software updates to be inserted on-the-fly. Commercial off-the-shelf (COTS) technologies offering modular plug-and-play systems and nano-satellites – which have become inexpensive to develop and can be reproduced quickly – lower the barriers to entry in the space domain and will be important in allowing air forces to move with speed or exploit partnerships with a growing number of commercial satellite operators that can provide bandwidth and other critical products for military operations at competitive costs.

However, the physical immenseness of the space domain makes the associated technical complexities and cost burdens of developing space power for any air force or nation entirely by themselves unrealistic. The space domain poses a need for both larger and smaller military actors in space – irrespective of their size – to collaborate and co-develop military space power. The requirement for air forces to coordinate space strategy with allies and partners, whether they have established processes and programs already in place or are at a start-up stage, will be vital for harnessing the true potential that the space domain has to offer military operators.

Intergovernmental, commercial, and research partnerships must form the cornerstones of any military space strategy. Such strategic partnerships will make it possible to benefit from the large body of existing knowledge and apply lessons learned from legacy programs and the experiences of established space actors. In addition, applied experimentation is vital for cultivating knowledge and identifying capability gaps and priorities more rapidly, which, when advanced in collaboration with allies and partners, can streamline the development cycle of space capabilities and provide the foundation to amplify long-term shared benefits.

"Super-sized satellite constellations formed between allies and partners promise to deliver a more diverse and powerful shared capability architecture otherwise not achievable and, crucially, build in redundancy to safeguard against sudden failure or loss of services."

Through strategic coordination, allied and partner air forces with individually stretched resources can limit their focus on creating small satellite constellations with niche capabilities, mechanisms, and orbits, which can be merged into larger or super-sized constellations. Super-sized satellite constellations formed between allies and partners promise to deliver a more diverse and powerful shared capability architecture not achievable otherwise and, crucially, build in redundancy to safeguard against sudden failure or loss of services. Building in redundancy is imperative as the introduction of new space actors and space threats over the coming decade will make the space domain more congested, which presents significant risks in itself, and becomes militarily contested for the first time.

The Dedicated Space Command

By distributing space-based capabilities across a space architecture shared with allies and partners, air forces will benefit from more diverse capability suites, higher availability, and extended reach. As space-based capabilities evolve toward a shared multinational architecture operated collectively by allies and partners, ground stations that control satellites that are currently stove-piped will need to be interconnected and brought closer to AOCs to support C2. As space assets provide products and services that are relevant for both civilian and military users, the use of the space domain complicates operational C2 with the potential need for other government departments to be involved in decision-making that has traditionally rested with military commanders.

"The traditional C2 cycle, processes, and structures were designed to exercise authority over physical units, whereas the space domain, which is focused on the acquisition and transmission of data and communications to deliver effects, requires different considerations."

Military commanders are, therefore, likely to have a reduced or constrained ability to prioritize in specific scenarios or react at the right time in the space domain. To the extent it is possible to insert such frameworks, standing agreements may clarify specific processes that need to be followed if services to other users will be affected by military operations. The traditional C2 cycle, processes, and structures were designed to exercise authority over physical units. In contrast, the space domain, which is focused on the acquisition and transmission of data and communications to deliver effects, requires different considerations. Therefore, a dedicated military space command is necessary for air forces to cater to the vastly increased magnitude of integration and coordination required between space staffs residing across sister services, other government departments, and externally, with allies and partners.

Within this emerging context, air forces are vital in providing solutions to harness space effectively for multi-domain operations. Air forces will be widely tasked with leading, managing, and cultivating the use of space from the defense perspective – this has been recently seen in the United Kingdom, Australia, and the Netherlands, whose air forces have recently established embryonic space commands. Once air forces establish initial operating capability, the structure and processes of C2 in the space domain must be able to evolve as new frameworks are created for generating integrated space domain awareness, defending sovereign, allied, and partner space capabilities, and advancing military space operations, plans, and capabilities holistically. Alongside bringing strategic alignment between sister services, which may not necessarily share a common vision for the use of the space domain or even fully appreciate its potential, a dedicated space command is vital for developing a new cadre of space specialists and the field-grade expertise required for space-enabled multi-domain operations.

Absorbing Emerging Technologies and Harnessing Innovation

For air forces to become capable of thinking, fighting, and winning across the operational domains, almost all legacy systems will need to be upgraded, and air forces will need to improve their ability to absorb mission-capable technologies in the face of rapid technological advances. As a result, air force acquisition planners have a tightrope to walk as the challenges associated with making judgments at key decision points in acquisition cycles intensify. Choosing between pursuing new solutions that offer a revolutionary capability, purchasing less costly commercial off-the-shelf (COTS) solutions to plug capability gaps, or upgrading legacy systems will become more nuanced options to consider. Striking the right balance between fielding the new and upgrading legacy systems will be exacerbated by routine challenges with new systems, which often cannot be fielded quickly enough.

There is an essential role for RPVs and autonomous systems to meet future operational requirements and preserve freedom of maneuver in the multi-domain battlespace. It is widely acknowledged that unmanned and autonomous systems reflect the future of air power; however, air forces tend to think primarily in terms of manned platforms and systems. The traditional focus on manned threats and platforms has led to the development of training and simulation, TTPs, and even C2 processes designed around advancing capability in terms of manned systems against manned threats. Air forces must make their thinking more holistic in terms of manned and remotely piloted and autonomous systems, within which AI has a tremendous role, to ensure they are appropriately accounted for and adequately drive thinking about future threats, capability development, training, live flying, and C2 itself.

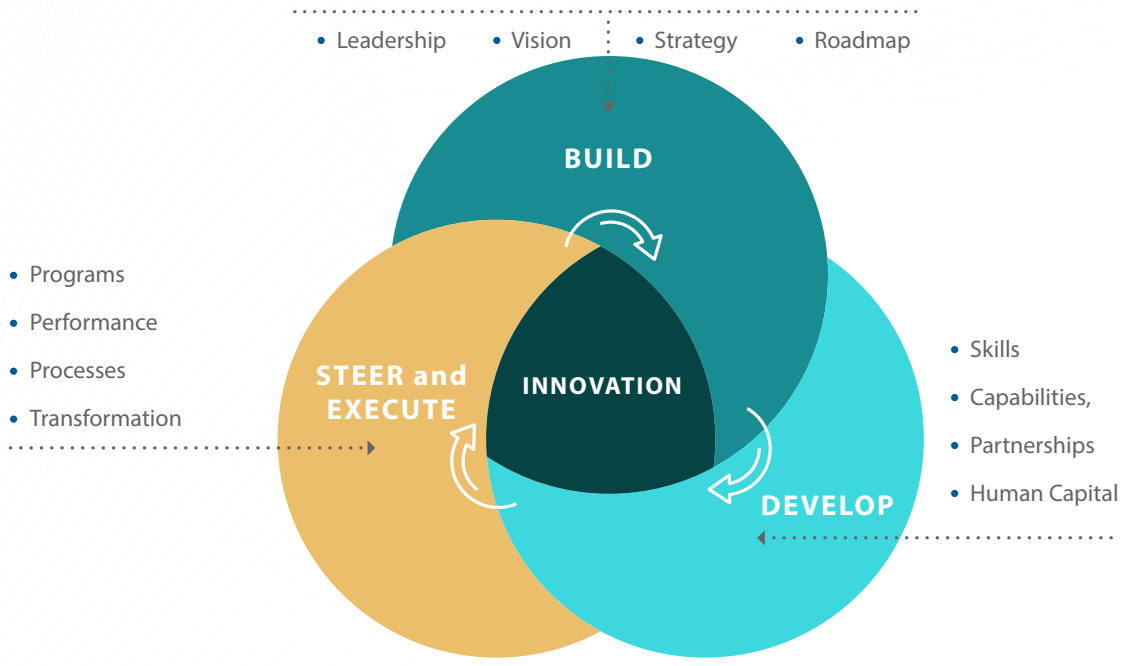
The next generation of airspace and battle management will need big data processing and AI to stretch the human decision space. There is also an underlying need for air forces to lean into rapid software development for providing cloud-based solutions securely accessible through authenticated military credentials. The biggest challenge with AI is the level of control associated with its utilization. For ethical, legal, and security reasons, it is not a viable proposition to not exert any control over AI at all – however, exerting human control beyond a certain degree effectively slows down the decision-making process it is purposed to accelerate. For the time being, AI will need to be geared towards generating and providing options for decision-makers, whether in the cockpit or C2 centers, but its role will grow as the operational cycle accelerates and warfare becomes more automated.

Establishing rapid capability offices may help resolve acquisition challenges by providing faster turnarounds for mission-critical frontline requirements; however, despite the potential for achieving rapidity in acquisition, air forces must ensure they can operate without specific systems by generating out-of-the-box solutions that mix existing technologies with human insight and innovation. The most innovative organizations around the world are

effective at harnessing the power of collective genius, and air forces must become better at fostering a culture of innovation by cultivating the enabling processes, partnerships, and mindsets down to the lowest levels. Ideas have no rank, and personnel at junior levels or non-enlisted officers can be important agents and catalysts for solving operational challenges when air force leaders create the organizational environment where innovation can flourish. By flattening organizations to reduce distances vertically between hierarchies and horizontally between departments, air forces can achieve a more deeply engaged workforce that is better positioned to harvest the benefits of innovation.

To become more technologically adaptive, air forces must develop future systems and digital solutions using common open architectures and become better at connecting operators and end-users with the engineers and the technical teams developing systems and tools, as well as the offices responsible for acquisition and sustainment decision-making. Deeper collaboration achieved through co-developing systems and tools iteratively creates shared ownership with operators and enables revisions to be made on-the-fly. The direct, continuous involvement of users will improve standardization – such as with graphical user interfaces – which supports operator training and can ensure service members are better prepared for success. Partnerships with industry partners and academia will be pivotal for compressing the development cycle of systems from ideation to prototyping, ensuring faster-to-failure pathways, and making air forces more technologically adaptive overall.

PROMOTING A CULTURE OF INNOVATION



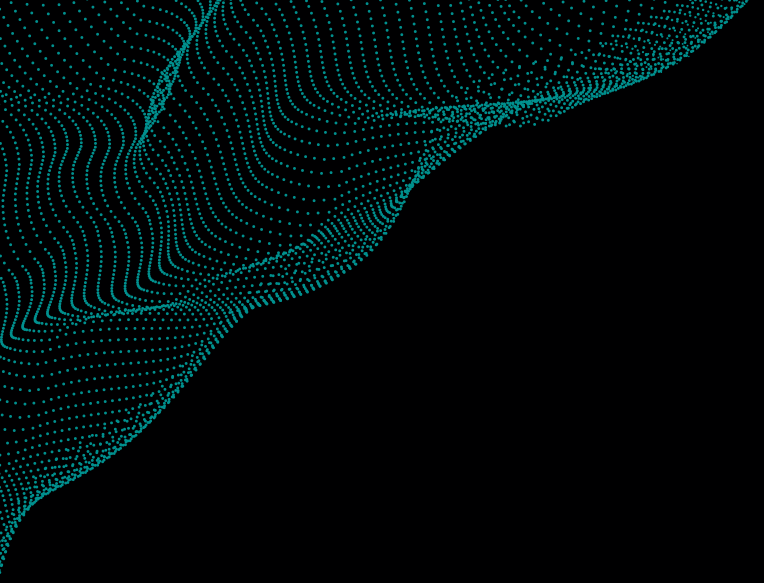
The Way Forward

Air forces must take advantage of the fluid domains, effectively combining the air, space, and cyberspace domains to strategically act (or signal) on the global stage – at range and speed, with enhanced choice, and minimized political risks.

Air power remains the most decisive capability for kinetic effects and airlift today; however, air force leaders must ensure that air power will remain relevant in 2030 and beyond. Air forces are already critically reliant on the ability to operate across the five operational domains – yet these domains are all becoming heavily cluttered and contested. The array of security challenges has grown, and so has the rate of change as potential threats accelerate, driven by the weaponization of disruptive technologies. Air forces will be challenged with finding solutions to potential losses of SA and preserving their ability to continue operating in the constrained and degraded operational spaces of the future. To become more survivable, agile, and resilient, joint responses that are threat-centric will be essential. Air forces must redefine how they cooperate, co-exist, and compete with sister services, allies, and partners. In doing so, air forces will need to become more connected and interoperable within, with sister services, allies, and partners, to succeed at multi-domain integration and deliver coordinated effects across the stretched battlespaces of the future.

"To become more survivable, agile, and resilient, joint responses that are threat-centric will be essential. Air forces must redefine how they cooperate, co-exist, and compete with sister services, allies, and partners."

While it is true that air forces across the world have been largely unable to leverage advantage in a single domain fully, let alone a multi-domain context, there are rich lessons to be learned from past experiences. History is replete with adaptive challenges, and air forces must develop strategies to drive the required transformation necessary to execute MDO. That transition must accelerate beginning with expanded demonstrations to connect sensors, shooters, and force elements across the operational domains. The MDO paradigm broadly demands that platforms and specialist personnel can simultaneously support a wide variety of operational requirements and joint commanders' connectivity. It will be human factors rather than technology factors that prove most decisive for air forces in transitioning to MDO. Approaches to training, developing, and leading personnel must be updated to reflect new battlespace realities and the imperative evolution toward a new way of warfare. Without this, efforts to achieve full network integration and actualizing combat clouds will not yield the results intended.



Think Ahead.

+971 (0)4 589 1276
contact@spps.ae
www.spps.ae