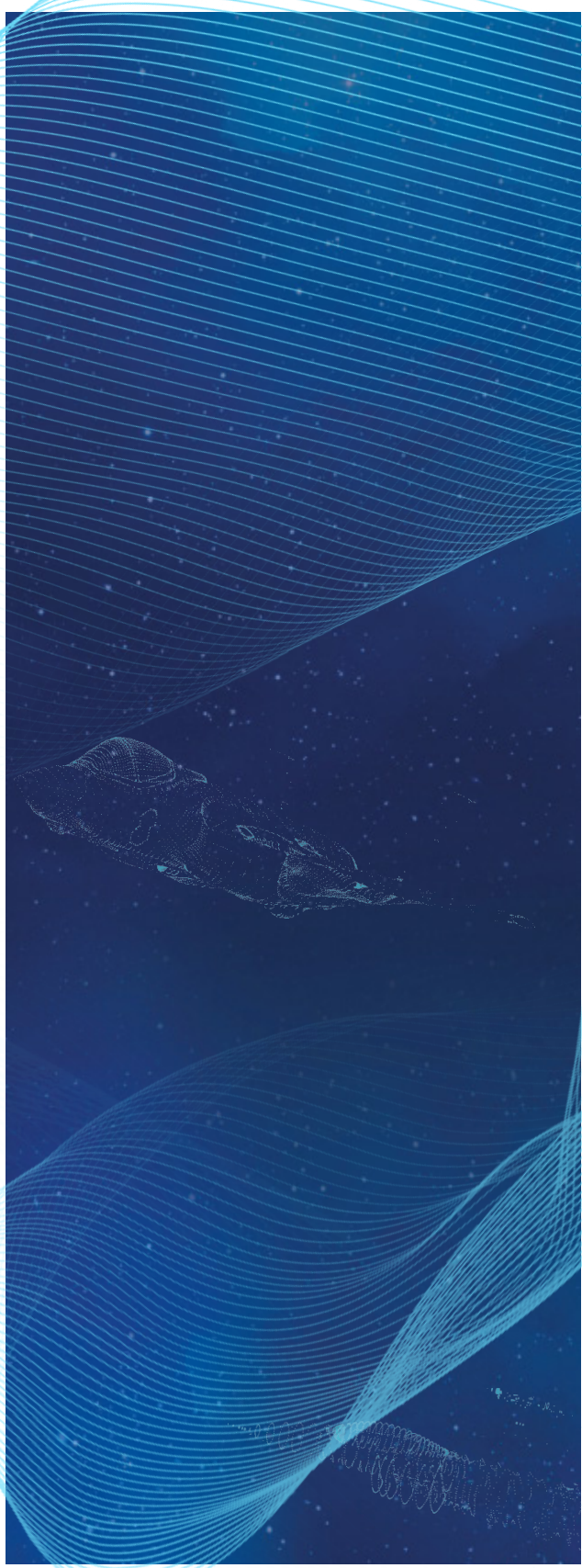
THE AIR POWER REPORT

2022

Transitioning to Multi-Domain Operations



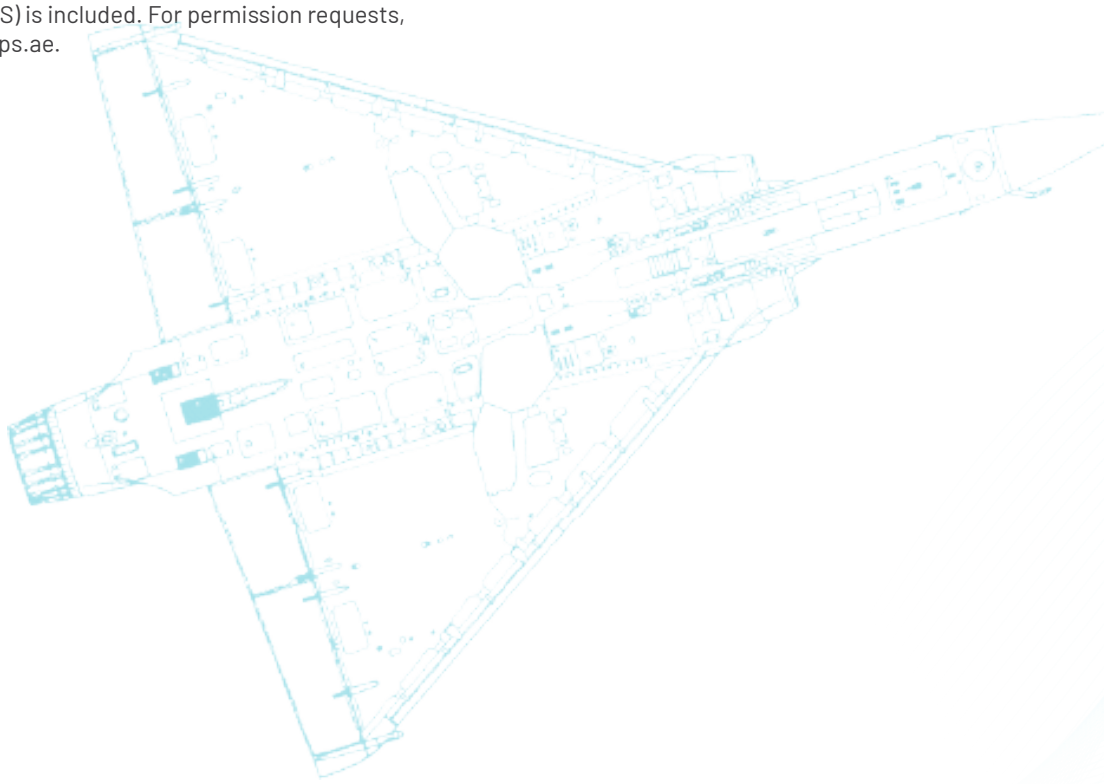
SP PS

Think ahead.

Disclaimer

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should 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 acting, or 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 is stretched across huge distances. Air forces will need to become highly adaptive and able to transition from coordination to synchronization rapidly through an ability to outpace threats in real-time in high-tempo operational environments with an agility not just in moving assets and personnel but also – crucially – information. 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.

Air forces are already critically reliant on the ability to operate across the five operational domains – yet these domains will all become heavily cluttered and contested. Air forces will need to transform the networks, systems and processes they use as well as their ways of working broadly and in fundamental ways to become able to think, fight and win across the length, breadth and height of the modern battlespace. Multi-domain operations (MDO) provide the lead-in for air forces to a new operational command, control and battle management (C2BM) which promises to radically improve joint effectiveness in synchronizing force elements and coordinating effects across a multi-domain battlespace in ways previously not possible.

This report provides a synthesis of the latest emerging perspectives on transitioning to multi-domain operations (MDO) for air forces by interlinking key operational paradigms, challenges and enablers of the strategic transformation necessary to evolve towards a new way of warfare.

Contents

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 to include 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 which may not recognize national borders or subscribe to international norms and practices.

Air forces will therefore operate in a multi-polar world characterized by persistent, sub-threshold engagements where the battlespace is stretched out across huge distances. Being 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 so air forces will need to accelerate change and build the capabilities for a new way of warfare allowing them win across the full spectrum of future conflict scenarios in a highly complex and stretched competition continuum – or risk becoming redundant.

The Operational Environment

Faced 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. As a consequence, 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 an 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 an agility not justin 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 (COACs) 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 therefore defense against them typically 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 right 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 together, rather than on the basis of 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. In doing so, and to enable more robust coordination, command relationships and structures 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 across a 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 transform the networks, systems and processes they use as well as their ways of working broadly and in fundamental ways. To operate at the speed of relevance, commanders across all levels will need access to robust, continuously updated SA delivered through a joint common operational picture (COP) to gain 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."

The same wealth of information that can create operational advantages may also overwhelm decision-making processes if it is not properly filtered and managed, however. 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 the 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 where information can move faster and further than ever but where there is also 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 sensors and shooters are merged into a single, master-grid network.

Legacy C2 doctrines, structures and processes, which can be based on decision-making loops of a 24 hour-cycle, will not suffice against future disruptive threats and the expected pace of operations. No level of technological advancement will make legacy C2 more 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 whereas data analytics and fusion engines exploiting big data processing will produce new opportunities for individual platforms, capabilities, and decision-makers to be integrated into a common digital environment from a joint and even pan-government perspective.

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

A common 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 planning or execution in real-time and at the same rate is those executing missions. Digital toolkits that are highly adaptable to meeting the needs of changing mission requirements will need to become readily available on combat clouds and accessible on-demand using military credentials

to aid better and faster decision-making across all levels. The development of a common digital environment shared between commanders and warfighters will make possible the decentralization of operational C2 and a geographical point-to-point distribution of the traditional functions of AOCs.

The Functional Distribution of AOCs

Distributed AOCs can be understood as being in different places at the same time rather than in one 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 to allow high volumes of communications to be received and high numbers 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 vulnerable to increasingly capable adversaries which can target such nodes through kinetic and non-kinetic means. The same risks exist in scenarios where natural disaster, fire or power outages at any centralized location receiving critical communications and providing operational C2 become a potential single point-of-failure.

A point-to-point distribution of AOCs will deliver 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 will also make it possible for air forces to be connected with more diverse expertise – which are routinely needed at more than one place at any given time – for solving complex operational challenges. Air forces will gain decisive advantages from minimizing the need to work off-cycle in order to get information where and when it is needed and, crucially, build in redundancy to become more operationally resilient. As the functions of AOCs are distributed, air forces will become empowered to adapt quickly to the changing demands of dynamic operational scenarios, including any potential loss of critical nodes in the C2 network, allowing edge warfighters to operate with more security and agility.

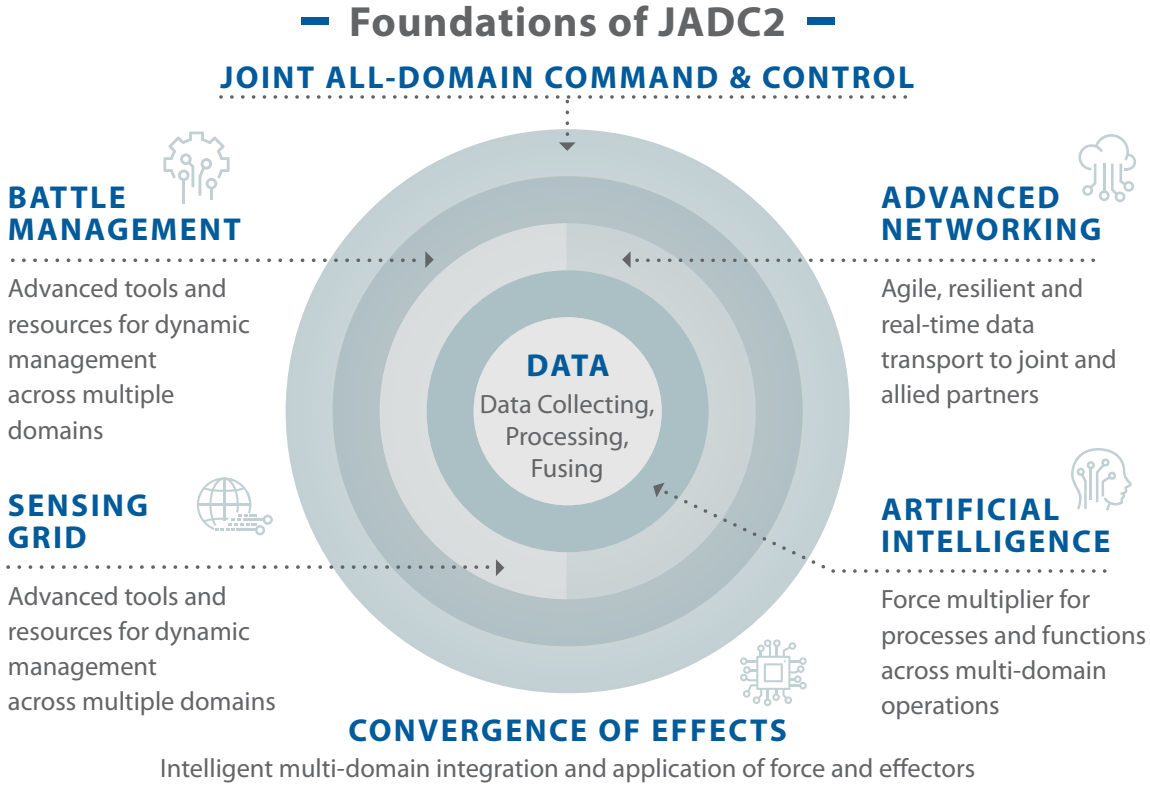
The most significant force multiplier effect promised by distributed AOCs architecture however is to make it possible for air forces to seamlessly tie into partner elements and capabilities positioned at different locations. Virtually bringing together allied and partner AOCs positioned across different locations will allow air forces to aggregate available coalition capabilities in order 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 be stressed for resources or personnel can be mitigated through consolidating coalition capabilities in a way that amplifies power and delivers 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 which slow down the operations cycle – and therefore reaction times – clear delegations to each level of command must be made allowing the prioritization of decision-making to be made at lowest level possible. A single commander connected to an agile, adaptable and assured network that receives data and relays commands should therefore be able to exclusively direct activities of subordinate units. It will remain essential that orders for the delivery of operational capability are properly prioritized however the future challenge will relate to who commands the commanders – particularly in scenarios where there are apparent pressures for multiple arms of government to be included into 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 are properly prioritized however the future challenge will relate to who commands the commanders- particularly in scenarios where there are apparent pressures for multiple arms of government to be included into the C2 decision making process."

Open architecture, system-of-systems (SoS) networks designed for high-speed, high-volume



data exchanges across a wide and dispersed user base will be essential for provisioning relevant information to the right person where and when it is needed. Link 16, which provides a common standard for interconnectivity and interoperability, will remain vital for coalition operations but will not be sufficient in itself even with a modernization program that is designed and implemented holistically among its 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 by itself 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 underpin combat success for the United States across every wargame scenario, provide the basis for the operational C2 of the future to connect the right sensor to the right shooter. The development of a highly scalable, fully-integrated and multi-classification network architecture with clearly defined delegations will be key to achieving the information superiority which allows commanders and warfighters to perform more effectively and efficiently. Current networks and systems need to be modernized and adapted to achieve the 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.

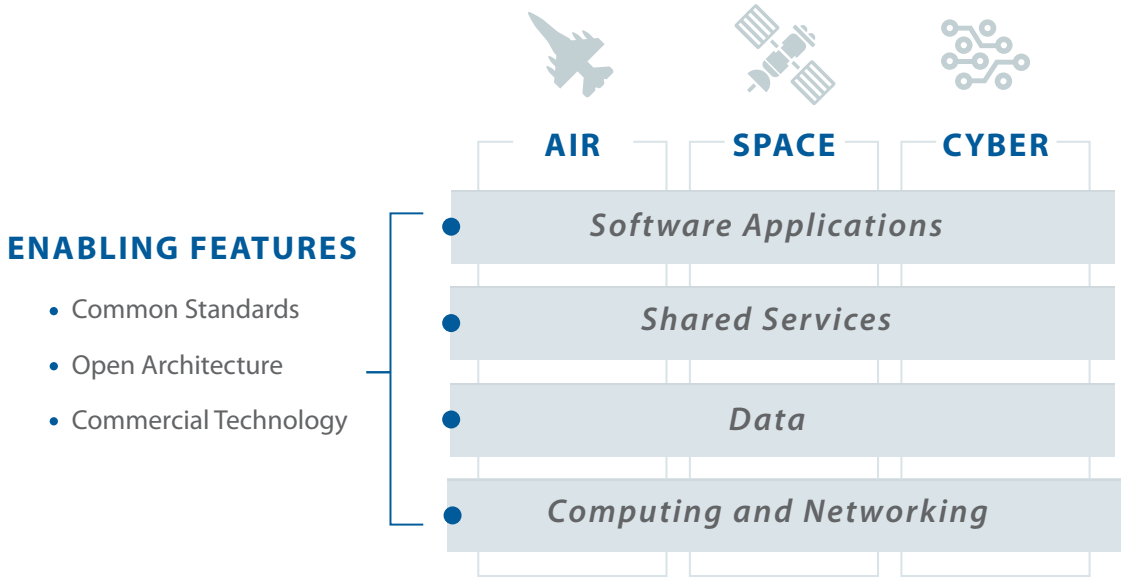
Agile and Collaborative Combat

Interoperability is key to future warfare and the step towards collaborative combat envisions information exchange across all platforms, not just combat fighters. Going beyond legacy fighters being led by new command-capable fighters, as fifth generation platforms are now making possible, interoperability will need to extend across all platforms including remotely piloted vehicles (RPVs) and autonomous systems. Interoperability together 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. Adapting legacy systems into a single grid, multi-domain network is the most crucial impending challenge for air forces and 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 its rapid exploitation while simultaneously preventing adversaries from obtaining the same.

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

Element of Interoperability in Multi-Domain Operations



break-down parochial ways of thinking, archaic policies for data and information-sharing and the cultural barriers which prevent them as organizations 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 when he called information the oxygen of the modern age as information power underpins effective warfighting in the future battlespace.

Interconnecting allied and partner assets, resources and specialist expertise further beyond what can be positioned in a single fixed location will become imperative for air forces to remain competitive in future conflicts. 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 possible point-to-point collaboration and information-sharing for hundreds of staff positioned across a range of locations and time-zones. Obstacles to interoperability with allies and partners will logically need to consider – and bring closer together – national cyber security approaches and their caveats which are designed to ensure the digital environment is protected and defended proactively. The inherent vulnerabilities of relying on and operating in cyberspace will give information warfighting a place alongside traditional warfighting. Simultaneously, the space domain and advances in quantum encryption will begin to mitigate the impact of sophisticated cyberspace threats by revolutionizing the way communications in military operations are conducted.

Interoperability and Coalition Effectiveness

Interoperability is the key measure of coalition effectiveness and will determine combat success in peer competition environments of the future. Transitioning to an all-domain operational strategy with MDO single-handedly without the contributions of allies and partners is not viable yet 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 will need to become an acquisition consideration if it is to be strategically advanced in the way that future conflicts demand in terms of the degree of coalition effectiveness necessary to fight and win.

There are important policy-level obstacles to interoperability which relate to, for example, the over-classification of acquisition programs and transfer of military systems. Such impediments to coalition effectiveness have become apparent in coalition warfighting campaigns in recent years and has prompted the United States, for example, to introduce new approaches such as with the Defense Exportability Features Program

which intends to bring about a paradigm shift in the ways in which interoperability is prioritized and pursued. Incorporating interoperability consideration into the concept of operations (CONOPS) of initial capability documentation for major acquisition programs will ensure that it is appropriately planned for in the design phase of future systems and strategically built into the acquisition process itself 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). The ways air forces train together, collaborate and cultivate working relationships hold the key to unlocking future operational advantages."

The United States will also place a stronger emphasis on co-developing systems with allies and partners and target the earlier exportability of systems, which can help improve overall system design and security on the one hand while compressing development timelines and reducing costs on the other. No air force can assume it always has the best technology solutions and concepts so importing capabilities when more superior alternatives are available in the international market will need higher prioritization. The indigenous development of military systems offers secondary advantages such as localizing economic benefits and cultivating high-skilled workforces through in-country job creation but come with trade-offs such as lower value for money or systems that do not match the same level of performance offered by alternatives.

Interoperability between equipment at the systems level is vital however warfighting platforms themselves and ensuring their interconnectivity alone are not sufficient for interoperability and do not automatically translate into improved coalition effectiveness. Air forces must strengthen the conceptual foundations of interoperability at a coalition level through developing shared CONOPS and tactics, techniques and procedures (TTPs). The ways air forces train together, collaborate and cultivate working relationships hold the key to unlocking future operational advantages. 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. It is not possible to search for trust in times of crisis or expect to be able to operate at the level and pace of operations required in the future.

Renewed efforts are necessary for air forces to improve synchronization and coordination with sister services as well as allied and partner air forces. The pathway towards a more robust sensor network and developing the capability to collect, store, process, analyze, fuse and share information at the right security level begin with bilateral discussions, advance with joint exercises and are actualized as lessons learned from continuous efforts and interactions are implemented broadly into training, education and eventually active operations themselves. Ultimately, it is the notion of trust that will figure more importantly than technological factors in amplifying power and attempts to realize integrated deterrence between coalition partners. Allies and partners can be a source of highly valuable insights and air forces must become more open to continuously sharing the threat picture with counterparts and sustaining the continuous interaction of ideas to support continuous improvement.

Trust and Information-Sharing

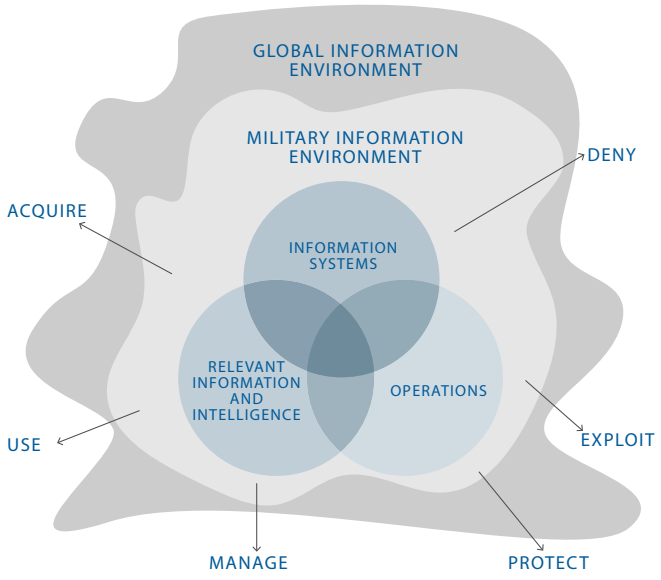
The way information-sharing occurs in an age where information is seen as power but where it becomes truly powerful only when it is shared is a key measure of effectiveness (MoE) when it comes to assessing trust between allies and partners. AI and neural networks will be able to process and analyze in real-time tremendous amounts of information which currently takes weeks yet how quickly air forces can think and react will hinge on their ability to provision 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, which it is governed by), the rationale is increasingly is recognized as legitimate and the means to enable it are also readily available in most instances. Patriarchally-framed policies and rules on 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.

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

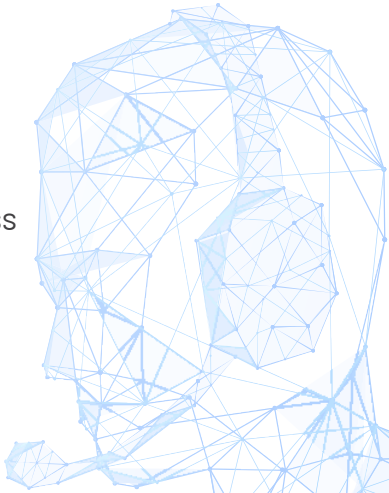
Archaic information releasability policies and a culture of rigid data ownership combine to restrict the flow of real-time and even historic information to where it is needed. Despite air forces possessing the motivation to work together more closely with allies and partners therefore they collectively 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 does not necessarily work in 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, on the one hand, a redesign of applicable information-sharing policies, rules and classifications to remove bottlenecks, and hardware and software solutions that lower operational security (OPSEC) risks of industrial-scale information-sharing on the other.

There are valuable lessons to be learned from the successes of the commercial sector in working out ways to safely improve connectivity and information-sharing at the enterprise level and, crucially, with external partners, resulting in improved productivity and higher value for

The Strategic Environment for IW



shareholders. The creation of 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 common data fabric by better aligning technology and processes with joint and allied or coalition partners. Accessibility to and the security of information and data networks across the operational domains will become a top priority, with the integrity, trustworthiness and reliability of information featuring as residual concerns.



The Cyberspace Domain and Information Warfighting

The ways air forces operate are becoming more complex with the accelerating role and adoption of digital technologies and innovation. With opportunities however also come risks as the information technology and systems that support air forces become a type of threat in themselves. Cyberspace is vital for bridging the immense distances across which the modern battlespace has been stretched and will thus remain a permanent and increasingly prominent element of military operations. Yet the rapid collection, control and distribution of vast amounts of information gives rise to a new type of warfare by generating persistent threats of a pervasive nature which traditional military systems must become able to fight and defend against. Cyberspace and the electromagnetic spectrum provide the vital terrain for information systems, weapons and platforms to function and one of the first considerations for commanders is the need to dominate the fluid operational domains to make them as inhibited and protected as possible against attacks which can introduce area denial issues.

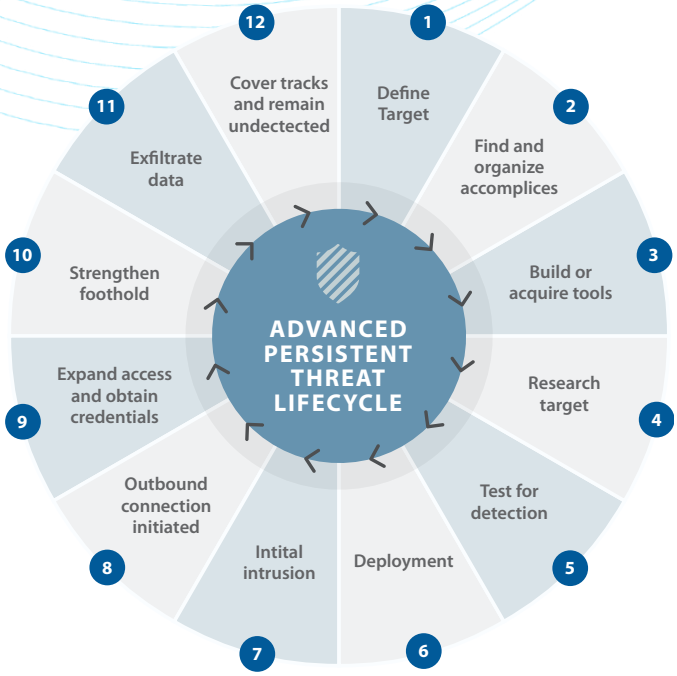
"Militaries broadly need to retrain organizational mindsets and institute standard operating procedures (SOPs) derived from a zero trust culture so that the information that warfighters are critically reliant on is continuously authenticated and verified across all levels."

Network protection and defending cyberspace by all means necessary will be imperative for militaries yet the future places the greater value of importance upon the data and information resources themselves rather than the networks which provide the terrain for them. Cryptography modernization will be vital for making possible assured and secure communications however educating the force on data protection and information security is a challenge that air forces will need to get right. 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. More broadly, the primary focus for militaries in cyberspace will remain

defending C2 physically and electronically through cybersecurity software and computer network operations.

Despite lingering challenges with establishing rules of engagement (RoE) in cyberspace nevertheless information warfighting will inevitably become a core competency alongside traditional warfighting in the years ahead. Militaries have observed the king of battle transition from artillery to air power, which steadily advanced to become available at any moment and any 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 as 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, data links enabled by satellites will be essential for synchronizing force elements in highly contested environments, in accelerating the observe, orient, decide and act (OODA) loop and for enhancing 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 and executing the high-tempo operations forecasted for the future. The integration of

the space domain into MDO will unleash a force multiplier effect by allowing for the creation of new networks across the operational domains and new mechanisms for distributed joint planning and execution to occur. As traditional ground-based and airborne command 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 more 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, for example) 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 geo-synchronous satellites will make possible a new form of operational C2 by providing connectivity across all types of manned platforms, RPVs and autonomous systems thereby allowing them to operate together 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 on-board satellites themselves and autonomously provide critical information services to commanders and warfighters in real-time. Air and space power come 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 into 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 other 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 in orbit and provide early warning of potential collisions. From that preliminary step, space infrastructure comprising ground stations, space vehicles and communication links are needed whereas the delivery of operational effect is dependent on specialized space staffs, operators and their toolkits, which, considered together, have the potential to 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 approaches for developing sovereign-controlled space capabilities that are cost effective and also flexible, such as for inserting hardware and software updates. Commercial off-the-shelf (COTS) technologies offering plug-and-play solutions and nano-satellites – which have become relatively inexpensive to develop and can be reproduced quickly at low cost – lower barriers to entry into the space domain and will be important in allowing air forces to move with the speed necessary, coma together with a growing number of commercial satellite operators which can competitively provide bandwidth and other critical products for military operations.

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

Intergovernmental, commercial and research partnerships will need to form a cornerstone of military space strategy so it is possible to benefit from the large body of existing knowledge and apply lessons learned from the experiences of established space actors and legacy programs. Applied experimentation will be important for air forces in cultivating specialist knowledge and in being able to identify capability gaps and priorities more rapidly which, when advanced in collaboration with allies and partners, can significantly streamline the development cycle of space capabilities and provide a basis 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 will be able to limit their focus to creating small constellations of satellites with niche capabilities, mechanisms and orbits to later be brought together and 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 otherwise not achievable 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 make the space domain not only more congested, which presents significant new risks in itself, but also militarily contested for the first time.

The Dedicated Space Command

By distributing space-based capabilities across a wider space architecture shared with allies and partners, air forces will be able to gain from more diverse suites of capabilities, higher availability and extended reach for worldwide secure communications. As space-based capabilities evolve towards an architecture shared between allies and partners, ground stations which control satellites that are currently stove-piped will need to be interconnected and brought closer to AOCs for improved decision-making in C2. As space assets provide products and services for both civilian and military users however 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 likely to have a reduced or constrained ability to prioritize in specific scenarios or react at the right time in the space domain. To a degree, standing agreements which, inserted where possible, may clarify specific processes that need to be followed if services to another user are to be affected by military operations. 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. A dedicated military space command is therefore a necessity for catering 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.

Air forces have a vital role to play in providing solutions to harness space effectively for multi-domain operations and will typically be tasked with leading, managing and nurturing space from the defense perspective – such as in the United Kingdom, Australia and the Netherlands, for example, 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 will evolve as new frameworks are created for generating integrated space domain awareness, for defending sovereign, allied and partner space capabilities and for advancing military space operations, plans and capabilities holistically. Alongside bringing strategic alignment between sister services, which may not share a common vision for the use of the space domain or even fully appreciate its potential, a dedicated space command will also be vital for cultivating a new cadre of specialist space staffs and expertise required for multi-domain operations by air forces.

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. Air force acquisition planners have a tightrope to walk as the challenges associated with making judgements at key decision points in acquisition cycles intensify. Making choices between pursuing new solutions which offer a revolutionary capability, purchasing less costly commercial off-the-shelf technologies (COTS) to plug capability gaps or attempting to upgrade legacy systems will become more nuanced. Striking the right balance between fielding the new and upgrading legacy systems will be exacerbated by the challenge of new systems that often cannot be fielded quickly enough.

To meet future operational requirements and preserve freedom of maneuver, there is an essential role for RPVs and autonomous systems in the multi-domain battlespace. It is widely acknowledged that unmanned and autonomous systems reflect the future air power however air forces retain a tendency 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, in order to ensure they are appropriately accounted for and properly drive thinking about future threats, capability development, training, live flying and C2 itself.

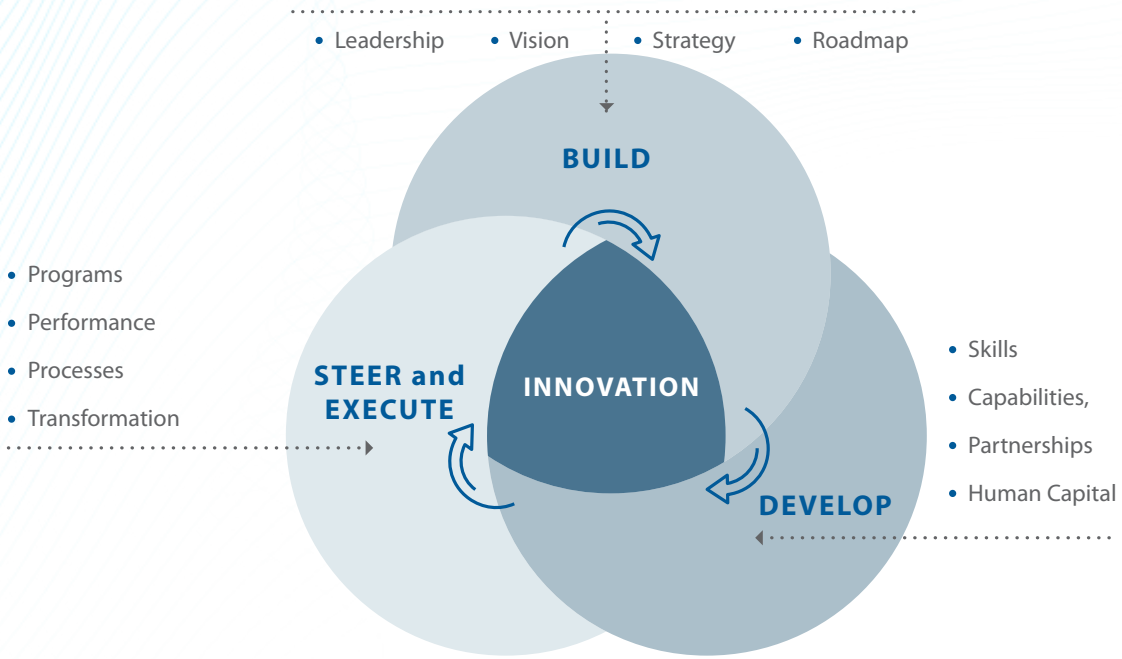
The next generation of airspace and battle management will need big data processing and AI to stretch the human decision space and there is also an underlying need for air forces to be able to lean into rapid software development for providing cloud-based service solutions which are securely accessible 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 in 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 are able operate without specific systems through 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 through 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 environments in which 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



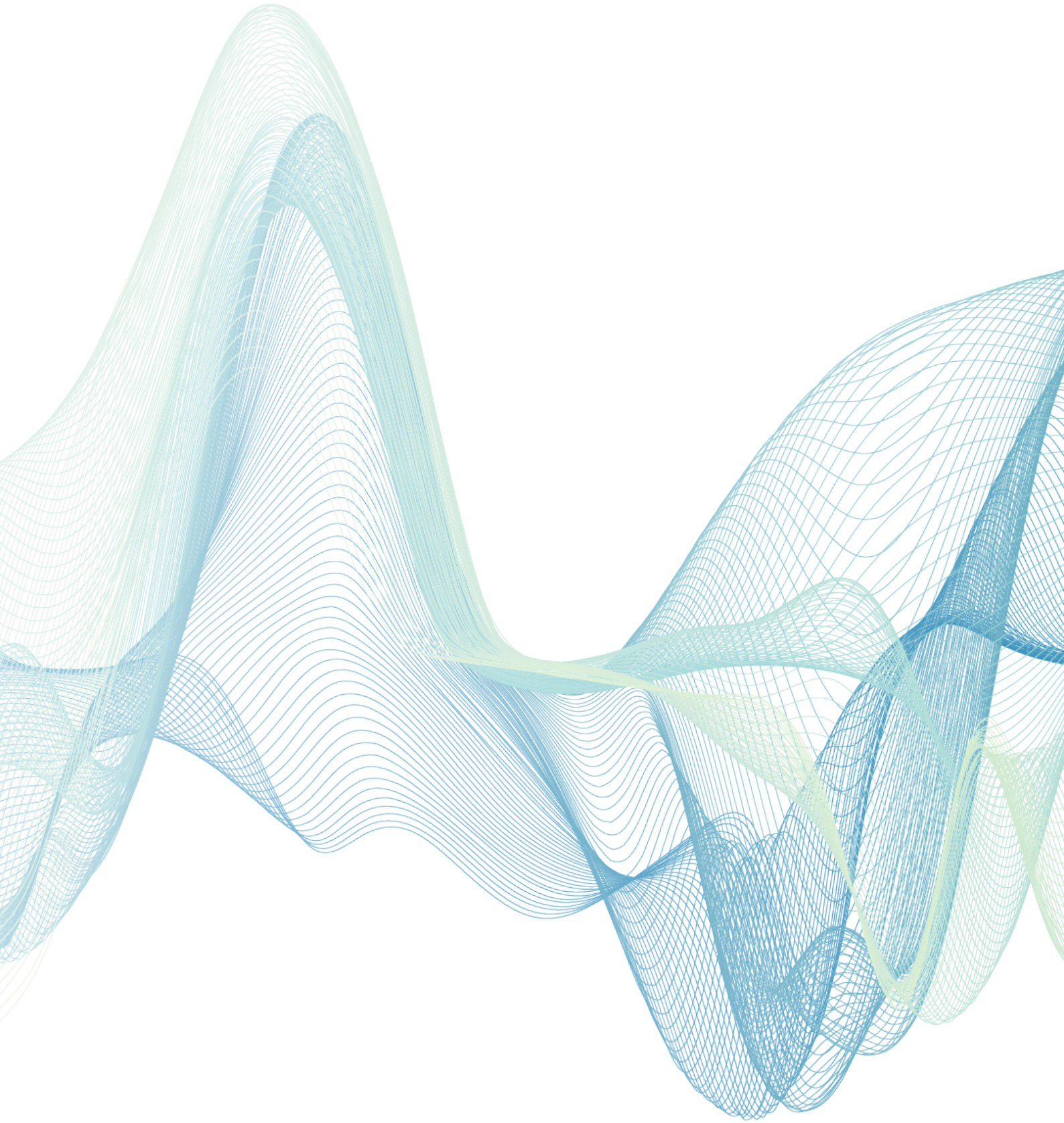
The Way Forward

Air forces need to become able to take advantage of the fluid domains, effectively combining air, space and cyberspace 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 can 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 will all become 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 for 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 and air forces must redefine how they co-operate, co-exist and compete with sister services, allies and partners. Air forces will need to become more interconnected and interoperable within, with sister services and allies and partners to succeed at multi-domain integration and for delivering 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 and air forces must redefine how they co operate, co exist and compete with sister services, allies and partners."

While it is true that air forces across the world have been unable to fully leverage advantage in a single domain let alone a multi-domain context, there are rich lessons to be learned from past experiences. History is replete with disruptive challenges and air forces must develop strategies to drive the required transformational changes 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 simultaneously support a wide variety of operational requirements and joint commanders' connectivity. It will therefore be human factors that will prove more decisive than technology in transitioning to MDO and approaches to training, developing and leading personnel must be updated to reflect the new realities and way of warfare if full network integration and the actualization of combat clouds into military operations is to be realized.



Think ahead.

THE AIR POWER REPORT