RESTORING AMERICA'S MILITARY COMPETITIVENESS:

Mosaic Warfare

By Lt Gen David Deptula, USAF (Ret.)
and Heather Penney

with Maj Gen Lawrence Stutzriem, USAF (Ret.)
and Mark Gunzinger

MITCHELL INSTITUTE for Aerospace Studies

Note to readers: this electronic edition features an interactive table of contents and endnotes. Click on the page number in the table of contents to be taken to the respective chapter; endnotes in the text are linked to their respective citation at the end of this study. Click on the citation number to go back.

RESTORING AMERICA'S MILITARY COMPETITIVENESS:

Mosaic Warfare

By Lt Gen David A. Deptula, USAF (Ret.)
and Heather R. Penney
with
Maj Gen Lawrence A. Stutzriem, USAF (Ret.)
and Mark A. Gunzinger

The Mitchell Institute for Aerospace Studies
Air Force Association
Arlington, VA
September 2019

About the Mitchell Institute for Aerospace Studies

The Mitchell Institute for Aerospace Studies is an independent, nonpartisan policy research institute established to promote understanding of the national security advantages of exploiting the domains of air, space, and cyberspace. The Mitchell Institute's goals are: 1) to educate the public about the advantages of aerospace power in achieving America's global interests; 2) to inform key decision makers about the policy options created by exploiting the domains of air, space, and cyberspace, and the importance of necessary investment to keep America the world's premier aerospace nation; and 3) to cultivate future policy leaders who understand the advantages of operating in air, space, and cyberspace. Mitchell Institute maintains a policy not to advocate for specific proprietary systems or specific companies in its research and study efforts.

Disclaimer:
Mitchell Institute for Aerospace Studies would like to recognize that this publication is based upon work supported by the Defense Advanced Research Projects Agency (DARPA). Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of DARPA.

About the Authors

Lt Gen David A. Deptula, USAF (Ret.), is dean of the Mitchell Institute for Aerospace Studies. Deptula has planned, flown in, and commanded air operations ranging from humanitarian relief efforts, to contingencies, to major theater war. He served as the principal air attack planner for Operation Desert Storm in 1991, was a joint task force commander in Iraq overseeing Operation Northern Watch, and led the initial air campaign of Operation Enduring Freedom as director of the Combined Air Operations Center. Deptula served 34 years on active duty, including his last assignment as the Air Force's first deputy chief of staff for intelligence, surveillance, and reconnaissance (ISR). He is a prolific author and commentator on modern military strategy and operations, defense, and aerospace power.

Heather R. Penney is a senior resident fellow at the Mitchell Institute, where she conducts research and analysis on defense policy with a focus on the critical advantage of aerospace power. Prior to joining Mitchell Institute, Penney worked in the aerospace and defense industry, where she led budget analysis activities, program execution, and campaign management. An Air Force veteran and pilot, Penney served in the Washington, DC, Air National Guard, flying F-16s and G-100s, and has also served in the Air Force Reserve in the National Military Command Center.

Maj Gen Lawrence A. Stutzriem, USAF (Ret.), is the Mitchell Institute's research director. He served as a fighter pilot, flying the F-4, F-16, and A-10. He directed air operations for Operation Southern Watch. Following 9/11, he led diverse teams spearheading complex air operations while innovating new operational concepts during Operation Enduring Freedom. He served as professor of military strategy and operations at the National War College, and later as the senior military representative at the U.S. Department of State. He oversaw strategy, plans, and policy for North American Aerospace Defense Command and U.S. Northern Command.

Col Mark A. Gunzinger, USAF (Ret.), is director of future aerospace concepts and capabilities assessments at the Mitchell Institute. He served on the National Security Council staff in The White House, and as deputy assistant secretary of defense in the Office of the Undersecretary of Defense for Policy. He led research for the Secretary of the Air Force and Air Force Chief of Staff on future concepts for air warfare, and he co-authored the Defense Department's first transformation strategy to sustain the U.S. ability to project power into contested areas. His recent studies include directed energy capabilities, concepts, and technologies to preserve U.S. military dominance across the electromagnetic spectrum.

Cover design by Zaur Eylanbekov;
photos: Northrop Grumman, U.S. Air Force, DOD, Jared Brashier, FoxbatGraphics.

Contents

Foreword

The fall of the Soviet Union and post-9/11 conflicts have transformed the U.S. military away from one that was optimized for high-end peer conflict to one designed to address limited regional hostilities. While the United States focused on counterinsurgency operations, nations like China, Russia, Iran, and North Korea aggressively advanced their military capabilities. The resultant increase in threats capable of challenging the United States demands a robust, strategic approach from the Department of Defense.

However, the U.S. military finds itself poorly aligned to meet these new challenges from an ends-ways-means perspective. Taking the Air Force as an example, the service has endured nearly 30 years of resource cuts that have reduced key force structure elements by more than half. Air Force force structure is the smallest and the oldest in the service's history. High operational tempo has worn both equipment and people. The bottom-line effect is that the nation is now ill-prepared to face the challenges posed by sophisticated nation-state threats.

Over the past few decades, global competitors studied how the U.S. military fights as a system, and they have responded smartly. Their strategy, operational concepts, and associated weapons are aligned to counter American military strengths. For the first time since the Cold War, the nation finds itself having to re-think its approach to warfare. The U.S. defense enterprise must unify around a future of U.S. warfighting strategy and a commensurate new force design. The approach cannot simply be a better status quo.

This study explores how the mosaic warfare formulation put forth by DARPA, the Defense Advanced Research Projects Agency, is designed to meet these aims. It is a future force design that leverages the dynamic relationship between force structure and operational concepts to gain offensive initiative against any enemy while being highly adaptable across the spectrum of military operations. The objective of the mosaic force design is to exploit information networks to create a highly disaggregated kill web that minimizes targetable U.S. nodes while ensuring that the U.S. military enterprise remains effective in contested environments.

The United States faces a crucial decision point. Without change, the public warnings of many in the defense community—that the nation risks losing its next conflict—may come true.

Lt Gen David A. Deptula, USAF (Ret.)
Dean, The Mitchell Institute for Aerospace Studies
September 2019

Abbreviations

A2/AD	Anti-Access/Area Denial
ACK	Adapting Cross-Domain Kill-Webs
AI/ML	Artificial Intelligence/Machine Learning
C2	Command and Control
CAOC	Combined Air Operations Center
CMCC	Common Mission Control Center
CRC	Control and Reporting Center
CNAS	Center for a New American Security
DARPA	Defense Advanced Research Projects Agency
DBM	Distributed Battle Management
DCGS	Distributed Common Ground System
DOD	Department of Defense
DyNAMO	Dynamic Network Adaptation for Mission Optimization
EW	Electronic Warfare
HVAA	High-Value Airborne Asset
ISR	Intelligence, Surveillance, and Reconnaissance
JCIDS	Joint Capabilities Integration and Development System
NDS	National Defense Strategy
OODA	Observe–Orient–Decide–Act
OTA	Other Transaction Authority
OT&E	Operational Test & Evaluation
PLA	People's Liberation Army
RSPACE	Resilient Synchronized Planning and Assessment for the Contested Environment
SAM	Surface-to-Air Missile
SLEP	Service Life Extension Program
SoSITE	System of Systems Integration Technology and Experimentation
STO	Strategic Technology Office
TACS	Theater Air Control System
TPFDD	Time-Phased Force Deployment Data
UTC	Unit Type Code

Executive Summary

The November 2018 report by the Commission on the National Defense Strategy for the United States issued a chilling forecast for the nation: "American forces will face harder fights and greater losses than at any time in decades … Americans could face a decisive military defeat … Put bluntly, the U.S. military could lose the next state-versus-state war it fights."[1] Consensus has grown since the release of the *2018 National Defense Strategy* that the United States must change its preferred way of war and how its military is designed to prevail in future peer-on-peer contests. The U.S. Department of Defense (DOD) must now focus on the greatest threats to the security interests of America and its allies: Chinese and Russian revisionist ambitions.[2] These great powers are using warfighting strategies that employ anti-access/area-denial (A2/AD) capabilities to prevent the United States and its allies from intervening against their acts of aggression.[3]

In particular, the United States must address the burgeoning threat that China poses and the way in which it has carefully designed its systems warfare strategy to counter America's traditional way of war.[4] While A2/AD threats are often treated as operational challenges, China intends to employ them to achieve strategic-level effects that render the most critical elements of U.S. operations ineffective.[5] By targeting U.S. data links, disrupting information flows, denying command and control, and kinetically targeting physical nodes of the U.S. information system, China is planning systematically to blind U.S. commanders and paralyze their operations.[6]

America's current way of war is incompatible with this kind of systems warfare. This is why a future U.S. force design must be mapped to how enemies intend to fight, and the resulting potential gaps in the current U.S. force. These include:

- Small inventories of quite capable, high-end multifunction platforms in the current force make U.S. operational architectures too vulnerable.
- The practice of buying multiple kinds of high-end weapon systems in limited numbers is inefficient and does not provide the force capacity needed for great power conflict.
- It takes too long to develop and field major new weapon systems.
- America's current force design cannot appropriately scale across the spectrum of conflict.
- Critical elements of current U.S. force design cannot withstand attrition, and survivability factors threaten to outweigh the ability to create effects in the modern, complex wartime environment.

"Mosaic" is a force design concept for a systems warfare strategy. The concept is designed to address the demands of the future strategic environment and the shortcomings of the current force. Mosaic warfare

exploits both the ability of advanced networks to seamlessly share information across an area of operations and recent developments in processing, computing, and networking. Functional capabilities, such as radar, fire control, and missiles, that once had to be hosted on a common platform, like a sophisticated combat aircraft, can now be disaggregated into their smallest practical elements. In the mosaic concept, platforms are "decomposed" into their smallest practical functions, creating collaborative "nodes" in a networked kill web that is highly resilient and can remain operationally effective, even as an adversary attrits some of the web's elements.

Mosaic uses highly resilient networks of redundant nodes and multiple kill paths to minimize the critical system value of U.S. nodes that an enemy could target. This ensures U.S. forces are effective in contested environments. At the same time, disaggregated functionality would allow a mosaic force to be highly adaptable across the spectrum of military operations. Mosaic combines the attributes of highly capable, high-end systems with the volume and agility afforded by numerous smaller force elements that can be rearranged into many different configurations or presentations. When composed together, these smaller elements complete operational observe–orient–decide–act cycles ("OODA loops") and kill chains. Like LEGO® blocks that nearly universally fit together, mosaic forces can be composed together in a way to create packages that can effectively target an adversary's system with just-enough overmatch to succeed.[7]

The guiding principles and technologies that underpin a mosaic force design will help enable the United States to prevail in long-term competitions with great power adversaries.

The mosaic force design concept is more than just an information architecture. Mosaic offers a comprehensive model for systems warfare that encompasses requirements and acquisition processes; the creation of operational concepts, tactics, techniques, and procedures; and force presentations and force-allocation action, in addition to combat operations. Mosaic is not simply about quickly closing kill chains. The attributes of a mosaic force design can help increase the speed of action across the U.S. warfighting enterprise, whether it involves quickly responding to urgent new requirements, integrating innovative and out-of-cycle capabilities, or operational planning. The guiding principles and technologies that underpin a mosaic force design will help enable the United States to prevail in long-term competitions with great power adversaries.

Implementing a mosaic force design will challenge issues of doctrine, tradition, parochialism, bureaucratic fiefdoms, and even the pride of victories past. Nonetheless, the American way of war must adapt if it is to support the priorities of the *2018 National Defense Strategy*. To migrate to a mosaic force design, the following areas of development are prerequisites that will require investment and smart oversight:

- Develop automated technology that can share information across different security levels;
- Develop appropriate policy for test, validation, and verification of artificial intelligence;
- Develop multiple and complimentary approaches to spoof-proofing artificial intelligence;

- Maintain commitment to current force structure and programs of record;
- Conduct an operationally focused cost assessment of force design alternatives;
- Aggressively invest in developing and fielding mosaic enablers; and
- Experiment with mosaic operational concepts, architectures, and empowered command and control at the edge.

There are many trends that already indicate the value and potential of mosaic operations. Early examples of systems, technologies, software, and architectures that are mosaic in nature are already being developed or fielded. Indeed, the U.S. Defense Advanced Research Projects Agency (DARPA) and the services have been investing in maturing many of the mosaic enablers that they have already identified. Mosaic-type operations are not new to the U.S. Air Force, and the service is perhaps the best candidate to take the lead role in developing a mosaic force design concept that could reshape DOD's planning, processes, force structure, and how it executes its missions.

Since a nation's military backstops the political grand strategy of any great power, the United States must out-adapt adversaries who have, and will continue to adapt to, an obsolescing U.S. force design. That said, the United States can migrate to a more effective force design even as new elements are introduced to make it more effective in character and operational concept. What cannot migrate is resistance to a new way of war—a mosaic force design—within defense culture largely conditioned by an atypical era of absolute military dominance, permissive threat environments, and a lack of peer adversaries. Swift decisions are needed at the apex to align thinking and resources to the enablers of mosaic warfare.

Introduction

The November 2018 report by the Commission on the National Defense Strategy for the United States issued a chilling forecast for the nation: "American forces will face harder fights and greater losses than at any time in decades … Americans could face a decisive military defeat … Put bluntly, the U.S. military could lose the next state-versus-state war it fights."[8]

This was not a one-off warning. The concern regarding America's potential eroding military dominance permeates the *2018 National Defense Strategy* (*2018 NDS*), which calls for a strategic shift toward addressing great power competition.[9] A Center for New American Security study cautions: "For the first time in decades, it is possible to imagine the United States fighting—and possibly losing—a large-scale war with a great power."[10] Developing a future force that is better prepared to defeat great power aggression will require "increased and sustained investment … because of the magnitude of the threats they pose" and "the potential for those threats to increase."[11]

DOD should balance its investments in new, traditional weapon systems—incredibly powerful, multifunction platforms that are intricate compilations of capabilities—with forces that are more modular, scalable, adaptive, and unpredictable.

Consensus has grown since the new defense strategy's release that the United States must change its preferred way of war and how its military is designed to prevail in future peer-on-peer contests. The U.S. Department of Defense (DOD) must now focus on the greatest threats to the security interests of America and its allies: Chinese and Russian revisionist ambitions.[12] These great powers are using warfighting strategies that employ anti-access/area-denial (A2/AD) capabilities to prevent the United States and its allies from intervening against their acts of aggression.[13] In doing so, DOD should balance its investments in new, traditional weapon systems—incredibly powerful, multifunction platforms that are intricate compilations of capabilities—with forces that are more modular, scalable, adaptive, and unpredictable.[14]

In particular, the United States must address the way in which China has carefully designed its systems warfare strategy to counter America's traditional way of war.[15] While A2/AD threats are often treated as operational challenges, China intends to employ them to achieve strategic-level effects that render the most critical elements of U.S. operations ineffective.[16] By targeting U.S. datalinks, disrupting information flows, denying command and control (C2), and kinetically targeting physical "nodes" of U.S. information system, China is planning systematically to blind U.S. commanders and paralyze their operations.[17]

This does not mean that DOD should ignore lesser threats to America's security interests. Regional adversaries like Iran and North Korea remain significant threats, given their possession of ballistic missiles and nuclear weapons technologies. Non-state actors such as the Islamic State group, al- Qaeda, the Taliban, and al-Shabab will also continue to threaten U.S. security interests. Ignoring these problems creates opportunities for them to grow in scale and severity.

The concurrency of these threats—from the high end to low end—is placing stress on an American military that is now too small, too old, and has too few high-end capabilities. DOD's current force design is in a position where it will likely need to use its high-end forces to handle lesser challenges. While this would provide force overmatch against adversaries at the low end of the spectrum, over the long term, it could also place America's military strength at risk. From both a human capital and technology vantage, using advanced combat aircraft for operations in permissive environments can decay their readiness to engage peer adversaries.[18] Moreover, it would likely accelerate their recapitalization schedule. For example, the high utilization rates of the U.S. Air Force's small fighter aircraft inventory in counter-terror operations advanced the need to start a Next Generation Air Dominance program. Because DOD's acquisition process takes decades to field sophisticated capabilities such as stealth aircraft, prematurely aging them could increase the department's cost burden and create additional risk in the event of peer conflict.

While rising peer adversaries must pace a new U.S. military force design, threats to America's military dominance are not purely external; there are also many internal organizational, bureaucratic, and statutory obstacles to regaining a strategic and military advantage.[19] DOD's 5000 series of acquisition regulations is a prime example. This large collection of policies, mandates, and resulting bureaucratic culture decreases the agility of the department's acquisition system and extends the time required to develop and field new capabilities. This places U.S. forces at a disadvantage in long-term competitions with peer or near-peer competitors.

Terms of Reference

Systems Warfare: A theory of warfare that does not rely on attrition or maneuver to achieve advantage and victory over the adversary. Instead, systems warfare targets critical points in an adversary's system to collapse its functionality and render it unable to prosecute attack or defend itself. A major objective of this approach is to maximize desired strategic returns per application of force (achieve best value).

Force Design: Overarching principles that guide and connect a military's theory of warfare and victory, its doctrine, operational concepts, force structure and capabilities, and other enterprise functions.

Disaggregated Element: Functionality that has been decomposed to its most basic practical combat element; for example, an observation or orientation function. These elements can range from simple functions, such as a single-sensor observation node, to more complex platforms, as needed, to be viable in the overall combat system, such as a multifunction aircraft.

Node: An element in the combat zone, whether disaggregated or multifunction, that participates in the operational architecture by receiving and sharing information.

Mosaic: A force design optimized for systems warfare. Modular and scalable, a mosaic force is highly interoperable and composed of disaggregated functions that create multiple, simultaneous kill webs against emerging target sets. A mosaic force's architecture is designed for speed, has fewer critical nodes, and remains effective while absorbing information and nodal attrition.

Mosaic warfare is a force design that can address these challenges in an era of growing risk to U.S. interests globally. The term "mosaic" reflects how smaller force structure elements can be rearranged into many different configurations or force presentations. Like the small, dissimilar colored tiles that artists use to compose any number of images, a mosaic force design employs many diverse, disaggregated platforms in collaboration with current forces to craft an operational system. Functional capabilities hosted on a common platform like a combat aircraft, such as radar, fire control, and missiles, can now be disaggregated into their smallest practical pieces. Mosaic, however, is not just an automated loyal wingman-like approach that takes manned and unmanned aircraft collaboration to an extreme.[20] A mosaic force design employs

disaggregated platforms that can collaborate in a flexible and adaptive manner to accelerate the pace of U.S. operations and close kill chains. This coordinated system is made possible by the use of advanced networks, data links, and enablers that employ automation and artificial intelligence/machine learning to connect its disparate capabilities, much like the mortar an artist uses to assemble tiles into a picture. Mosaic leverages the dynamic relationship between force structure and operational concepts—*means* and *ways*—to regain offensive initiative against enemy systems warfare. Said another way, a traditional approach to dealing with emerging threats is to devise new, more effective ways to use existing military forces, or acquire new capabilities that will improve a military's ability to perform its missions. The mosaic concept does both.

At its foundation, mosaic leverages the power of information networks to create a highly disaggregated kill web that: (1) minimizes the critical system value of U.S. nodes that an enemy can target, and (2) ensures U.S. power-projection forces are effective in contested environments. At the same time, disaggregated functionality will allow a future mosaic force to be highly adaptable across the spectrum of military operations. A mosaic force structure is made of disaggregated platforms that, when composed together, complete operational observe–orient–decide–act cycles ("OODA loops") and kill chains. Like LEGO® blocks that nearly universally fit together, mosaic forces can be composed together in a way to create a focused, bespoke force package near time of need that can effectively target an adversary's system with just-enough overmatch to succeed.[21]

Mosaic leverages the dynamic relationship between force structure and operational concepts—*means* and *ways*—to regain offensive initiative against enemy systems warfare.

This study's purpose is to describe the attributes of mosaic warfare and propose a notional, abstract architecture for conducting mosaic warfare against a peer adversary, such as China. The attributes, architecture, and functional relationships between the components of a mosaic force are derived from decomposing kill chains and enabled by artificial intelligence across information networks. While mosaic warfare is a framework that spans all domains and joint operations, this study focuses on the air domain. This choice is deliberate, as aerospace power has historically executed operations using attributes that one could describe as mosaic.

As DOD moves to implement the *2018 National Defense Strategy*, it has an opportunity to develop a mosaic force design that will help transform its increasingly obsolescent way of war into one that can prevail against peer adversaries postured to defeat the U.S. military's current force design and operating concepts. The breadth of a mosaic force design is ambitious and has the potential to impact the whole life cycle of the American warfare complex, from its requirements and acquisition processes to its operational planning, tactics, techniques, procedures, and actual operations. In short, DOD must act if it is to remain a dominant military force capable of serving U.S. interests globally. Mosaic warfare is a path to this objective.

Describing the American Way of War and Force Design

The American way of war is inherently offensive. Since World War II, American combat power has been based on projecting large numbers of forces from garrisons in the United States to secure national interests abroad. U.S. military operations rely on offensive principles such as maintaining the initiative, gaining freedom of access and maneuver, and forcing an adversary to react to the U.S. game plan, not the other way around.[22]

Industrial and technological superiority has long underpinned America's military dominance. During the Cold War, U.S. strategists developed nuclear weapons and the means for their delivery to offset the Soviet Union's ability to mass superior forces and win a war of attrition with the United States and its allies. Described as the *First Offset Strategy,* this approach was sufficient for a period to deter Soviet conventional aggression.[23] After the Soviet Union developed similar nuclear capabilities, the United States embraced a new nuclear weapons strategy called mutually assured destruction and incorporated tactical nuclear capabilities into its conventional war plans.

> The American way of war is inherently offensive.

In the 1970s, a *Second Offset Strategy* sought to maximize the effectiveness of DOD's conventional forces. The theory of the case was that U.S. forces would have the capacity needed to neutralize the Soviet military's massed forces, if individual U.S. weapon systems—whether a bomber, fighter, or tank—could achieve a higher kill ratio.[24] American forces could then maintain the initiative and prevail in an attrition-based conflict. To that end, the U.S. military pursued advanced technologies to enhance its situational awareness and command and control in areas of operation, improve its ability to attack with precision using laser-guided bombs and other weapons, and develop more-survivable weapon systems such as stealth aircraft.

These technologies and force enhancements revolutionized the U.S. military's kill efficiency. For instance, instead of allocating the weapon loads of an entire squadron of F-4 Phantom fighters to drop a bridge, a single sortie and single laser-guided munition could achieve the same effect. This "one bomb, one target" ability would allow air planners to reallocate other F-4s in a squadron to attacking additional targets. In addition to fielding precision weapons technologies, this radically improved ability to target with precision required the Air Force to develop new concepts of operation that better integrated information flows in wartime environments, accelerated information processing, and streamlined command-and-control procedures.

As the *Second Offset Strategy* unfolded, U.S. service members at all levels saw their relationship with information change. No longer was this commodity the primary purview of high-level commanders responsible for strategy development, target planning, and operational maneuver. Information from systems designed into precision-delivery platforms and weapons became an advantage to military personnel at all operational levels.

Furthermore, it was increasingly important to deny this kind of information to an adversary. An example of this new reality was the incorporation of stealth technologies into combat aircraft to give American pilots a new means of denying an enemy the information needed to detect and target them.[25]

While facets of this new information warfare approach began to emerge during the Vietnam War, the concept was more fully employed during Operation Desert Storm in 1991 against Iraq. Stealthy F-117 Nighthawk fighters armed with laser-guided bombs easily penetrated Iraqi air defense systems. The combination of stealth and precision weapons enabled fewer U.S. aircraft to destroy a much greater number of targets relative to non-stealth aircraft using unguided bombs.[26] The reason was simple: without stealth, packages of strike aircraft needed a larger number of aircraft to jam enemy sensors and suppress surface-to-air threats. With stealth and precision, U.S. air forces could destroy targets using a relative handful of highly survivable aircraft (see Figure 1).[27]

Systems Warfare: Operation Desert Storm

Beginning in the 1980s, the Air Force's force design was characterized by the precision delivery of munitions, stealth, advanced processing, and unchallenged information superiority. This force design proved to be a stunning success in Operation Desert Storm.[28] As pivotal as new technologies were against Iraqi forces in 1991, one should remember that the coalition of the United States and its allies achieved victory as the result of how it used new technologies. The U.S. military showcased a *systems warfare strategy* during the conflict that was based on achieving specific desired effects.[29] In particular, the Desert Storm air campaign was a distinct departure from the traditional military campaign strategy of attrition warfare. Instead of waging blunt, force-on-force warfare as pre-war contingency plans originally called for, the air campaign was designed to immobilize Iraqi fielded forces by disrupting their command chain and isolating them from their leadership. This was achieved by targeting the Iraqi regime as a system.[30]

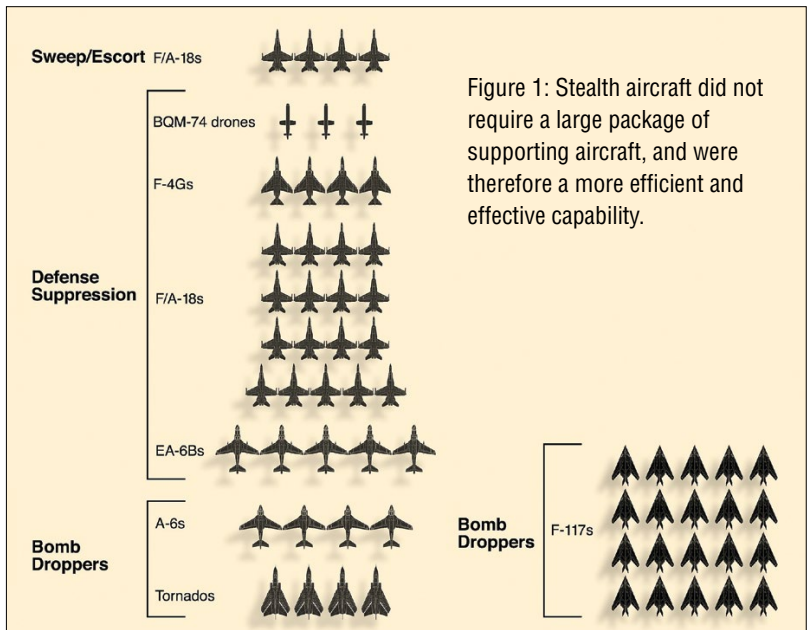


Figure 1: Stealth aircraft did not require a large package of supporting aircraft, and were therefore a more efficient and effective capability.

Source: Deptula, *Effects-Based Operations.* Artwork: FoxbatGraphics.

Coalition air planners understood the Iraqi political regime and military were tightly linked and operated as a system akin to Soviet operating practices. Centralized command and control meant that the system had networks and key nodes that they could physically target. Accordingly, the coalition master air attack plan sought points of vulnerability in the Iraqi military enterprise whose destruction would precipitate

regime collapse and incapacitation of its fielded forces, leaving units and leadership figuratively and literally in the dark. This systems warfare approach targeted the Iraqi military's information and command-and-control systems to "blind" them and paralyze their ability to act. For example, the coalition specifically targeted one bridge that crossed the Tigris River in Iraq not because destroying the bridge would limit maneuver, but because critical communications lines from an Iraqi air defense center ran underneath the structure. Taking the bridge down would disconnect that critical node from Iraqi missile sites.[31]

In the decade that followed Desert Storm, the Air Force continued to develop more-advanced information-centric technologies like fifth-generation fighters with an integrated sensor suite, advanced C2 systems, and space-based precision navigation and timing. In particular, data links that enabled the sharing of information and accelerated kill chains became an essential element of modern American combat power.

Despite these innovations, key elements of this nascent U.S. force design were nearly abandoned after the launch of Operation Enduring Freedom in 2001 in Afghanistan and Operation Iraqi Freedom in 2003. As the campaigns turned into grinding occupations, U.S. decision makers grew comfortable pursuing military modernization paths whose success required permissive, uncontested threat environments. Cancelling the Air Force's F-22 Raptor fighter program in favor of capabilities that could not survive in high-end threat environments was emblematic of such trends.[32] On top of this, the U.S. military became highly dependent upon networks and ubiquitous information sharing that enabled a severe level of centralized operational control. This led to a level of micromanagement that many considered necessary to reduce risk of losing "hearts and minds" from collateral damage during counterinsurgency operations, especially operations in urban areas. Further, some U.S. defense officials maligned lessons learned in the early days of systems warfare as increasingly irrelevant in the absence of a peer competitor.[33] At the same time, the perceived lack of a peer adversary cultivated overconfidence that U.S. forces would always be able to maneuver freely in all operational domains, including cyberspace. The very foundation of the American way of war—networks and information—evolved on a sideways course that ultimately created a tremendous degree of fragility and vulnerability.

This systems warfare approach targeted the Iraqi military's information and command-and-control systems to "blind" them and paralyze their ability to act.

Today, the ability to share information in near-real-time provides U.S. forces with better operational awareness and the capability to close kill chains more responsively and with greater precision than in any time in the past—in permissive operational environments. As has often been the case, assumptions on "the way of the future" have led to a way of war that is now increasingly vulnerable in a peer conflict. Since Desert Storm, adversaries have systematically worked toward eroding the U.S. military's advantages and exploiting deep vulnerabilities in its force design. Their military strategies, backed up by A2/AD capabilities, are designed to block America's physical access to combat zones and negate its ability to maneuver.[34] Wargames centered on major conflicts with China and Russia have resulted in loss after loss for U.S. forces.[35] According to senior RAND analyst David Ochmanek, "In our games, when we fight Russia and China, blue gets its ass handed to it."[36] Something must change.

Changing U.S. Force Design is Critical For Implementing the *2018 NDS*

A military strategy is typically broken down into ends, ways, and means. *Ends* are the objective, such as dissuading and deterring a nation's adversaries or defeating them across the spectrum of conflict. In order to dissuade or deter, a military must pose a credible threat to an adversary and cause its leadership to conclude that it may not be able to achieve its goals or do so at an acceptable cost. It is in this way that the U.S. military assures America's allies, deters conflict, and defends the nation when deterrence fails.

The *ways* of a strategy describe how to achieve its objectives, and *means* such as bombers, fighters, ships, or tanks, are the tools to execute the ways. In any conflict, force structure and capabilities available shape of the art of strategy. Means and ways are tightly coupled: weapon systems possessed by a military (means) and its tactics, techniques, procedures, and operational concepts (ways) interact in a constant and dynamic fashion.

The term "force design" is used to describe the underlying principles and composition of a military: its organization; doctrine and operational concepts; weapon systems; tactics, techniques, and procedures; and force presentation in support of a defining military strategy. A force design is the deliberate composition of ways and means to best achieve a strategy's ends, and a military's means constrain the ways it can operate and therefore limits ends it can accomplish. This is why force design matters.

The term "force design" is used to describe the underlying principles and composition of a military: its organization; doctrine and operational concepts; weapon systems; tactics, techniques, and procedures; and force presentation in support of a defining military strategy.

Warfare is a contest, and one must conceptualize the principles that underlay any force design within the context of that competition. Since the fall of the Soviet Union, the U.S. force design has largely been driven by a series of defense resource cuts to achieve arbitrary budget targets, not to support the nation's defense strategy. In other words, it is not the product of a deliberate strategic vision.[37] It is true that operational concepts and tactics can quickly evolve in response to new threats, and innovative uses of existing weapon systems can create powerful new effects. However, using old items in new ways can only go so far, and it often takes decades for a military to develop and field new weapon systems.

Today, adversaries are developing capabilities and shaping their militaries and operating concepts to blunt or dismantle America's legacy way of war and its inherent vulnerabilities. A new U.S. force design is needed if the United States is to regain its competitive advantage. In other words, DOD must develop the right mix and quantity of military capabilities and prepare to employ them in ways that will achieve the *2018 National Defense Strategy's* objectives. This is a major reason why the U.S. military must adopt a new force design. Failing to do so would risk losing a future great power conflict because of a force design that is too small, too old, too fragile, and overmatched.

China's and Russia's Anti-Access/Area-Denial Threats

The U.S.-led coalition victory against Iraq in 1991 was a wake-up call to China and Russia. Since then, they have examined the American way of war and the operational concepts and technologies that have made it successful. In response, both developed force designs meant to stymie U.S. military advantages.[38]

It is important for U.S. military planners to understand that while China's and Russia's A2/AD complexes are both designed to counter how America projects military power, their warfighting strategies are different. One can roughly characterize Russia's A2/AD as Soviet redux, using advanced technologies to create an umbrella that protects its own field maneuver operations.[39] While Russia's design relies on attriting NATO aircraft on the ground and in the air, China has adopted a more strategic doctrine. Having studied Desert Storm and subsequent U.S. contingency operations, China has developed systems warfare doctrine *with Chinese characteristics*.[40] This way targets critical nodes in the U.S. military's C2, information, and other systems in order to paralyze its operations and negate its forces.[41]

China has developed systems warfare doctrine *with Chinese characteristics.*

Describing Anti-Access/Area Denial

Anti-access systems and operations are designed to undercut the U.S. military's ability to project power quickly over long distances into a combat zone in a theater.[42] Whether volleying ballistic missiles against U.S. bases or using anti-ship cruise missiles to interdict strategic lines of communication, anti-access operations can delay U.S. forces and create time to achieve a fait accompli.[43] Air Force Maj Gen Alexus G. Grynkewich, now the commander of the 9th Expeditionary Task Force-Levant in Kuwait and the lead officer in charge of the Air Force's 2016 Air Superiority Enterprise Capability Collaboration Team, cautions that anti-access operations are not limited to the physical warfighting domains: "Cyberspace capabilities might be used against air or space capabilities or against friendly cyber forces. Such threats might preclude logistics in forward areas for aircraft or force cyber operators to shift to a defensive focus—the virtual equivalent of denied battlespace in the physical domains."[44] An anti-access approach can cause U.S. forces to operate from distances that exceed the ranges of their weapon systems.[45]

Area-denial capabilities, such as advanced surface-to-air missiles (SAMs), are designed to deny U.S. forces freedom of maneuver in an area of operations.[46] Grynkewich explains, "They cannot attack an adversary's area-denial threats because anti-access capabilities prevent them from projecting power into a theater. They cannot attack the anti-access threats because they are heavily protected by area-denial capabilities."[47]

Russia's A2/AD

Russia is the primary developer and exporter of A2/AD systems.[48] In addition to foreign military sales of the S-300 SAM system to a large number of countries, Russia's Rosoboronexport has deployed advanced

S-400 SAMs to the Baltics and Crimea, as well as exported the system to China and Turkey.[49] The S-400 is a particularly lethal mobile SAM. Its Tombstone phased-array radar has exceptionally long detection ranges and can display hundreds of targets simultaneously, including ballistic missiles and aircraft with limited-aspect stealth.[50] Russia's A2/AD complex also includes advanced missile systems such as the SS-26 Iskander short-range ballistic missile and Kalibr sea-launched cruise missile.[51] In addition to these kinetic threats, Russia has widely fielded electronic warfare (EW) systems to exploit the United States' heavy reliance on information and data links. Daniel Gouré, PhD, senior vice president with the Lexington Institute, assesses that "Russian EW systems have demonstrated a highly sophisticated ability to jam communications systems, deny access to GPS, and interfere with the operation of sensor platforms."[52]

Using A2/AD systems in a conventional, attrition-based manner, Russia can create an umbrella of air superiority to support its air, ground, and sea operations. Russia's Vostok (West) 2018 exercise integrated long-range SAMs like the S-300 and S-400 and short- and medium-range ballistic missiles. The purpose was to "demonstrate to NATO that Russia is indeed a minefield for enemy aircraft daring to penetrate its airspace," reported *The National Interest* magazine.[53] By creating a strategic buffer zone between NATO and Russia, A2/AD defenses, as Russia employs, could deny the United States and its allies the initiative and freedom of maneuver early in a conflict.

There is evidence that Russia is beginning to evolve its Soviet redux strategy.

There is evidence that Russia is beginning to evolve its Soviet redux strategy.

China's A2/AD

In contrast to Russian military thought, China will use its layered A2/AD systems and other military capabilities to wage systems warfare against U.S. forces. While Russia's approach to A2/AD seeks to improve the operational effectiveness of its air and ground forces, China is taking a strategic vector that presents the United States with a quite different challenge.[55]

The overwhelming effectiveness of the United States in Operation Desert Storm precipitated a major shift in Chinese military theory, as China scholar M. Taylor Fravel, PhD, notes: "China's intensive study of the United States through the 1990s, especially towards the end of the decade, was also intended to identify weaknesses that could be exploited in addition to areas to copy."[56] In the official history of the Gulf War by the People's Liberation Army (PLA), China's Academy of Military Science concluded, "The Gulf War has led to a world-wide military transformation characterized by the shift from mechanized warfare to information warfare."[57] In other words, information essential to high-tech weaponry and to coordinate and synchronize military operations has become the focus of modern warfare.

By 2002, this perception of the role of information in warfare was transforming China's military strategy. In a speech to the Chinese central military commission, the highest military body of the Chinese communist party, Jiang Zemin, then-party chairman and Chinese president, announced four trends that characterize Chinese military investments and strategy. First, "informatized" military weapons and equipment are core to a nation's military strength. Second, China needed stand-off, long-range strike capability to target adversary command and control; intelligence, surveillance, and reconnaissance (ISR); and air defenses. Third, systems warfare would become the defining characteristic of modern warfare. Finally, space "would become the new high ground," said Zemin.[58] These statements were indications of the characteristics that would come to define how China intends to employ its A2/AD systems.

China needed stand-off, long-range strike capability to target adversary command and control; intelligence, surveillance, and reconnaissance (ISR)... systems warfare would become the defining characteristic of modern warfare.

The extended range of China's A2/AD systems creates a forward strategic defense in depth that can prevent many U.S. command-and-control and ISR assets from operating close enough to a combat zone to be of value, thus significantly degrading the overall U.S. system of waging war.[59] Robert O. Work, former US deputy defense secretary, stated that in a conflict with China, the Chinese would "attack the American battle network at all levels, relentlessly, and they practice it all the time."[60] This is in line with China's "system-of-systems paralysis" strategy, which asserts that the way to victory is to target an adversary's C2.[61] China's 2005 Science of Military Strategy asserts that:

> *Intelligence, reconnaissance, communication, command-and-control systems link the battlefield into an organic whole, so that the enemy's information systems and decision-making processes are becoming the most important targets in information warfare. … By destroying, confronting, suppressing, and interfering in the enemy's information systems and decision-making processes, one can destroy the enemy's information capability and paralyze his combat structure, so that one can better grasp the initiative on the battlefield and achieve the war purposes more effectively.*[62]

A translation of China's 2013 edition of this same strategy makes the connection between information and kinetic operations even more explicit:

> *Strike, triggering its system damage linkage, making the integrity, stability, and balance of the system impetuous decline, and then cause its structural defects, program disorders, and functional decline. … In information-based warfare, information soft-killing and firepower destroying [sic] each other.*[63]

RAND analyst Jeffrey Engstrom calls China's strategy "system confrontation" and its theory of victory "system destruction warfare."[64] China's July 2019 defense white paper did not materially update or alter its systems confrontation and theory of systems destruction warfare.[65] The Chinese A2/AD complex remains part of China's strategy to degrade and disrupt U.S. operations by targeting U.S. forces as a system.

In combat operations, Engstrom notes that "PLA planners specifically seek to strike four types of targets, through either kinetic or non-kinetic attacks, when attempting to paralyze the enemy's operational system."[66] These attacks encompass:

Degrading or disrupting the flow of information in the adversary's operational system. These attacks target networks and data links and key nodes to leave elements of the operational system "information-isolated" and thus ineffective.[67]

Targeting the key nodes or functionalities within the adversary's operational system. These "essential factors" include command and control, ISR, and firepower: "if the essential elements of the system fail or make mistakes, the essence of the system will … [become] non-functional or useless."[68]

The U.S. military must reinvigorate the analytical rigor and the theory of systems warfare first manifested during Operation Desert Storm. Mosaic warfare is an innovative force design for composing U.S. forces and operational concepts in ways that will optimize them for systems warfare of the future, rather than for conflicts of the past.

Degrading or disrupting the operational architecture of the adversary's operational system. This seeks to disrupt how elements of an adversary's system collaborate and support each other.[69]

Distorting and extending the adversary's time sequence or operational tempo (OODA loop). Objectives of these attacks are to slow down or induce friction, confusion, and chaos into an adversary's system by employing deception, creating nodal failures and network/datalink outages, and other means that might cause "stutter" at any phase of an enemy's OODA loop or kill chain.[70]

Future adversaries will learn from China's progress toward maturing a systems warfare theory that targets U.S. force design and operations. In other words, systems warfare will not be limited to China, and DOD should consider "systems confrontation" and "systems destruction warfare" as leading indicators of how peer and near-peer adversaries could hold U.S. forces and operational architectures at risk in the future.

Consequently, without significant changes, neither the ways nor the means available to U.S. forces will be sufficient to accomplish the ends outlined in the *2018 National Defense Strategy*. The U.S. military must reinvigorate the analytical rigor and the theory of systems warfare first manifested during Operation Desert Storm. Mosaic warfare is an innovative force design for composing U.S. forces and operational concepts in ways that will optimize them for systems warfare of the future, rather than for conflicts of the past.

Today's Force: Lack of a Clear Design

If the *ways* U.S. forces have to achieve *ends* are limited by *means*, why not simply recapitalize and field new capabilities? Would recapitalization and modernization alone create the force design the nation needs? Current recapitalization programs and those in early stages of formation suggest otherwise. While emerging A2/AD challenges are now well understood, some in DOD continue to adhere to a traditional, linear approach to defeat them. While more-advanced technological innovations will undoubtedly be valuable additions to the future force, DOD must not neglect developing concepts for how they could best be used to counter how China intends to target U.S. forces *as a system*.[71] This is key: DOD cannot simply focus on building a better mousetrap. China's strategy is to target, disrupt, and disable the military systems of its adversaries.[72] New operational concepts coupled with a new force design are needed that will negate China's strategic assumptions and the value of the critical command-and-control loci they will target. These concepts and force design must also ensure future U.S. forces will be capable of projecting power with sufficient lethality and agility to impose severe costs on peer adversaries.

Relying on Old Approaches to New Problems

Many of the debates currently consuming DOD center on what technologies and approaches will be required to counter A2/AD umbrellas. Should the United States shift toward fighting from outside them using stand-off weapons? How will U.S. forces obtain "tip-and-cue" information needed to close precision kill chains from a distance? What capabilities will they need to negate advanced integrated air defense systems in order to achieve freedom of maneuver?[73] And if U.S. forces plan to penetrate contested areas, what technologies will they need to survive?

DOD must not neglect developing concepts for how they could best be used to counter how China intends to target U.S. forces *as a system*. This is key: DOD cannot simply focus on building a better mousetrap.

These are also linear, attrition-based approaches that will present peer adversaries with a math problem they can solve by fielding additional forces and better A2/AD technologies. Other perspectives are just as linear. For example, Christopher M. Dougherty, senior fellow with the Center for a New American Security (CNAS), notes: "U.S. operational concepts for defeating Chinese or Russian aggression should focus on … power-projection forces operating within functional A2/AD networks, before those forces can seize key objectives. … [and on] developing concepts and capabilities that within 72 hours can damage or destroy roughly 300-plus high-value PLA navy vessels in Chinese littoral waters" and even more massive numbers of Russian armored vehicles.[74]

It is also important to note that these debates treat Russian and Chinese A2/AD challenges in a similar fashion, with differences focused primarily on theater geographic features and attack force compositions (such as land versus sea forces) best suited for them. Because Russia's doctrine for using its A2/AD systems is relatively conventional, traditional approaches such as those highlighted above could help deter Russian

aggression. This is a dangerous assumption if one believes that similar operational concepts and force designs will prevail against China. It is unlikely that using new technologies in traditional ways will sufficiently mitigate weaknesses in U.S. operational architecture that China is preparing to exploit. To gain the full value and potential of high-end capabilities like stealth fighters and B-21 Raider bombers, DOD must augment and employ them within the context of a broader, enhanced strategy.[75] Continuing to adhere to reactive, linear approaches to counter China's A2/AD technologies could, over time, lead to the further erosion of America's comparative military advantages.

A New Design Must Be Balanced for Low-End and High-End Threats

DOD is challenged with another strategic choice: should it continue to build traditional weapon systems that will be capable against peer adversaries, but may not meet capacity requirements, or should it buy greater numbers of less capable platforms for low-end operations? DOD cannot afford to do both. Indeed, present defense budgets do not procure the number of high-end platforms the United States needs or do so at the rate they are required. There is no budget space for low-end capabilities. In this context, the current approach to force design must be biased toward high-end capabilities in order to meet the demands of the *2018 NDS*.

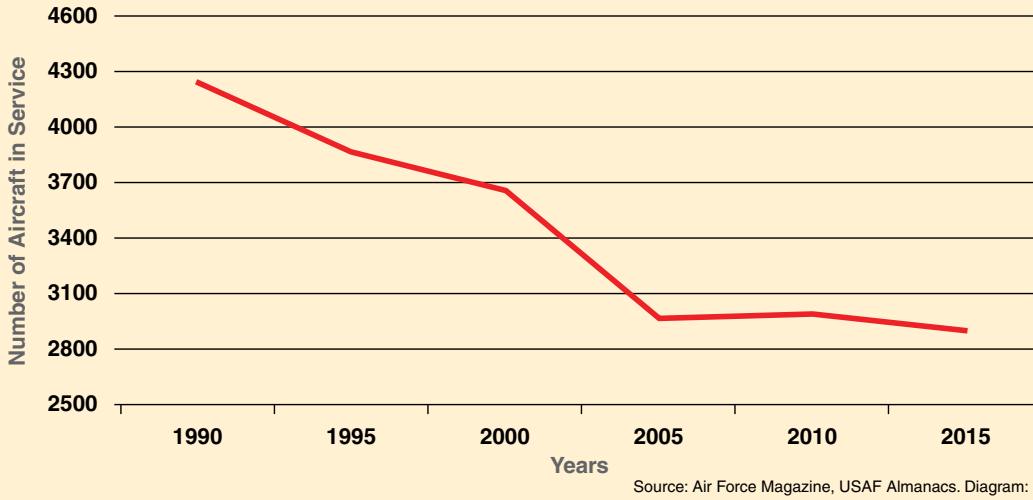
Despite a public weary of conflict and mixed signals from numerous administrations, it is unlikely that U.S. forces will soon leave the Middle East.[76] The rapid expansion of the Islamic State in 2014 served as a cautionary tale of the risks that can follow premature military disengagements. But using higher end capabilities like the F-16 Fighting Falcon, F-15E Strike Eagle, and even F-22 and F-35 Lightning II fighters, in less demanding operations can be inefficient, cost-imposing, and harmful to the long-term health and readiness of the force. Sustained high operations tempo can prematurely wear out advanced weapon systems with limited life spans and further strain the defense budget.[77] With no viable alternatives, depending on high-end forces for low-end conflicts can cause operators to lose their combat edge and reduce their readiness to quickly respond to advanced threats. Diminished readiness incentivizes adventurous behavior by global rivals who may take advantage of security voids.

A U.S. force design must be able to compose and scale appropriately across the spectrum of conflict. Measured in readiness, force flexibility, or simply treasure, DOD's current force design works against this goal. This does not mean that the department should refrain from using some high-end assets in low-end arenas. As any military official knows, there is a minimum viable force and support package necessary to deploy and support operations even in relatively permissive environments. Future conflicts, low-end or otherwise, will require forces that are modular, relevant, and affordable.

Budget Limitations Will Continue to Be Significant Drivers of Force Design

Since the Soviet Union's decline, budget pressures have been the predominant factor that shaped U.S. force design. In the absence of a peer threat, every one of the services suffered drastic cuts in the interest of reaping a so-called peace dividend. The Air Force lost more than half its force structure in the 1990s, and

Figure 2: Air Force capacity has been cut by more than half since the 1990s and is smaller than at any time in the service's existence (since 1947).

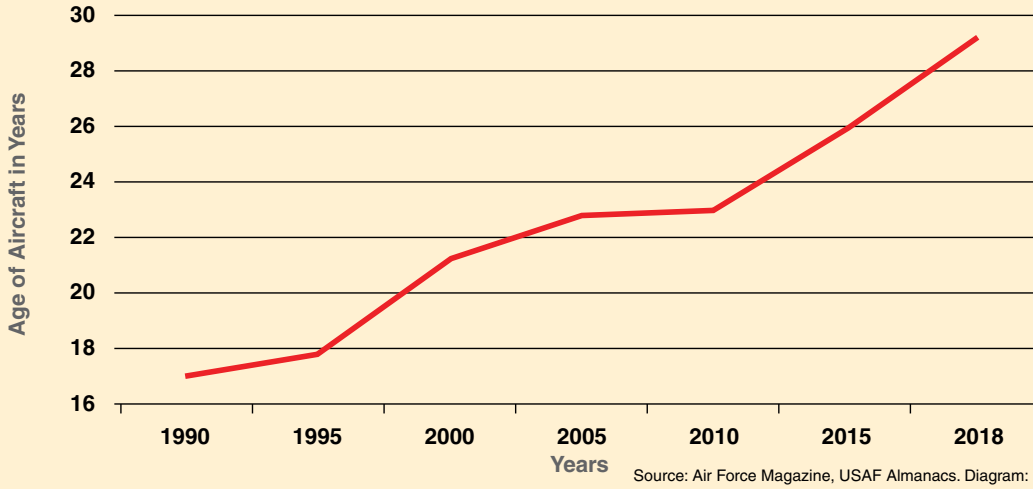


Source: Air Force Magazine, USAF Almanacs. Diagram: FoxbatGraphics.

its capacity is now at a record low (see Figure 2).[78] With peer threats a seemingly distant concern in the years after the Cold War and through much of the War on Terror, those inside and outside DOD decided to cut high-end force modernization accounts because there were seemingly no appreciable consequences for these reductions in the near-term.[79]

Unable to recapitalize with newer weapon systems at a level that aligned with emerging real-world operational demands, the Air Force funded service life-extension programs (SLEPs) to prolong the service lives of its older aircraft (see Figure 3).[80] Budget space required to extend the lives of legacy aircraft had to come from somewhere, and often, it was created by reducing recapitalization rates. Reduced recapitalization rates tend to increase the cost of SLEP programs, which meant there was less money available to buy new aircraft. This vicious cycle is still occurring today.

Figure 3: The average age of the Air Force's aircraft inventory rose from 17 years in 1990 to nearly 30 years by 2018.



Source: Air Force Magazine, USAF Almanacs. Diagram: FoxbatGraphics.

The increased costs of more-capable, multifunction aircraft and other means also affect force design. It makes sense to pursue economies of scale that yield program cost savings. However, this was not always the case in the post-Cold War era. Instead, large programs for advanced weapon systems were cut because that was where the money was, which increased their unit costs, which often begot additional cuts. In defense industry circles, this is known as the "death spiral." This cycle was a contributing factor in the termination of the F-22 program.[81] Ironically, many of these cuts were levied just as new weapon systems were beginning to meet their key performance and procurement cost goals, leaving the services with less capable and less dependable early production variants.

Aircraft and other systems that are capable of performing multiple functions, especially sensor-shooters, can increase the mission flexibility and lethality of a force design. In the post-Cold War era, however, a number of DOD leaders used the increased effectiveness of weapon systems as justification for cutting force structure or buying fewer new systems. This has led to today's anemic aircraft inventories that cannot meet the capacity demands of peer conflict. No matter how capable an aircraft is, it cannot be in two or more places at one time. There is a point where the force is simply too small, and the Air Force crossed that point years ago.

The proliferation of advanced weapons and improved information processing and software have dramatically undercut the U.S. military's legacy capabilities.

It is important to remember the broader context of the original *Second Offset Strategy* when considering future force designs. While *Second Offset Strategy* technologies gave a smaller U.S. force the capability to blunt a Soviet invasion of Central Europe, this smaller force continued to rely on tactical nuclear weapons to check the adversary's larger mass. The situation is different today. Not only has the United States relinquished the preponderance of its tactical nuclear weapons, the military modernization programs of its great power competitors have eroded America's technological advantage. The proliferation of advanced weapons and improved information processing and software have dramatically undercut the U.S. military's legacy capabilities. In other words, advantages unilaterally enjoyed by American forces in Desert Storm have proliferated to competitors. This is a reality that some U.S. decision makers still do not understand.

Make no mistake, advanced capabilities like fifth-generation aircraft are incredibly powerful weapon systems that incorporate cutting-edge software and sensor-fusion capabilities essential to winning in modern threat environments. However, numbers do matter. For too long, U.S. leaders in charge of key budget decisions assumed too much risk shedding capacity for short-term fiscal savings, rationalizing their decisions by pointing to the superiority of U.S. weapon systems. It is time to recognize the U.S. military no longer wields such a technological advantage.[82] Smaller but more capable is a myth in this era of renewed great power competition, and America's future force design must generate more capability *and* capacity.

Weapon Systems Survivability/Lethality Tradeoffs and Force Design

Weapon systems, such as aircraft, have a limited amount of internal space. Key factors in aircraft design is characterized as "SWAP-C," which stands for space, weight and power, and cost. Cooling capacity is also

critical. Aeronautical engineers have typically focused on designing military aircraft for the range, speed, endurance, maneuverability, and payloads they will need for specific missions. In the past, aircraft payload has often been defined by how many weapons it could carry. As aircraft became more multifunctional, their payload requirements had to account for the integration of sensors, processors, and other mission systems.

DOD is now challenged with creating a future force that can penetrate A2/AD environments, execute assigned missions, and then safely recover to its bases. A traditional approach to countering emerging threats is to increase the number of defensive systems used to ensure mission effectors survive. At a systems level, one might consider the payload constraints of stealth fighters. These aircraft must carry weapons internally in order to avoid detection in challenging radar environments. As a result, they are constrained to carrying smaller weapon loads when in a stealth configuration. The alternative of carrying weapons externally would increase their probability of being detected by enemy sensors. Adding to this is the increasing need for penetrating aircraft to have systems that gather information for defensive functions, which could reduce internal capacity available for offensive systems. Information requirements may overlap for some missions such as fighter sweeps or the suppression of enemy aircraft, but for the most part, information needed to close kill chains is not the same as information needed to defend against threats.

...traditional approaches to dealing with emerging threats can lead to the creation of a force design that shifts a military's center of mass toward defensive capacity at the expense of offensive capacity.

At a certain point, emphasis on improving the survivability of aircraft and other weapon systems that must operate in A2/AD environments may outweigh provisioning them with mission systems for offensive operations. Taken to absurdity, one could imagine a suite of defensive systems that took *all* of a weapon system's SWAP-C and payload capacity, leaving little or no remaining space for offensive capabilities. Expanding this logic to the macro level, traditional approaches to dealing with emerging threats can lead to the creation of a force design that shifts a military's center of mass toward defensive capacity at the expense of offensive capacity. A new force design for the U.S. military must seek to balance its defensive and offensive capabilities and capacity.

Own Worst Enemy? The Defense Acquisition System

It is not just budget pressures that have placed U.S. military dominance at risk. As potent as both fifth-generation and advanced legacy aircraft are, it is also true that U.S. forces remain vulnerable because complex weapon systems take far too long—in some cases nearly two decades—to develop and operationalize. Given the incredible pace of advancement in processors, materials, and computation, a 20-year developmental cycle means the newest U.S. weapon systems may lag state-of-the-art technology by several generations when fielded. The pattern of relying on decades-long defense acquisition programs to deliver large, multi-capability platforms has helped create a force that is perpetually nearing obsolescence compared to adversaries that are able to advance at a faster pace.

What is clear is that more of the same, even with acquisition reforms or incremental changes to DOD policies, is not going to restore America's advantage over its great power competitors. Numerous acquisition offices have been created to accelerate the development and fielding of advanced capabilities. To ensure the United States can stay ahead of its adversaries, Congress has also explored reforms such as requiring DOD to create a panel to review acquisition regulations. As directed by Section 809 of the 2016 National Defense Authorization Act, this panel reviewed the efficacy of other transaction authority (OTA) agreements that are intended to provide faster alternatives to the traditional DOD 5000 series acquisition processes. While OTA agreements are useful, they still do not guarantee that new weapon systems will rapidly advance from prototypes to production models.

Genuine DOD acquisition reforms that are responsive to the pace of developing technologies and emerging threats seem elusive. Efforts that try to work around the existing acquisition system often fail to directly address the root causes of the lack of innovation, program delays, and cost overruns. To be truly effective, any approach must be able to work *within* the existing acquisition system constraints and still field capabilities in relevant timelines. This could be aided by a new force design concept that addresses problems created by bureaucratic processes and cultures that resist reform.

Current Information Networks: Lost Opportunities for Force Transformation

Data links enabled higher levels of command to reach into cockpits and make engagement decisions for operators.

The information architectures and command-and-control systems that enabled the U.S. military to dominate permissive combat zones of the past are now increasingly at risk. Constructed within the strategic context of supporting counterinsurgency campaigns in permissive air environments, their architectures, security features, and other attributes are not survivable in a great power conflict. Limited, fixed, and brittle, U.S. information networks are becoming lucrative targets for China and Russia.[83]

The terrible irony is that the development of modern data links and networks should have led to a more resilient U.S. force design that relied on multiple kill paths of a web to conduct disaggregated operations. Networks did accelerate kill chains through more efficient cross-cuing, but they did not lead to disaggregated and decentralized operations. Instead, commanders generally used information networks to further centralize the execution of operations. Data links enabled higher levels of command to reach into cockpits and make engagement decisions for operators. The stories about commanding generals and lawyers on the communication loop directing tactical engagements in real-time are true. This normalization of network-enabled, centralized execution of operations means that today's military personnel are losing their ability to operate in a synchronized and independent manner. Micromanagement by centralized command and control drives tremendous inefficiencies and risk into operations. Tactical decision making and execution by committee at higher headquarters usually fail to move at a speed necessary to meet rapidly changing circumstances. It also fails to recognize that actors at the forward edge of the combat environment often

have the best understanding of complex circumstances. The tight coupling of strategic, operational, and tactical control is exactly what a systems warfare strategy seeks to achieve, much as the United States paralyzed Iraqi forces in Operation Desert Storm.

U.S. Military Information Network and Data Link Capabilities Could Fail Against Spectrum-savvy Adversaries.

U.S. military forces and operational concepts that rely on centralized C2 and other operational structures do not pose complex, wicked problems for adversaries. Current U.S. force design is also comprised of far too few fifth-generation aircraft and other advanced weapon systems. Moreover, the loss of a small number of networks or high-value airborne assets (HVAAs) could have a major impact on U.S. operations against a great power adversary. A U.S. force that relies on too few advanced weapon systems—all of which are dependent on vulnerable and brittle networks—reduces a peer competitor's operational problem.[84]

The U.S. Force Design Must be Relevant to Emerging Warfighting Strategies and Threats

The past 18 years of counterinsurgency operations have created a disconnect between the U.S. military's operating concepts, doctrine, and technologies. Instead of advancing the operational art and intellectual underpinnings of systems warfare, the U.S. military regressed toward an attrition-focused, occupation-based strategy to combat insurgent forces and terrorist extremist groups. U.S. military operations have come to rely on information systems and networks for C2, ISR, communications, and other operations with insufficient consideration for their vulnerabilities in a great power conflict. As Dougherty of CNAS notes, "many of these [C2, communications, computers, and ISR] assets and much of this experience [have] been oriented toward the relatively permissive environments prevailing in conflicts against weaker opponents."[85] Bluntly stated, the U.S. military is now dependent on information networks and systems that are not designed to survive high-end systems warfare. It also lacks a strategy for systems warfare that will shape the design of its future information systems and networks. This dissonance between the intellectual and the technological leave U.S. forces vulnerable to systems warfare. Given that DOD's defense acquisition system runs at a geologic pace, a more-of-the-same approach to building the future force could fail to deliver capabilities and capacity needed to maintain the advantage over great power competitors. *This is why America could lose a future war.*

U.S. military forces and operational concepts that rely on centralized C2 and other operational structures do not pose complex, wicked problems for adversaries.

Any future force design must be mapped against these gaps. The following points summarize some of the challenges and weaknesses in the U.S. military's force design, describe how they may affect its future operations, and briefly address the characteristics of a future force that is better able to absorb, sidestep, or frustrate how a systems warfare adversary could dis-integrate U.S. operations.

Endemic Problems of Current U.S. Force Design:

- **Small inventories of highly capable, multifunction platforms in the current force make operational architectures too vulnerable.** As powerful as they are, limited numbers of advanced, multifunction platforms present extremely valuable targets to the adversary because of the U.S. military's disproportionate operational dependence on them. The loss of a small number of fifth-generation, low-density aircraft or HVAA would weaken the United States' operational architecture and make remaining forces more vulnerable and less effective.

- **The practice of buying multiple, highly capable high-end weapon systems in small numbers is inefficient.** Preparing for a major conflict with a peer competitor will require increasing the overall size of America's military. DOD could reduce the cost of increasing its force capacity by exploiting mission systems that can be integrated in multiple new capabilities. It could also achieve economies of scale by procuring major new capabilities, such as stealth aircraft and unmanned systems, in larger numbers and at faster rates than in the past.[86]

- **It takes too long to develop and field new weapon systems.** The complexity of developing and integrating tightly coupled advanced technologies has extended the time required to field new weapon systems. However, this is more than a technological and engineering challenge; DOD's current policies and bureaucratic practices add a great deal of complexity and time to its acquisition process. In combination, these factors delay the fielding of new capabilities and create time for U.S. adversaries to develop offsetting systems.[87]

Current U.S. Force Design is No Longer Competitive in Today's Threat Environment:

- **The U.S. military's current force design cannot appropriately scale across the spectrum of conflict.** DOD's force structure is not large enough and lacks survivability against A2/AD threats. Moreover, persistently using high-end forces in low-end conflicts is an imprudent practice. The preponderance of legacy forces now in the U.S. military is the worst of both worlds: too costly for low-end operations, and not survivable-enough for great power conflicts. [88]

- **Current U.S. force design cannot withstand attrition, and survivability factors threaten to outweigh the ability to create effects in the modern, complex wartime environment.** The most-capable and most-valuable assets in the U.S. military's inventory, like fifth-generation fighters, are also those for which it has the least. High-value assets are lucrative targets, the loss of which would disproportionately degrade U.S. operations.[89] Because U.S. force design cannot withstand many losses of these critical platforms, survivability concerns threaten to bias DOD's technological investments and operational plans. The high number of increasingly less survivable fourth-generation aircraft in the force also increases the risk that well-trained aircrew could be attrited. These aircrew would be exceedingly hard to backfill quickly during great power conflict.

Mosaic Warfare: A Notional Framework for a Future Force Design

A future U.S. force design should address shortfalls in America's current defense enterprise summarized in previous sections. Given the many interdependencies between the ends, ways, and means of the *2018 National Defense Strategy*, a new design should be derived from an overarching operational concept that overcomes deficiencies that great power competitors can target. More specifically, DOD should consider a force design that builds upon the strengths of its current highly capable weapon systems partnered with large numbers of disaggregated elements to prevail against pacing threats delineated in the *2018 NDS*.[90] Adaptiveness across the range of missions and threat environments—from defeating an existential threat to eliminating a violent extremist organization—must be a key attribute of this new force design.

Given the many interdependencies between the ends, ways, and means of the *2018 National Defense Strategy*, a new design should be derived from an overarching operational concept that overcomes deficiencies that great power competitors can target.

Analysis in previous sections of this study suggest the following points should inform a new U.S. force design:

- **Combining highly capable, multifunction aircraft with additive, disaggregated systems will help empower collaborative teaming operations that diminish the vulnerability of U.S. military architectures.** Although highly capable systems now in the force perform certain functions exceedingly well, their limited numbers constrain a commander's strategic options. Moreover, the loss a handful of systems, such as HVAA, can have a high impact on U.S. operations. Collaboratively teaming disaggregated capabilities and highly capable aircraft could greatly enhance mission effectiveness. The loss of a disaggregated platform will not jeopardize the functionality of an entire system.

- **Disaggregated platforms, even those with advanced capability, will likely be more affordable and can be procured in greater numbers than highly capable platforms.** Sensors and systems integration represent a growing percentage of the cost of major new capabilities. Decreasing the quantity of sensors on future platforms could help decrease their size, weight, complexity, and overall unit cost. Lower program costs will allow DOD to buy more new systems and grow its force capacity.

- **Augmenting highly capable aircraft with disaggregated platforms could accelerate the development, testing, and fielding of a future force design.** The more complex a weapon system, the more time it takes to develop, test, and field it. Shifting toward procuring more disaggregated platforms could help reduce the time needed for DOD to create a force design needed to support the *2018 NDS*.

- **Creating a mixed force of highly capable and disaggregated platforms capable of operating in dynamic, collaborative ways should enable U.S. planners and commanders to tailor their task forces better to meet operational needs across the conflict spectrum.** A more modular force structure would allow operational commanders to configure task forces better to achieve desired outcomes and help ensure that highly capable systems are not overtaxed supporting low-end missions. If a commander can compose the force that will make up a warfighting system near the time of conflict, then the uncertainty of anticipating the far future (and its consequences on the requirements and acquisitions process) is lessened.

- **The U.S. military must grow its force structure so it can provide the degree of domain control and density of attacks needed to maintain the initiative and prevent an adversary from adapting to its operations.** This means increasing the quality and quantity of high-end highly capable platforms, disaggregated systems, and resilient mosaic enablers that will connect them in the future battlespace.

- **The United States must be able to rapidly field a force composition that surprises future adversaries and denies them the ability to predict and prepare for its military operations.** Surprise cannot be realized by a force that requires months to attain the degree of connectivity needed to ensure its full functionality. Quickly composing disaggregated capabilities into forces that surprise adversaries will require every element of the future force to be highly interoperable.

- **U.S. networks and information architectures must be flexible, adaptive, and resilient.** This does not mean more hardened and denser. Instead, future architectures should push information to specific forces and capabilities when and where needed, rather than everything to everything and all the time. This degree of flexibility will require the capability to maneuver information across the network and around threats when necessary.

- **The U.S. military's future force must be able to withstand virtual or actual combat attrition.** This means that no platform can be a single point of failure whose loss has a disproportionately negative impact on the force's operational effectiveness.

- **The force design must provide decision superiority despite the attempts of an adversary to disrupt OODA cycles at all level of operations.** An operational and information architecture that can both outpace adversary information operations and withstand attempts to degrade OODA cycles will be critical to prevailing in future great power conflicts.

These insights suggest that DOD should grow the size of its future force by maximizing to the extent possible its ability to network modular, heterogeneous, disaggregated platforms to create operational systems. But what might this framework look like? What kind of operational concept would it support? And how should it move information to achieve OODA superiority in the future?[91] Answers begin by examining past examples of a system's action cycle.

Colonel John Boyd's OODA Loop and the Kill Chain

Any student of Air Force Col John R. Boyd's OODA loop—the continuous cycle of *observe*, *orient*, *decide*, and *act*—will be familiar with the importance of speed through the OODA cycle and its subsequent iterations (see Figure 4). One gathers information from the environment (observe) and then orients oneself to the environment so that one can decide on a course of action, and then act. That action creates a response, and the cycle begins again. The faster one can complete the OODA loop and get inside a competitor's decision cycle, the greater is one's advantage. Usually the emphasis is on speed; by getting inside an adversary's OODA loop, the enemy will be responding to a situation that is no longer relevant, creating errors in their decision making and actions. Over time, these errors compound, reducing an enemy's cohesion and effectiveness.

Although Boyd was initially describing the mental processes of a fighter pilot in a dogfight, the OODA loop is an excellent cognitive model to describe organizations and systems as well. ISR-gathering activities correspond well with Boyd's observe step. Those observations are filtered, correlated, evaluated, and fused by analysts using specialized computers and algorithms and programs, like those that make up the Distributed Common Ground System (DCGS). Those processed observations (as intelligence) inform the commander's orientation of the area of operations. The commander then makes decisions, which are expressed through a tasking order, and forces in the area act based on the commander's decision. These actions are usually a mission, which may or may not result in a kinetic strike or other kind of effect.

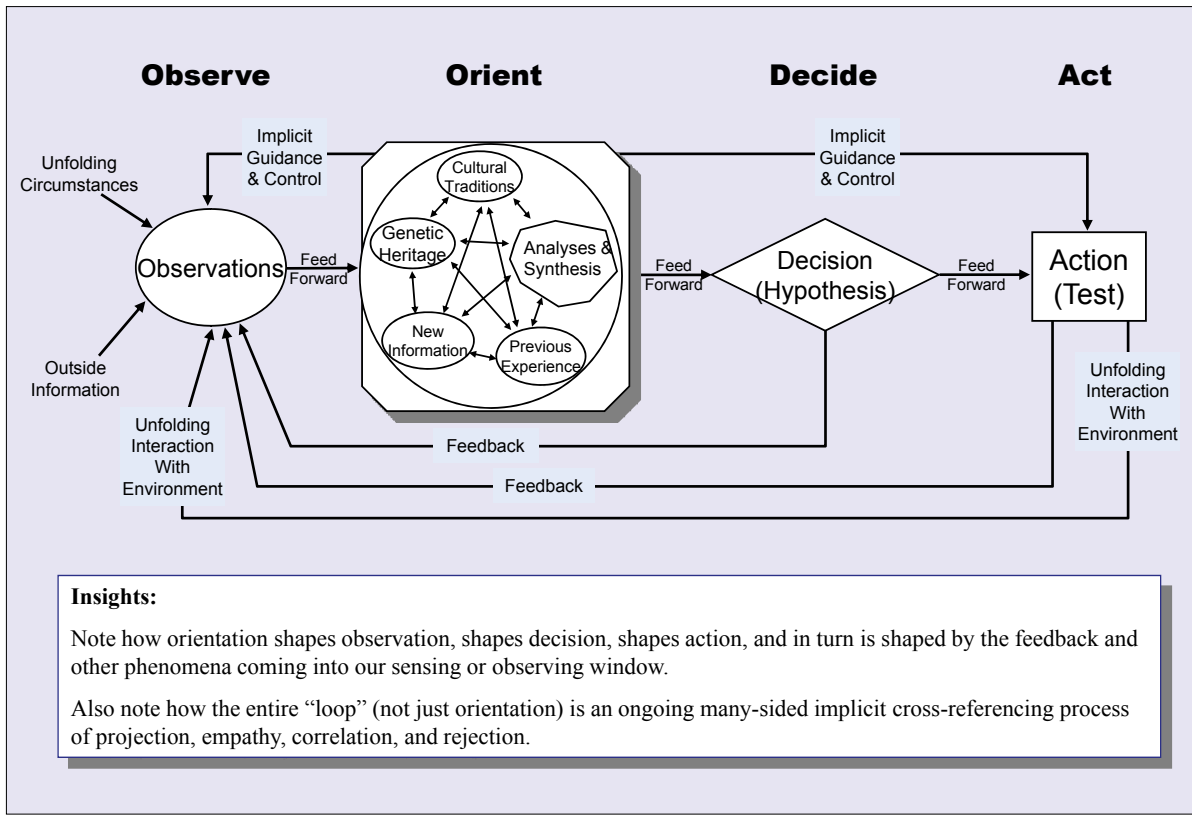


Figure 4. John Boyd's OODA Loop Sketch[92]

In World War II, Allied reconnaissance airplanes would fly over continental Europe taking photographs of areas of interest (*observation*). Military targeteers and intelligence personnel would process the images to create an *orientation* of the combat zone. Using that initial processed orientation, bomber commanders would layer additional meaning to *decide* their target priorities and dispatch orders to their forces. Bombing missions were the *action* step of this OODA cycle: they would *find* targets; *fix* them (affirm they were the correct targets); *track* and *target* them in their Norden bombsights; drop bombs to *engage* the targets; and then conduct initial battle damage *assessments*. The OODA cycle would then begin all over again (see Figure 5).[93]

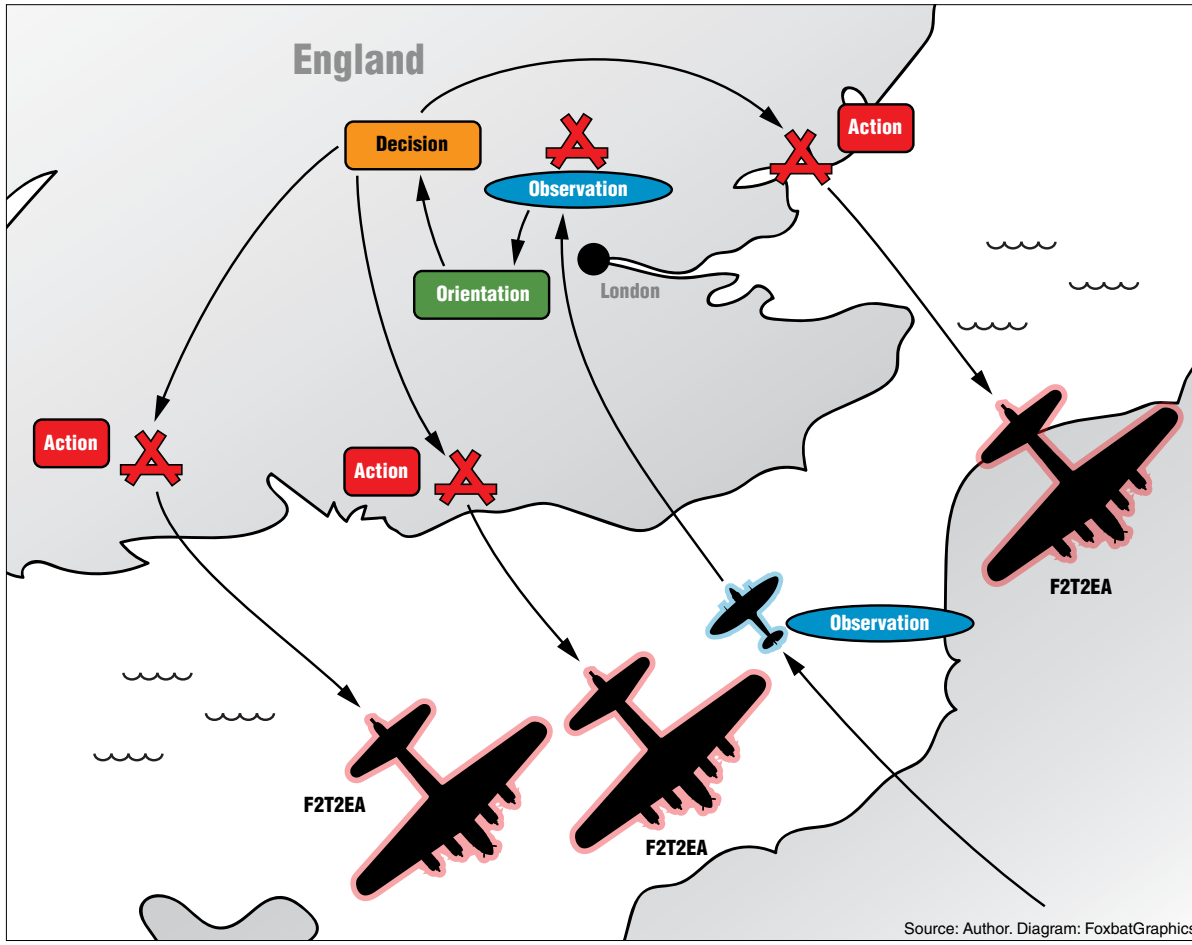


Figure 5. A depiction of the OODA loop in practice during the reconnaissance missions of the Allies during WWII.[94]

This OODA cycle could take weeks or even months to accomplish, since it was very sequential. Without observations, there could be no orientation, and observations required good weather and dedicated reconnaissance sorties that had to penetrate the air defenses of the Luftwaffe, the German air force. Allied reconnaissance airplanes could not maintain a persistent presence in the operations area, and the physical distances they had to fly took time. Once they returned, developing their film and the interpretation and manual analysis by intelligence analysts and targeteers to create orientation required more time. Making decisions regarding target sets and missions at higher headquarters, far behind the zone of combat, took the most time.

All these steps had to be accomplished sequentially before Allied bombers could be dispatched on missions. Then, the time needed for bombers to fly their missions decreased the operational tempo and density of Allied strikes to the benefit of German forces. The need to use bomber bases in the United Kingdom meant that Allied bomber routes and targets were fairly predictable, and their time en route allowed the Luftwaffe to focus its defenses against them. The Allies simply could not attack with enough sustained concentration and mass to prevent the Germans from adapting to them. The lack of sufficient Allied bombers and bomber crews contributed to this dynamic. The following points summarize major factors that extended 8th Air Force Bomber Command's OODA cycle.

- *Observations:* Allied air forces lacked the ability to conduct persistent and real-time ISR;
- *Orientation:* Processing images from reconnaissance aircraft took time and occurred well outside the immediate area of operations;
- *Decisions*: Occurred at higher headquarters located far from the combat zone; and
- *Action:* Bombing missions had to fly long distances to and from their target areas, driving more time into the cycle.

Today, the proliferation of persistent sensors across the wartime environment, combined with information networks and data links to share high-fidelity, weapons-quality data across platforms, has transformed OODA cycle execution. Instead of being sequential and linear, today's OODA cycles and kill chains are far more integrated (see Figure 6).

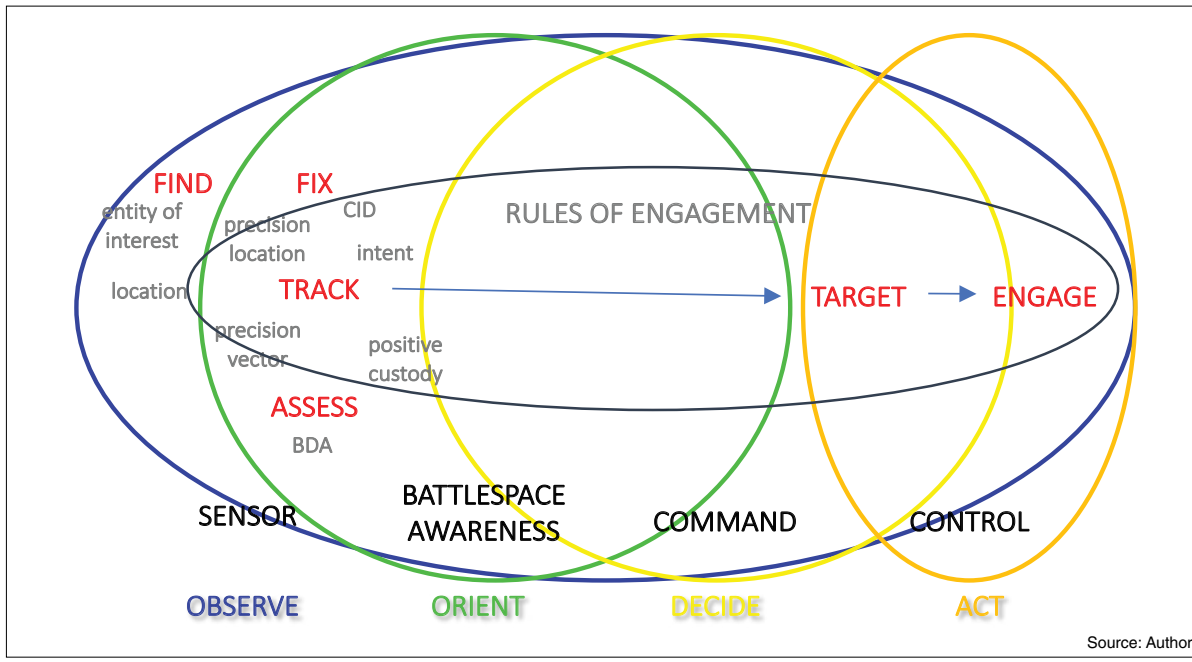


Figure 6. Venn Diagram of Kill Chain Functionalities in Boyd's OODA Loop[95]

For instance, long-endurance MQ-1 Predator remotely piloted aircraft equipped with full-motion imaging sensors and data links helped create kill chains for counter-terror operations in Afghanistan and Iraq that

were not sequential. The power inherent in this integrated sensor-shooter approach was recognized and led to the rapid fielding of sensor pods on nearly all U.S. combat aircraft.

The challenge for U.S. military officials today is to create a force design that will take maximum advantage of this new OODA ecosystem. Such a force design must align the operational architectures, information architectures, and command and control in order to maximize the effectiveness of the force and create a speed that denies the adversary the ability to predict or adapt.

A Mosaic Operational Concept

The first step toward creating a new force design for the U.S. military is to define a concept that will align its forces to support a systems warfare strategy. Although information networks make disaggregated systems warfare possible, mosaic is more than just an information architecture. Mosaic offers a comprehensive model for systems warfare that encompasses requirements and acquisition processes; the creation of operational concepts, tactics, techniques, and procedures; and force presentations and force-allocation action, in addition to combat operations. Mosaic is *not* simply about quickly closing kill chains. The attributes of a mosaic force design can help increase the speed of action across the U.S. military enterprise, whether it is quickly responding to urgent new requirements, integrating innovative and out-of-cycle capabilities, or operational planning. The guiding principles and technologies that underpin a mosaic force design will help enable the United States to prevail in long-term competitions with great power adversaries.

Mosaic warfare is based on the ability to seamlessly share information across operational areas when and where needed as a result of advancements in processing, computing, and networking. Functional capabilities, such as radar, fire control, and missiles, that once had to be hosted on a common platform like a combat aircraft can now be disaggregated into their smallest practical elements. Platforms in the zone of operations would be functionally and physically decomposed into a networked kill web—not a linear and monolithic kill chain.

Mosaic Empowers the Combat Edge

Fifth-generation aircraft have proven the value of pushing *orientation, decision*, closer to *action* at the forward edges of combat. Advances in processing power, algorithms, and data links have made these aircraft incredibly valuable battle managers in contested and dynamic environments. Historical case studies have shown that *orientation* must be located where there is processing capacity to filter, correlate, and fuse those observations into meaning, or *orientation*. Furthermore, the closer both *orientation* and *decision* nodes are to the point of *action*, the faster and more effective are the outcomes.

Mosaic's disaggregated elements or nodes are based on the OODA loop construct. There are observation nodes, orientation nodes, decision nodes, and action nodes. Functionality across the OODA loop is enabled by advanced data links. Observation nodes collaborate to cross-cue each other and provide multi-phenomenal observations to orientation nodes, which then create a picture of the operational area. Based on this orientation, decision nodes activate multiple, simultaneous kill paths to create desired effects on a designated target. These kill paths can remain active until effects are achieved, at which point designated action nodes flex to alternate targets.

Although orientation and decision nodes in a mosaic force concept are layered throughout the area of operation, the most-active nodes are at the forward edge (see Figure 7). Posturing orientation and C2 capabilities with appropriate processing power closer to the edge of the combat zone can increase the speed and accuracy of actions.

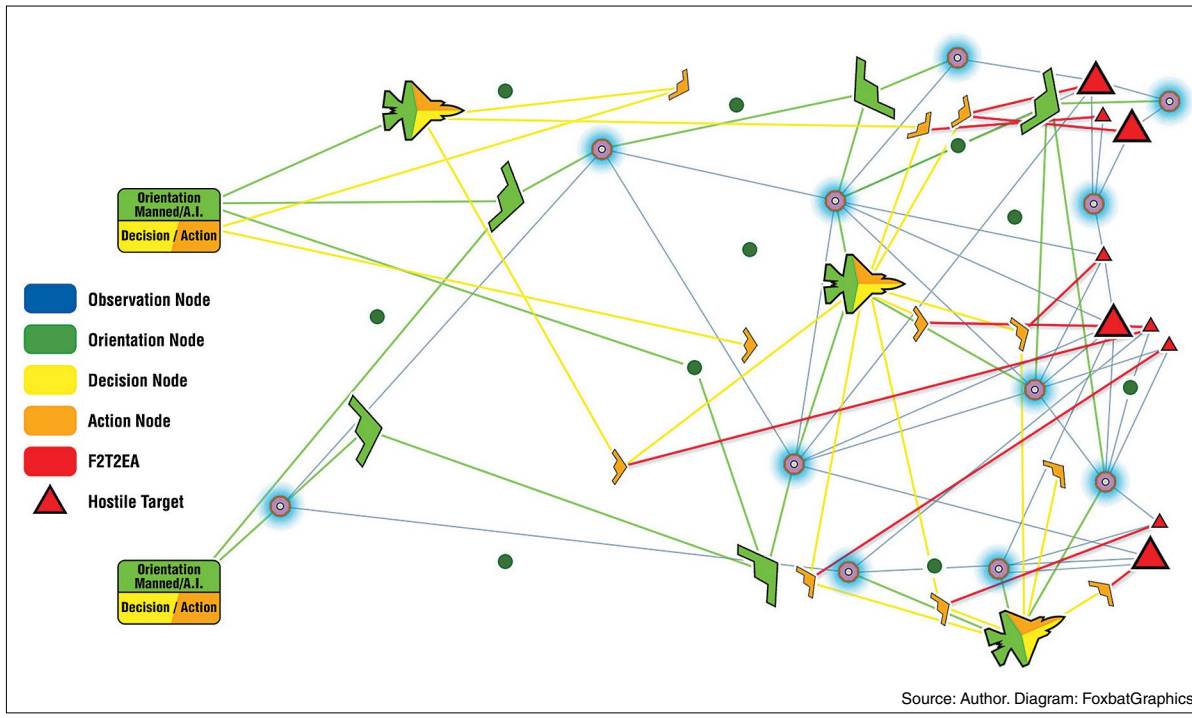


Figure 7. A highly simplified, static representation of a notional mosaic operational architecture. The "aircraft" in this diagram do not represent actual aircraft, fielded or otherwise. They are merely symbols depicting notional airplanes in a combat zone. The most significant symbols in the diagram are the colors that represent the OODA nodes and the notional and selective "data link" connections that characterize the simultaneous and multiple kill paths.[96]

Functional Decomposition and Mosaic. Functional decomposition is a methodology that reduces operations down to their practical functional and technological pieces to illuminate how the elements work together. It is more than tracing information paths—it also makes explicit the relationships between *ways* and *means* and creates insight on how to structure future information architectures to execute effective combat operations.

Functional decomposition analysis of combat operations is what sets mosaic warfare apart from "systems of systems" approaches. Before advanced data links, multiple functions had to be aggregated on single platforms in order to leverage information best across sensors and systems. For instance, a radar, fire-control computer, and an air-to-air missile all had to be integrated in a single fighter aircraft to detect a threat, make sense of the contact information, and then turn that data into information the missile could use to track and guide to the target. Mosaic seeks to make functional OODA nodes interoperable, compatible, and nearly interchangeable.

Increasing Force Resiliency. Creating large numbers of redundant functional nodes across a network will also dramatically increase the resiliency of information flows and kill paths. Rather than hardening information pathways, mosaic warfare suggests a type of network architecture that, by design, can resiliently

absorb information and information-pathway attrition. Even with combat losses in a contested area of operations, a mosaic kill web confers a substantial advantage due to its resilient multi-axis sensing, network maneuver, and ability to create off-axis effects underpinned by information sharing and processing at the combat edge. There are no critical nodes, no key high-value airborne assets, or no essential platforms that will lead to mission failures if lost. This disaggregation and edge-processing will ensure operations continue to be effective even when forces are no longer in contact with higher headquarters or other mission force-structure elements.

Artificial Intelligence/Machine Learning (AI/ML) and Mosaic. A mosaic force design moves beyond tightly coupled, cross-cued, and distributed-but-linear kill chains to create simultaneous, multi-path kill webs with multiple effect providers. With many possible kill paths running concurrently, it becomes necessary to orchestrate the mosaic composition. Command and control should be modular, hierarchical, and abstracted between layers of a mosaic force; it cannot be centralized as it has for the last 30 years. Placing decision nodes at the forward edge of the combat zone will be key to creating a resilient force. If an adversary attempts to isolate elements of a mosaic force operating in some areas of a combat zone, the mosaic force's orientation nodes and empowered decision nodes will ensure it continues operations in accordance with command intent.

Placing decision nodes at the forward edge of the combat zone will be key to creating a resilient force.

The need for increased speed of action in an area of operations means that orientation should be accomplished by AI/ML systems or by AI/ML providing decision aides to human battle managers. At a mosaic warfare workshop that Mitchell Institute led in July 2019, Air Force operators, science and technology thought leaders, and Office of the Secretary of Defense officials agreed that humans must continue to play a significant role in a mosaic operational concept. Humans bring the art of war to the combat zone, using their ingenuity and creativity to accomplish actions in ways that are unpredictable and create operational problems that are far-more difficult for adversaries to solve. One technologist at the workshop cited how the decentralized execution of some Allied operations in World War II caused German commanders to perceive them as chaotic, disorganized, unpredictable, and, therefore, difficult to counter.[97] Participants also noted that humans handle ambiguity and uncertainty well, improvising and taking action even when the best course is not entirely clear.[98]

In summary, a mosaic force design does more than accelerate OODA functions and architectures. Because of the informatized, high tempo, and lethal nature of system confrontation warfare, deconstructed elements of command and control must also be built into the architecture at the forward edge. This is distinctly different from having commanders in a combined air operations center (CAOC) reach into the cockpit. Rather, decomposed C2 elements facilitate self-coordinated execution and resiliency in a more rigorous and unpredictable (to the adversary) manner. Systems warfare requires a force design that organizes and energizes action nodes and kill webs that come from different domains, are geographically co-located, or are from the other side of the globe.

A Mosaic Force Design for Information Age Systems Warfare

The previous analysis should provide a clear assessment of the vulnerabilities of the U.S. military's present force design. The United States' current way of war will not successfully compete against a systems warfare strategy and it cannot scale appropriately across the range of other military commitments. Mosaic is a force design that combines the attributes of highly capable systems with the volume and agility afforded by smaller force elements that can be rearranged into many different configurations or presentations. A mosaic force builds upon current investment in important, highly capable systems to yield smaller, more numerous, disaggregated elements. Similar to tiny, fractured color tiles of mosaic artwork, these disaggregated elements may network together to create a coherent operational system in partnership with highly capable system platforms.

The United States' current way of war will not successfully compete against a systems warfare strategy and it cannot scale appropriately across the range of other military commitments. Mosaic is a force design that combines the attributes of highly capable systems with the volume and agility afforded by smaller force elements that can be rearranged into many different configurations or presentations.

Using a resilient information architecture, a fully mature mosaic force design composes these specialized capabilities and effectors in combination with other platforms at the combat edge. Highly integrated aircraft like the F-35 or B-21 can add their functionality to the larger mosaic without the need to distract their aircrew from primary operational duties. The many sensors on these aircraft could be "virtually disaggregated" to become nodes in the mosaic to the extent that their disaggregation does not degrade their own performance. Virtually disaggregating highly capable systems to participate in the mosaic would enhance the mosaic system as a whole. Advanced processing, computing, and information networks and data links will allow DOD to tactically distribute single-purpose or single-function elements in partnership with higher end, highly capable systems, and then quickly recompose their capabilities through networks to achieve synergistic effects in areas of operation.

Mosaic as a Force Design Adaptively Connects Means and Ways to Achieve Necessary Ends

Grounded in information age systems warfare, mosaic leverages networks and data links to move information across a dynamic, disaggregated system. Because of the disaggregated nature of a mosaic force structure, different pieces may be integrated and tailored specifically for the needs of an operation. Mosaic can adapt and scale across the spectrum of military operations, from high-end war to surgical strikes, humanitarian responses, or long-duration, low-intensity conflict.

Mosaic assets can be managed in time frames that are organic to those platforms and quickly adapted to meet the needs of military personnel in a highly dynamic combat environment. Multiple and simultaneous ways and means are continuously constructed and made available to the forward edge of the zone to create many possible kill paths to close desired effects. A mosaic force design can significantly shorten planning cycles and provide commanders with more creative and surprising ways and means to achieve their strategic objective. This also disrupts and injects uncertainty in an adversary's operational planning.

Mosaic as a Force Design Reduces Vulnerabilities

Systems warfare strategies target data links and their nodes to collapse the effectiveness of a system. In a truly mosaic force, there are no single points of failure, no single data link, no universal standard, no one type of waveform on which enemies can concentrate. This is the point of functional decomposition. The key to the mosaic force design is the quantity and the composition of the nodes it can create in an area of operation. Disaggregated elements contribute to system resiliency, because their loss represents the loss of only one function and not the many functions of a highly capable, traditional platform. Networked together, disaggregated elements can create out-sized value to U.S. forces. The larger system functionality continues even when attrition occurs, since there is no single node or small set of nodes whose loss will collapse the entire system. Disaggregation also expands the number of potential kill paths, posing a targeting conundrum to an adversary.[99]

Mosaic as a Force Design Speeds Acquisition and Reduces Predictability

A mosaic force design could help accelerate the development and fielding of new capabilities. The time and cost required for a military to develop and field new technologies are as critical to long-term great power competitions as actual combat. Integrating highly complex systems drives much of the time and cost into DOD's acquisition programs. Shifting toward acquiring disaggregated elements that can be modularly combined—whether on a shared platform or networked in the architecture—should reduce their integration challenges, testing requirements, and possibly their SWAP-C requirements. DOD's current acquisition system can achieve this, reducing the need to maintain multiple specialized offices that are designed to "work around" the Pentagon's bureaucratic morass. It could also help create a more robust defense industrial base.

All of this translates directly to accelerating the development and fielding of new technologies at a pace and possibly a cost that competitors cannot match. Incrementally migrating the current force to a system of disaggregated capabilities is an approach that could finally achieve the goals that many of DOD's previous attempts at acquisition reform have sought.

Dispelling Myths About Mosaic Warfare

To this point, this study has presented a broad summary of principles that guide a mosaic force design. The following bullets are meant to dispel misperceptions about the mosaic warfare concept. Although

mosaic warfare is premised upon and enabled by advanced information networks, processing, automation, and AI/ML, it is far more than just an information architecture. Mosaic, as a force design construct, is a comprehensive systems warfare model that encompasses operational concepts, planning, force structure, force presentation, force allocation, doctrine, command and control, and tactics, techniques, and procedures.

- **Myth: Mosaic is an entity with a hard delivery date and budget line like any other program of record.** As a force design, mosaic provides guiding principles for developing operational concepts and future technologies, conducting operational planning, presenting forces, and commanding and controlling them in real-world operations. It should be expected that elements of a mosaic force will mature at different paces, resulting in their gradual integration into the force instead of creating a sudden, sweeping force transformation. Broadly speaking, a mosaic force design concept will encourage the development of new, highly interoperable capabilities designed to speed through the acquisition system.

> ...a mosaic force is less about "what" a new system is and more about how it will behave within a broader enterprise.

- **Myth: Mosaic will replace current platforms with swarms of expendables.** In many ways, a mosaic force is less about "what" a new system is and more about how it will behave within a broader enterprise. Swarms of expendable systems may be a design element of a future mosaic force design, as will other weapon systems and concepts. Mosaic seeks to create a heterogenous mix of many different types of elements, functions, and capabilities that can collaborate in unexpected ways to complicate an adversary's planning and targeting. High-end, highly capable platforms will continue to provide great value in future areas of operation, and it is unrealistic and imprudent to divest them arbitrarily. As mosaic force elements are fielded, they will change how highly capable platforms are employed, further enhancing their value and effectiveness.

- **Myth: Mosaic will impose a single architecture or standard on the force.** The notion of creating a single architecture or standard is antithetical to the diversity, complexity, and resilience that define a mosaic force design. Imposing a unitary requirement on every platform in a combat zone would be costly, could result in the procurement of systems that are quickly obsolete, and could help competitors to understand and adapt to new systems quickly. Mosaic will require systems to be interoperable, but one can achieve this in ways that do not require a single standard. Using many different types of data links, waveforms, message formats, and other phenomena will increase the resiliency of U.S. networks.

- **Myth: Mosaic is an interdependent portfolio of programs.** Mosaic is not a tightly integrated system of systems where the failure of one system could impede the development of others or collapse the whole architecture. Operations of a system of systems are dependent on extremely rigid rules, roles, and responsibilities. Mosaic seeks to construct a system-wide federation of interoperable platforms, capabilities, and enablers that have stand-alone value, can collaborate in a synergistic manner, and can remain operationally effective while absorbing failures and losses. As a loosely coupled system, a mosaic force design can quickly assimilate and use new capabilities as they mature.

- **Myth: A mosaic force design will require everything in a network to be connected all of the time.** Advanced information networks enable a mosaic force design; it does not seek to connect all things all of the time. The interdependence of mosaic capabilities means they must have the ability to connect in a highly automated manner when needed. The distribution of too much data to too many entities in a network can slow its operations, since each entity will need to filter massive amounts of information to determine what is necessary. Sometimes less is more. Getting the right information to the right entity when needed does not require constant connectivity. What a mosaic network *does* require is information processing at the combat edge. This will require smart aides and routers to identify data that specific entities need and the best path to pass the information to them.

- **Myth: Mosaic relies on geographically distant cloud services for processing and information "pulls."** Mosaic does not reach back to pull information from a server farm. Relying on rear-area processing can create risk that actors in a combat zone will not get the information they need. The physical distances involved also induce latency into the system that can mean the difference between mission success and failure. Increased computational power and faster processing speeds will allow the development of processing nodes that can be placed at the forward edge of an area of operation to push information to mosaic entities.

Likely Challenges to the Creation of a Mosaic Force Design

Breaking with the past. Transitioning America's military to a mosaic force design will not be easy. Creating it will require the services to break with old, well-ingrained approaches to waging war, including the tight, centralized command, control, communications, and execution practices that have become habituated since the September 2001 terror attacks on the United States. Changing training practices to ensure battle management officers are able to make decisions at the combat edge will be essential to mosaic warfare. DOD will also need to break with its current notions of cyber security. A mosaic force is not hardened in the traditional "moat-and-castle" approach to which DOD subscribes. The United States cannot win systems warfare in the information age with a single or even small handful of network or nodal entry points. Such an architecture would impose time into operations, expanding the OODA loop and conceding an important advantage to any adversary. A mosaic architecture, by definition, has numerous nodes and networks, dramatically expanding the potential surface attack area for a cyber threat. U.S. industry has been successfully safeguarding information on "zero-trust" networks for years, and there likely are other, more innovative ways to evaluate, filter, or even quarantine corrupted nodes and networks.

The United States cannot win systems warfare in the information age with a single or even small handful of network or nodal entry points.

Increasing the ability to adapt. While the mosaic is not a mesh-type network, its functional architecture will be quite complex and include many potential pathways; nodes with the capability to automatically discover, connect, and identify the information needs of other mosaic elements; the ability to adapt when elements are degraded or denied; and the ability to integrate new capabilities automatically. There will be

no single network or standard to govern the mosaic architecture that could constrain the incorporation of emerging technologies and lock it into technological obsolescence. Developing the ability to translate data, transform waveforms or other types of links, and integrate new nodes in real time without major gateway nodes will be essential to creating an adaptive mosaic force design. This will not be a small task.

Developing automation and artificial intelligence. Automation and artificial intelligence/machine learning aides are essential to creating a mosaic force that can rapidly adapt and execute its functions. These software aides will be embedded in every platform and optimized for their function. Identifying the many combat functions of elements of a mosaic force design, developing the right algorithms, and training the algorithms will be critical to the success of a force design.

Dealing with increased complexity. A complex architecture is not the only challenge a mosaic force poses. Building a large, diverse force of disaggregated elements will create concerns over their sustainment and life-cycle costs. Diversity in platforms implies diversity in spares, equipment, training, and other operational expenses. However, many mosaic elements will be smaller than large multifunctional platforms, and their physical and functional systems may be less complex, easier to diagnose, and easier to repair. The military logistics community and DOD's industry partners will need to assess and develop new ways to sustain a large, heterogeneous force affordably.

Automation and artificial intelligence/machine learning aides are essential to creating a mosaic force that can rapidly adapt and execute its functions.

More in-depth assessments are necessary. DOD will need to conduct assessments that take a hard, critical look at assumptions that underlie its current force design and compare its effectiveness and affordability with a mosaic force design. The evolving military strategies of America's great power competitors must inform these analyses rather than what has worked for the United States against lesser adversaries of the past. In short, further analysis must be done on which future force design will be in the best interest of the nation. In particular, analysis should address if the disaggregated elements take the form of an entire independently operable platform like an aircraft or spacecraft, or if they are more suited as sub-elements of such platforms that make up the modular pieces (e.g., power, processing, propulsion, sensing, weapons, communications) that can be combined to create platforms to achieve different effects. Or, is mosaic some mix of both?

In summary, the strategic, operational, and tactical advantages that a mosaic force design promises far outweigh the challenges that creating and sustaining it present. Compared to the U.S. military's current force design, a mosaic force may better withstand a systems confrontation with China and other adversaries. Its ability to adapt and create unpredictable, resilient force compositions poses the potential to create perplexing problems for the nation's enemies. Mosaic's disaggregated and networked nature means that it will also be scalable to low-end conflicts without wasting excess capabilities or capacity. A mosaic force design has the potential to restore speed to U.S. military OODA loops at every scale of war.

A Practical Course to a Mosaic Force Design

To some, a mosaic force design might seem more like science fiction, or an overly ambitious and impossible twist on "DARPA-hard" research efforts. However, a number of mosaic building-block technologies have already been demonstrated, and the Air Force and other services have several programs of record and initiatives that are closely aligned with core mosaic principles. Information and sharing information seem obvious to everyone, as does leveraging advanced processing, automation, and the growth of artificial intelligence and machine learning.

The Air Force, for example, has started fielding its common mission control centers (CMCCs); the first of them is located at Beale Air Force Base in California. Designed to replace the legacy control and reporting center (CRC) function with the Theater Air Control System (TACS), the CMCC will "manage C2 productivity, shorten the task execution chain, and reduce human-intensive communications."[100] During CMCC's "walk" and "run" development phases, the system demonstrated the "ability to dynamically re-plan assets based on enhanced awareness of the battlespace" to include directing and managing a number of live aircraft.[101] One early demonstration showed the ability of CMCC to task an RQ-4 Global Hawk remotely piloted aircraft dynamically using an emerging universal C2 data standard that enables interoperability across weapon systems.

Similarly, the Air Force's future Advanced Battle Management System (ABMS) will fuse information from hundreds of space and air assets—current and emerging systems—"seamlessly in real time across a fast-changing, dispersed combat area of operations."[102] Described as a system of systems, ABMS will integrate "battlefield surveillance information and provid[e] commanders better situational awareness in combat," states an Air Force press release.[103]

These programs and initiatives use artificial intelligence algorithms to marry information from disparate sources to create a coherent picture of an area of operation.

What both CMCC and ABMS demonstrate is the ability to collect, filter, and fuse information feeds from diverse platforms. These programs and initiatives use artificial intelligence algorithms to marry information from disparate sources to create a coherent picture of an area of operation. Dynamically re-tasking an RQ-4 using CMCC is based upon the ability to share and process machine-to-machine data sets from many sources.

There are many technologies and concepts within both these programs that are congruent with mosaic design principles and attributes, and both are demonstrating some of the capabilities a mosaic force will need for implementation. The challenge here is that while both programs have developed promising technologies, they still represent a tightly coupled system of systems and a static, universal standard. It should be clear from the previous analysis that such an approach is not compatible with leveraging the most-advanced technologies or rapidly integrating new capabilities. Moreover, both of these programs characterize highly centralized constructs—all of which will extend the OODA loop of U.S. forces.

DARPA, the Pentagon's development shop for breakthrough technology, is also pursuing the technologies needed to make mosaic a reality. Adapting Cross-Domain Kill-Webs (ACK), for example, will assist decision nodes with "rapidly identifying and selecting options for tasking and re-tasking assets within and across organizational boundaries," states the agency's website.[104] DARPA's Distributed Battle Management (DBM) program is focused on creating automated decision aides at the combat zone.[105] These are a small sampling of DARPA research areas that are focused on the details of how to enable a mosaic force and move and manage information in a mosaic kill web.

DARPA's progress toward defining key areas for further research is just as important as its successes. For example, DARPA has embraced the on-demand, mission-responsive Dynamic Network Adaptation for Mission Optimization (DyNAMO) program, which is currently "developing and testing technologies that enable … networking among diverse airborne platforms in contested environments," according to the agency's website.[106] However, DyNAMO is pre-programmed based on planning assumptions and cannot yet adapt to changed environmental conditions.

Likewise, DARPA's Resilient Synchronized Planning and Assessment for the Contested Environment (RSPACE) program seeks to address the highly centralized and slow pace of current command and control of air operations. Intended to enable distributed planning and resilient operations in the face of disrupted and uncertain communications, RSPACE has identified additional important areas of research, such as scalable automated planning, distributed coordination, and human-centered automation.[107]

Such mosaic related projects offer insight regardless of their outcome. In many cases, associated research is quite valuable, even if the entire program is not adopted. Identifying what may not work, what limitations exist within particular approaches, and identifying areas for further research, will help foster technology development on which a mosaic force will depend. To that end, most of the projects that DARPA pursues are well targeted and demonstrate valuable progress in developing and maturing necessary mosaic enablers.

A critical consideration for any of these research, development, and new programming efforts is how they advance DOD's future force structure and capabilities in a coherent force design that can compete in systems warfare.

A critical consideration for any of these research, development, and new programming efforts is how they advance DOD's future force structure and capabilities in a coherent force design that can compete in systems warfare. All too often, despite the diligence, intelligence, and hard work of requirements officers and other involved in the process, new capabilities are developed in a "stove-piped" manner—meaning done without consideration for how they will integrate and fit with other systems—and do not help create the system synergies of a mosaic force design.

DOD's current processes are not wholly without context or value; current capability-gap assessments and analyses of alternatives take threats, technologies, and even potential new tactics or other non-materiel solutions into consideration.[108] The Pentagon's Joint Capabilities Integration and Development System

(JCIDS), although bureaucratically bloated and cumbersome, does help the services identify, refine, and procure the means they need to execute their missions.

However, DOD currently does not have an overarching theory of design that truly describes how it will integrate all its force components together to fight, particularly not for peer conflict. The mosaic warfare concept provides that. As a warfare concept, the mosaic force design furnishes the connective tissue of interoperability, orientation aides, decision aides, and information routing that enables diverse combat elements to work together as a system, including current U.S. forces.

Mosaic Technological Enablers

Prioritizing the development of key mosaic enabling technology is essential to transforming the U.S. military force. These technologies will allow legacy platforms and programs anywhere in the acquisition process to begin operating in a mosaic manner. By focusing on these enabling technologies, the United States hedges its risk with its current force structure, and as DOD fields mosaic enablers, it will dramatically increase the effectiveness of the U.S. military's legacy systems.

Mosaic enabling technology falls into two broad categories: technologies needed to build, plan, and compose a mosaic force; and technologies needed to execute mosaic operations. DOD must pursue both in parallel; it makes little sense to focus on a mosaic force composition if one does not have the execution enablers in place. This is not to say that enablers are so tightly coupled that they must be fielded simultaneously. Mosaic is not like past "system of systems" concepts. Many of these enablers provide value even without the others, but maximum value will come with the fielding of more enablers.

Mosaic enabling technology falls into two broad categories: technologies needed to build, plan, and compose a mosaic force; and technologies needed to execute mosaic operations. DOD must pursue both in parallel...

Today, the service components manually plan their operations. Operational planners take existing plans, dubbed OPLANs, and modify them, using them as templates to determine what forces and logistics are necessary to deliver capabilities that combatant commanders request. Force packages for each OPLAN are already set by other planners who have taken years to validate that force composition against the scenario and threat. This mission planning is essentially where a force architecture is developed, with some modifications specifically tailored to the immediate need. The challenge is that the number of options available to planners is limited to the existing as-built capability. Any machine-to-machine connectivity that does not already exist is a lost opportunity, and supporting tactics and doctrine are relatively set. The years involved in developing the OPLAN and the many months and people it takes to modify it for an operation mean that the U.S. military's current force design, operational architecture, and information networks require a tremendous amount of warning and preparation. Ultimately, this long and predictable planning cycle gives the adversary the advantage of foreknowledge and time.

Mosaic, on the other hand, is designed to accelerate this planning and force-composition cycle. With automated and intelligent mosaic planning and composition tools, commanders will be able to accelerate their OPLAN OODA loop. The modular way in which planners build their time-phased force deployment data (TPFDD) for a plan is already mosaic in nature. Planners select unit type codes (UTCs), which are "blocks" of capabilities, such as a single intelligence analyst or a six-ship group of F-16s, that are each coded for the logistics, technicians, pilots, and other elements needed to support it. Seamless interoperability and information networks will allow a mosaic system to create a wholly unique plan rapidly and compose a force in unpredictable ways. This force will present a system that surprises an enemy, creates effects that it cannot anticipate, and confounds its ability to target U.S. forces. Thus, mosaic enablers will include technologies that create interoperability across an area of operations: adaptive and resilient, as-needed networks, functionality from the edge of combat, operational planning aides, and enablers that can rapidly recommend force compositions.

In a system confrontation, centralized command and control, or even centralized *orientation* processing will not provide the speed, responsiveness, or unpredictability that U.S. operators need.

Operational Evolution Towards Mosaic

Information networks and data links will be the foundation of a system that functionally disaggregates future operations. The Air Force has a long history of operating in a networked, functionally disaggregated manner. An early example of sharing information across entities to construct more-effective and more-responsive kill chains are the balloon observers of World War I. Observers in a tethered balloon would find, fix, and track the enemy with binoculars and then use a telephone wire to relay targeting information to artillery batteries. The balloon observer would then assess the artillery's fires and provide corrections to the team. This is an early example of how functions could be composed to create a more effective kill chain.

Today, airmen use the power of data links, full-motion video feeds, and voice radios to share the functional information elements across the kill chain. In a notional example, an E-8 JSTARS ground-surveillance aircraft might detect a moving target and cue an F-16 to investigate. This F-16 might share the location of a potential target with his wingman while simultaneously sending video to a joint terminal attack controller, who coordinates air strikes from a forward position on the ground, and to the CAOC to receive clearance for a weapons release. The F-16 pilot then releases a laser-guided bomb that his wingman lases to ensure precision.

Although the systems used for this example of a precision attack are enabled by networks and shared information, they still represent fairly linear kill chains that are reliant on centralized command and control. In a system confrontation, centralized command and control, or even centralized *orientation* processing will not provide the speed, responsiveness, or unpredictability that U.S. operators need. Technological enablers, organized around the combat tasks of the OODA loop/kill chain, as described previously in this study, will be critical to moving beyond rigid networks, tactics, and vulnerable platforms/nodes of today's force design.

While information networks and data links will create the foundation of a system that functionally disaggregates operations, data links alone will be insufficient. Sensors will need to learn how to collaborate together, cross-cueing their observations machine-to-machine to create multi-static and multi-phenomena looks at entities or activities or interests. These observer nodes may pre-process their information prior to passing their data to orientation nodes. Again, this information flow will be machine-to-machine, and update rates and orientation nodes may change as needed, depending on feedback from the orientation nodes.

Orientation nodes may have several layers of associated nodes with different purposes, and some orientation nodes may be paired with human actors who also are decision nodes and further supported by decision aides that may also have several layers of functionality. Determining the available and best priority effects, identifying potential actors, routing multiple and simultaneous kill paths to multiple actors to ensure effects are delivered, and then re-tasking those actors will all be key functions in a mosaic system. As new functionalities and capabilities are fielded, these mosaic enablers must be able to add that value rapidly and without any "stutter."

As the force becomes more interoperable and as more mosaic enablers are built in, architectures will be less purpose-built focused and far more universal and adaptive.

To make this a reality, mosaic technological enablers will require varying levels of automation and AI/ML. Some elements, like orientation nodes, will require significant experimentation, refinement, and training iterations. Data collection presents a challenge to overcome, as does deciding how to train the AI/ML elements of mosaic functionality. Doing so, however, will be key to developing a mosaic system that is resilient, adaptive, and confounds future enemies.

This transformation will take time to achieve, and the U.S. military needs to begin operating as a system now. Developing and fielding a system of systems is difficult. They are often unwieldy, brittle, and could fail if one or more critical elements falters or is attrited. The value of a mosaic planner and controller is that until a fully mosaic force is achieved, a system architecture can be purpose-built for that force and for a mission. Information architectures can be simplified because the network is focused on one campaign, operation, or even mission and can focus on the composition, functions, and platforms of a particular need. As the force becomes more interoperable and as more mosaic enablers are built in, architectures will be less purpose-built focused and far more universal and adaptive.

Weapon Systems and Functionality in a Mosaic Force Design

Transforming the U.S. military to a mosaic design is no small task and will take time. Retaining legacy platforms will be crucial to hedging against risk and ensuring the military can continue to provide for the nation's security. As mosaic enablers are matured and fielded, legacy platforms may experience a renaissance of relevance. This cannot distract from the need to field disaggregated combat elements. The demands of peer conflict also necessitate quantity as well as quality. Highly capable, multifunction platforms may not be able to deliver both if recent small buy history becomes the norm.

The United States is not procuring highly capable weapon systems that characterize higher end U.S. capabilities in the rapidly increased quantities necessary to meet the demands of the *2018 National Defense Strategy*. These platforms are impressive and incredibly capable, pushing the boundaries of technology. DOD must remain committed to these programs of record—and even increase their quantity—while it also begins to field more-affordable platforms, in order to scale.

Affordability does not mean pursuing an "80 percent solution," and it certainly does not mean "new-old," like the new purchase of old fourth-generation aircraft. While mosaic operations are designed to accept attrition, it is not the goal to send non-survivable platforms into contested areas of combat. Instead, affordability is achieved through disaggregating capabilities from one platform into many.

Much of the time and cost that is driven into today's advanced aircraft has to do with the many layers of highly capable sensors, weapons integration, stealth management, and processing to manage all those elements—all incorporated into one vertically integrated program. There were many good reasons to aggregate as many cutting-edge capabilities on one platform as possible, the most important of which was to take full advantage of information. But the development of advanced networks and data links means that the United States no longer is limited to fusing information on a single platform. The U.S. military can achieve the benefits and synergies of information fusion across disaggregated platforms through networks and mosaic enablers.

The U.S. military can achieve the benefits and synergies of information fusion across disaggregated platforms through networks and mosaic enablers.

Disaggregating force elements to single functions has the potential to combine them in many different ways, enabling a reduction in an individual platform's physical size; sensor/systems integration challenges; number of test points, reporting, and reviews needed to prove its effectiveness; and, importantly, unit cost. Much of the cost and complexity of current acquisition programs stems from managing the integration of their many complex systems. This point is crucial, because the ability to speed new capabilities to the field is just as critical to long-term great power competitions as preparing for actual combat. A mosaic force design will help achieve this objective.

A mosaic force design disaggregates battlespace functions, enabling the potential use of platforms tailored by mosaic force elements networked together to achieve synergistic effects. It can also make it possible for DOD to field new capabilities at a rate that adversaries cannot anticipate or match. Even under the Pentagon's current acquisition system, it will help it to field new capabilities at a rapid pace. Furthermore, the diversity of functionality results in a more robust industrial base and an influx of new platforms. By incrementally augmenting and then migrating the current force to a system of mixed and disaggregated capabilities, such a shift in platform paradigms would have revolutionary consequences on the effectiveness of the U.S. military as a system, and the modernization cycle competition between the United States and its adversaries.

Conclusion

The resurgence of great power competition—specifically, the systems confrontation warfare posed by China and future adversaries—presents a clear challenge to the current U.S. force design. This challenge involves more than surmounting A2/AD threats. Should DOD choose to continue a traditional practice of linear competition, critical operational elements upon which U.S. forces depend will be exposed to the targeting strategy of systems warfare. This involves the destruction of key nodes and networks whose incapacitation will blind and paralyze U.S. forces. At the same time, DOD cannot ignore lesser threats to America's security interests. Any force design it adopts must be flexible and scaled to a broad range of threats. This is especially true given the prolonged life span of many weapons systems, the unpredictable nature of the threat environment, and role of aerospace power as one of the most agile and rapidly responsive tools to ensure the nation's security. The concurrency of these threats—from the high end to low end—is placing extreme stress on an American military that is now too small, too old, and has too few high-end capabilities.

As DOD creates a force design better suited to an era of great power competition and confrontation, it should also address its acquisition system and other processes that present organizational, bureaucratic, and statutory obstacles to regaining a strategic and military advantage. Despite many previous efforts focused on acquisition reform, the time required to develop and field new capabilities can still take decades. This is not fast enough to surprise adversaries and counter emerging threats.

This study proposes a force design that addresses these challenges in an era of growing risk to U.S. global interests: mosaic warfare. "Mosaic" reflects how smaller force structure elements can be rearranged into many different configurations or force presentations by exploiting information networks to create a highly disaggregated, resilient kill web. This approach offers an operational concept, framework, and the technological enablers necessary to implement the *2018 National Defense Strategy*, while also addressing challenges that will impact U.S. security interests for decades into the future.

Should DOD choose to continue a traditional practice of linear competition, critical operational elements upon which U.S. forces depend will be exposed to the targeting strategy of systems warfare.

Implementing the Mosaic Transformation

Implementing a mosaic force design will challenge established doctrine, programs, bureaucratic fiefdoms, and traditions. Nonetheless, there are already examples of technologies and emerging operational concepts that point to the feasibility of a mosaic force design. A number of mosaic building-block technologies have been demonstrated. The Air Force and other services are pursuing programs of record and other initiatives that closely align with core mosaic principles. Furthermore, mosaic enablers and other elements will enhance the operational value and resiliency of DOD's current and programmed highly capable weapon systems. Mosaic-type operations are nothing new to the Air Force, and in many ways, this is a natural operational concept for the Air Force to pioneer for DOD.

More work, however, is needed to migrate to a mosaic force design. Operational concepts must be explored, tested, and refined. The technological enablers must be identified, developed, and fielded. Force structure sizing, capabilities, and mixes must be validated through operational analysis. This work will provide value to military personnel even through the process of transformation to a mosaic force.

While this study describes mosaic warfare as a force design and explores its feasibility, key areas for development became evident during the supporting assessment. Analyses in the following areas would help add substance to the mosaic force design framework outlined in the study.

- **Aggressively Invest in Developing and Fielding Mosaic Enablers.** DARPA's Adapting Cross-Domain Kill-Webs, Distributed Battle Management, and some of the filtering and fusion processes internal to the Common Mission Control Center and Advanced Battle Management System are early examples of mosaic enablers. DARPA has also identified and is investing in mosaic enablers such as System of Systems Integration Technology and Experimentation (SoSITE), which successfully demonstrated the ability to transmit rich, complex data exchanges across "Non-Enterprise Data Links," meaning different data links without a "gateway" translator.[109] Advanced data links, such as machine-learning radio frequencies and laser-based data links, are early emerging technologies fundamental to a mosaic force. Other high-potential technology research is underway, and the Air Force should partner more closely with DARPA to assess the potential operational advantages of these technologies and transition leading projects into programs of record.

- **Experiment with Mosaic Operational Concepts, Architectures, and Empowered Command and Control at the Edge**. A full alignment of information and command-and-control architectures with an operational concept is crucial to any force design. Continuous experimentation with cutting-edge technologies, combined with rigorous operational analysis, is necessary to explore the art of the possible and how to exploit mosaic enabling technologies. These experiments would also help identify other needed technological investments and refine future doctrine and operational architectures.

...the Air Force should partner more closely with DARPA to assess the potential operational advantages of these technologies and transition leading projects into programs of record.

- **Conduct an Operations-Focused Cost Assessment of Force Design Alternatives.** A future U.S. force capable of deterring or, if necessary, prevailing in a high-end systems warfare conflict will require greater capacity compared to the current force. Sufficient capacity (force size) as well as the right mix of capabilities will be critical to achieving the attack density needed to defeat great power aggression and sustain a deterrent posture in other theaters. High-quality wargaming of force design alternatives augmented by operational and cost analyses could help identify the right force size and mix needed to implement the *2018 NDS*.

- **Maintain Commitment to Current Force Structure and Programs of Record.** Mosaic force design will not happen overnight, and the fragility of the current force means that DOD should carefully consider the implications of disrupting high-priority programs in the near term. Legacy aircraft, including those designed in the 1970s, must be replaced with next-generation capabilities as quickly as possible. The acquisition of high-end capabilities, like the F-35 and B-21, should be accelerated to hasten DOD's implementation of the *2018 NDS,* as should the development of disaggregated elements to create a future mosaic force. Analyses are needed to determine how DOD should prioritize its resources to maintain needed capacity and capabilities as it transitions to its future force.

- **Assess and Then Develop Automated Technology That Can Share Information Across Different Security Levels.** This is not a new challenge. While security classifications do protect information, they also focus on guarding sources, means, and methods. Although it is certainly possible to exchange the former without disclosing the latter, this can induce time into networked operations. Rapid exchange of information is especially important at the forward edge of combat, for the value of actual data is often transitory and diminishes as time and circumstance pass. The development of a technological approach to share information automatically and rapidly among diverse users and across multiple classifications and allied nations will be a key to creating the future force.

- **Assess and Formulate Appropriate Policies for Testing, Validation, and Verification of Artificial Intelligence.** Military personnel need confidence in the capabilities they take to war. New capabilities must undergo operational test and evaluation to ensure that the capability meets its specifications, performance requirements, and does not create unseen weaknesses. To this end, systems and concepts are tested meticulously. Platforms that incorporate any kind of artificial intelligence or machine learning will pose a serious challenge to DOD's operational test and evaluation (OT&E) teams. After all, the point of artificially intelligent algorithms is to change their behavior or outputs as a result of numerous data inputs or iterations of exercises. DOD should assess and then formulate policies that will guide the validation of AI/ML in future military applications.

No longer can the U.S. military rely on a defense culture largely conditioned by an atypical era of absolute military dominance, permissive threat environments, and a lack of peer adversaries.

- **Develop Multiple and Complimentary Approaches to Spoof-proofing AI.** Artificially intelligent machines depend on data and iterations. But what happens when their algorithms are fed corrupted data, or receive data intended to deliberately distort their performance? These concerns are not unique to elements in a mosaic force. However, the redundant nodes and multiple layers a mosaic system should allow for this kind of system corruption to be detected and isolated. For example, if one *orientation* node goes bad, others should be able to identify erroneous findings and effectively quarantine it from participating in the system. If an *observation* node continually cross-cues others to non-target, these other nodes should phase out those cues. DOD should assess its need for technological enablers, whether AI/ML, architectural structures, or some other means, capable of providing a robust check and balance across a system.

Leadership in an Age of Great Power Challenge

No leader currently in the American national security enterprise has experience dealing with a sudden rise of great power competitors bent on changing the global status quo. This last happened prior to World War II, when the Axis of dictatorial powers used leading technologies in innovative ways in an attempt to achieve political, cultural, and racial supremacy across Europe and Asia. For the past 30 years, America's defense leadership faced ever-increasing security challenges, but never the possibility of an American defeat that could cause enduring damage to the nation's status, power, or welfare. Since a nation's military backstops the political grand strategy of any great power, the United States must out-adapt adversaries who have and will brilliantly adapt themselves to an obsolescing U.S. force design. Migrating the U.S. military to a more effective force design, even as new capabilities integrate into the force, will help achieve this objective. No longer can the U.S. military rely on a defense culture largely conditioned by an atypical era of absolute military dominance, permissive threat environments, and a lack of peer adversaries. It must swiftly transition to a new way of warfare: the mosaic force design. ✪

Endnotes

1 Eric Edelman and Gary Roughead (co-chairs), *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: United States Institute of Peace, 2018), 14, https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf. Authors' note: More specifically, the commission stated: "If the United States had to fight Russia in a Baltic contingency or China in a war over Taiwan (see Vignette 1), Americans could face a decisive military defeat." Further, "The prolonged, deliberate buildup of overwhelming force in theater that has traditionally been the hallmark of American expeditionary warfare would be vastly more difficult and costly, if it were possible at all. Put bluntly, the U.S. military could lose the next state-versus-state war it fights."
(All links accessed August 2019)

2 Edelman and Roughead, *Providing for the Common Defense*, 6-8.

3 Ibid.

4 M. Taylor Fravel, "China's Changing Approach to Military Strategy: The Science of Military Strategy from 2001 and 2013," in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, DC: The Jamestown Foundation, 2016), 62.

5 Ibid.

6 Roger Cliff, Mark Burles, Michael Chase, Derek Eaton, and Kevin Pollpeter, *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States* (Santa Monica, CA: The RAND Corporation, 2007), 51-64, https://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG524.pdf; and Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: The RAND Corporation, 2018), 15-16, https://www.rand.org/pubs/research_reports/RR1708.html.

7 Authors' note: LEGO® is a trademark of the LEGO Group. Mitchell Institute's use of the LEGO block as a conceptual analogy is intended to describe mosaic interoperability in a way that is easily accessible due to the high popularity of the building-block toy. It is not meant to infringe on the rights or intellectual property of the LEGO Group in any way.

8 Edelman and Roughead, *Providing for the Common Defense*, 14.

9 U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America* (Washington, DC: DOD, 2018), 1, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

10 Christopher M. Dougherty, *Why America Needs a New Way of War* (Washington, DC: Center for a New American Security, 2019), 1, https://s3.amazonaws.com/files.cnas.org/CNAS+Report+-+ANAWOW+-+FINAL2.pdf.

11 DOD, *Summary of the 2018 National Defense Strategy of the United States of America*, 4.

12 Edelman and Roughead, *Providing for the Common Defense,* 6-8.

13 Ibid.

14 Authors' note: For a discussion on rethinking the technological and capability challenges of the new "revolution in military affairs," see: Christian Brose, "The New Revolution in Military Affairs: War's Sci-Fi Future," *Foreign Affairs*, 98, no. 3 (May-June 2019), https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs.

15 Fravel, "China's Changing Approach to Military Strategy," 62.

16 Cliff, et al., *Entering the Dragon's Lair*.

17 Engstrom, *Systems Confrontation and System Destruction Warfare*, 16-17.

18 Authors' note: For a discussion on the impact of low-intensity operations on high-end force structure and the implications of this practice, see: Michael Buck, with Lawrence A. Stutzriem and Douglas Birkey, "Light Combat Aircraft: Looking at O/A-X and Beyond," *Mitchell Institute Policy Papers*, 11 (Arlington, VA: Mitchell Institute for Aerospace Studies, 2018), 7-9, http://docs.wixstatic.com/ugd/a2dd91_e2048a87f83c4fd5ab950d4ba107d7c2.pdf.

19 Authors' note: A primer on DOD's byzantine weapons requirements, development, and acquisition processes can be found here: Moshe Schwartz, *Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process*, CRS Report No. RL34026 (Washington, DC: Congressional Research Service, 2014), https://fas.org/sgp/crs/natsec/RL34026.pdf.

20 Authors' note: Manned-unmanned teaming describes the collaborative partnership and tight coupling of unmanned aircraft with physically crewed aircraft. While their respective roles will vary depending on mission circumstances, their teaming is intended to maximize the scale and scope of mission effects they can create while guarding against points of vulnerability.

21 Authors' note: LEGO® is a trademark of the LEGO Group. Mitchell Institute's use of the LEGO block as a conceptual analogy is intended to describe mosaic interoperability in a way that is easily accessible due to the high popularity of the building-block toy. It is not meant to infringe on the rights or intellectual property of the LEGO Group in any way.

22 Authors' note: The post-World War II American defense posture and operational concept of power projection are discussed at length in: Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenge* (Washington, DC: Center for Strategic and Budgetary Assessments, 2003), https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf.

23 Zachary Keck, "A Tale of Two Offset Strategies," *The Diplomat,* November 18, 2014, https://thediplomat.com/2014/11/a-tale-of-two-offset-strategies/; and Daniel Gouré, "Winning Future Wars: Modernization and a 21st Century Industrial Base," The Heritage Foundation, October 8, 2018, https://www.heritage.org/military-strength/topical-essays/winning-future-wars-modernization-and-21st-century-defense.

24 Keck, "A Tale of Two Offset Strategies."

25 Authors' note: For perspectives on how the second offset altered the U.S. military's relationship with information, see: Robert Martinage*, Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability* (Washington, DC: Center for Strategic and Budgetary Assessments, 2014), 13-15, https://csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf.

26 David A. Deptula, Lawrence A. Stutzriem, and Heather R. Penney, "Ensuring the Common Defense: The Case for Fifth Generation Airpower," *Mitchell Institute Policy Papers*, 20 (Arlington, VA: Mitchell Institute for Aerospace Studies, 2019), 13.

27 Deptula, *Effects-Based Operations: Change in the Nature of Warfare* (Arlington, VA: Aerospace Education Foundation, 2001), 9. Authors' note: The numbers from which this figure was derived come from Deptula's April, 19, 1991, paper "F-117 Target Analysis." Deptula's notes associated with the citation are as follows: "Of 688 targets on the MTL [master target list] (corrected for duplication), 298 were attacked by F-117s. Data from (S) 'Master Target List,' 1 March 1991, Central Command Air Force (CENTAF) Iraq Target Planning Cell and 37th Tactical Fighter Wing Mission Electronic Database, March 1991. The F-117 flew 1,299 of 74,091 combat sorties (1.75 percent) between 16 Jan 91 and 28 Feb 91. The definition of combat sorties used here includes only coalition fighter or bomber aircraft, not tankers, airlift, or other types of support. Data from (S) GWAPS, pp. 334-335. Information extracted in unclassified." See: *Effects-Based Operations*, endnote 27.

28 Martinage, *Toward a New Offset Strategy,* 16.

29 Deptula, *Effects-Based Operations*, 1.

30 Authors' note: For an in-depth discussion of the air campaign targeting the Iraqi regime and military as a system, see Richard P. Hallion, *Storm Over Iraq: Air Power and the Gulf War* (Washington, DC: Smithsonian Institution Press, 1992); and Diane T. Putney, *Airpower Advantage: Planning the Gulf Air Campaign, 1989-1991* (Honolulu, HI: University Press of the Pacific, 2006).

31 Deptula, *Effects-Based Operations*, 1.

32 Authors' note: For a discussion on the post-2001 trend of cancelling high-end capability to plus up low-intensity force structure, see: Deptula, et. al., "Ensuring the Common Defense," 5-6.

33 Authors' note: Nearly two decades later, many in DOD have forgotten—or never learned—this systems warfare approach.

34 Elbridge Colby, "How to Win America's Next War," *Foreign Policy*, May 5, 2019, https://foreignpolicy.com/2019/05/05/how-to-win-americas-next-war-china-russia-military-infrastructure/.

35 Ryan Pickrell, "The U.S. has been getting 'its ass handed to it' in simulated war games against Russia and China, analysts say," *Task & Purpose,* March 8, 2019, https://taskandpurpose.com/russia-china-war-games.

36 Sydney Freedberg, "U.S. 'Gets Its Ass Handed To It' In Wargames: Here's a $24 Billion Fix," *Breaking Defense*, March 7, 2019, https://breakingdefense.com/2019/03/us-gets-its-ass-handed-to-it-in-wargames-heres-a-24-billion-fix/.

37 Deptula, et. al., "Ensuring the Common Defense," 26-27.

38 Authors' note: For a discussion on PLA reflections and responses to American-led success in Operation Desert Storm, see: Roger Cliff, John Fei, Jeff Hagen, Elizabeth Hague, Eric Heginbotham, and John Stillion, *Shaking the Heavens and Splitting the Earth: Chinese Air Force Employment Concepts in the 21st Century* (Santa Monica, CA: The RAND Corporation, 2011), 35, 40-41, https://www.rand.org/content/dam/rand/pubs/monographs/2011/RAND_MG915.pdf. For analysis on Russian A2/AD challenges to the United States and NATO, see: Dominik Jankowski, "Six Ways NATO Can Address the Russian Challenge," *The New Atlanticist* (blog), Atlantic Council, July 4, 2018, https://www.atlanticcouncil.org/blogs/new-atlanticist/six-ways-nato-can-address-the-russian-challenge.

39 Douglas Barrie, "Anti-Access/Area Denial: Bursting the 'No-Go' Bubble?," *Military Balance* (blog), International Institute for Strategic Studies, London, March 29, 2019, https://www.iiss.org/blogs/military-balance/2019/04/anti-access-area-denial-russia-and-crimea.

40 Fravel, *Active Defense: China's Military Strategy Since 1949* (Princeton, NJ: Princeton University Press, 2019), 218.

41 Cliff, et al., *Entering the Dragon's Lair*.

42 Authors' note: A thorough discussion of the challenge that A2/AD poses to the United States can be found in: Krepinevich, Watts, and Work, *Meeting the Anti-Access and Area-Denial Challenge*.

43 Krepinevich, et al., *Meeting the Anti-Access and Area-Denial Challenge*, 3-5.

44 Brig Gen Alex Grynkewich, USAF (deputy director for global operations, Joint Chiefs of Staff), "An Operational Imperative: The Future of Air Superiority," *Mitchell Institute Policy Papers*, 7 (Arlington, VA: The Mitchell Institute for Aerospace Studies, 2017), 7, http://docs.wixstatic.com/ugd/a2dd91_4638a-708c6a14f18ab9922d1c07930b3.pdf.

45 Jordan Wilson, *China's Expanding Ability to Conduct Conventional Missile Strikes on Guam*, U.S.-China Economic and Security Review Commission Staff Research Report (Washington, DC: USCESRC, 2016), https://www.uscc.gov/sites/default/files/Research/Staff%20Report_China%27s%20Expanding%20Ability%20to%20Conduct%20Conventional%20Missile%20Strikes%20on%20Guam.pdf.

46 Krepinevich, et al., *Meeting the Anti-Access and Area-Denial Challenge,* 5.

47 Grynkewich, "An Operational Imperative," 7.

48 Defense Intelligence Agency (DIA), *Russia Military Power 2017: Building a Military to Support Great Power Aspirations* (Washington, DC: DIA, 2017), 32-33. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937.

49 Sean O'Connor, Konrad Muzyka, Huw Williams, "Analyzing Russia's SAM Capabilities," Jane's IHS Markit Defense Intelligence Briefing, presentation slides and text, August 31, 2017, www.janes.com.

50 "64N6 / 91N6E—TOMBSTONE / Big Bird," GlobalSecurity.org, https://www.globalsecurity.org/military/world/russia/tombstone.htm.

51 Ian Williams, "The Russia—NATO A2AD Environment," *Missile Threat*, the website of the Center for Strategic and International Studies' Missile Defense Project, January 3, 2017, https://missilethreat.csis.org/russia-nato-a2ad-environment/.

52 Gouré, "Winning Future Wars," 65.

53 Adam Cabot, "Fortress Russia: How Can NATO Defeat Moscow's A2/AD Strategy and Air Defenses?" *The National Interest,* November 3, 2108, https://nationalinterest.org/blog/buzz/fortress-russia-how-can-nato-defeat-moscows-a2ad-strategy-and-air-defenses-35087.

54 Jonas Kjellen, *Russian Electronic Warfare: The role of Electronic Warfare in Russian Armed Forces*, R-4625-SE (Stockholm: Swedish Defense Research Agency, 2018), 83, http://www.worldinwar.eu/wp-content/uploads/2018/12/Russian-Electronic-Warfare1.pdf.

55 Authors' note: For a discussion of PLA doctrine and how it relates to systems attacks against communications, logistics, basing, and space systems, see: Cliff, et al., *Entering the Dragon's Lair, 51-64.*

56 Fravel, *Active Defense,* 205. Authors' note: See chapters six and seven for a discussion of how U.S. military victories from 1991 through the present have influenced Chinese military strategy, doctrine, and modernization priorities.

57 Junshi kexue juan lishi yanjiu bu. *Haiwan zhanzheng quanshi* [*A Complete History of the Gulf War*] (Beijing: Junshi kexue chubanshe, 2000), 519, in Fravel, *Active Defense*, 190.

58 Fravel, *Active Defense*, 224-225.

59 Fravel, "China's Changing Approach to Military Strategy," 56.

60 Work quoted in Pickrell, "The U.S. has been getting 'its ass handed to it' in simulated war games against Russia and China, analysts say."

61 John Costello and Peter Mantis, "Electronic Warfare and the Renaissance of Chinese Information Operations," in *China's Evolving Military Strategy*, 179.

62 *The Science of Military Strategy,* ed. Peng Guangqian and Yao Youzhi (Beijing: Military Science Publishing House, 2005), 339-340.

63 Translation of Military Strategic Research Department Academy of Military Science, *The Science of Military Strategy* (Middletown, DE: 4th Watch Publishing Co., 2018), 93, 95.

64 Engstrom, *Systems Confrontation and System Destruction Warfare*, 16.

65 The State Council Information Office of the People's Republic of China, *China's National Defense in a New Era* (Beijing: Foreign Languages Press Co. Ltd., 2019), http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc.

66 Engstrom, *Systems Confrontation and System Destruction Warfare*, 16.

67 Ibid.

68 Ibid., 17. Authors' note: Engstrom cites one source saying "if the essential elements of the system fail or make mistakes, the essence of the system will change … [thereby becoming] non-functional or even useless."

69 Ibid.

70 Ibid.

71 Dougherty, *Implementing the National Defense Strategy Demands Operational Concepts for Defeating Chinese and Russian Aggression* (Washington, DC: Center for a New American Security, 2019), https://www.cnas.org/publications/commentary/implementing-the-national-defense-strategy-demands-operational-concepts-for-defeating-chinese-and-russian-aggression.

72 Engstrom, *Systems Confrontation and System Destruction Warfare*, 15.

73 Mark Gunzinger, Carl Rehberg, Jacob Cohn, Timothy A. Walton, and Lukas Autenried, *An Air Force For an Era Of Great Power Competition* (Washington, DC: Center for Strategic and Budgetary Assessments, 2019), 35, https://csbaonline.org/uploads/documents/CSBA_AFAIS_Report_v7.pdf.

74 Dougherty, *Why America Needs a New Way of War*, 24. Authors' note: Dougherty writes: "Instead of methodically battering down adversaries' defenses or vainly hunting for mobile missile systems, U.S. operational concepts for defeating Chinese or Russian aggression should focus on defeating Chinese or Russian power-projection forces operating within functional A2/AD networks, before those forces can seize key objectives and present the United States with a fait accompli."

75 Authors' note: The AirSea Battle operational concept was an attempt to rethink how to employ existing assets and new capabilities against an A2/AD foe, in the context of greater competition with China. See: AirSea Battle Office, *AirSea Battle: Service Collaboration to Address Anti-Access & Area-Denial Challenges* (Washington, DC: DOD, 2013), https://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf.

76 Authors' note: See Edelman and Roughead, *Providing for the Common Defense*, ix. They write: "U.S. security commitments and operations in the Middle East cannot be wished away."

77 Authors' note: For more on the long-term effects of overusing high-end capabilities in low-end conflicts see: Buck, et al., "Light Combat Aircraft," 7-9.

78 Authors' note: Original figure derived from collected data from "The Air Force in Facts and Figures," *Air Force Magazine*, almanac editions, May 1996, 2000, 2005, 2010, 2015, and June 2019, http://www.airforcemag.com/Almanacs/Pages/default.aspx.

79 Authors' note: The post-Cold War drawdown, and its effect on capacity and force structure vis-a-vis aerospace power, is discussed extensively here: Deptula and Birkey, "The Force We Need: Key Factors for Shaping the Air Force for the Future," *Mitchell Institute Policy Papers*, 19 (Arlington, VA: Mitchell Institute for Aerospace Studies, 2019), http://docs.wixstatic.com/ugd/a2dd91_7f1dd52770df4faa993a3f90df9622b3.pdf.

80 Authors' note: Original figure derived from collected data from "The Air Force in Facts and Figures," *Air Force Magazine*, almanac editions, May 1996, 2000, 2005, 2010, 2015, and June 2019, http://www.airforcemag.com/Almanacs/Pages/default.aspx.

81 Deptula, et. al., "Ensuring the Common Defense," 5-7.

82 Authors' note: As the U.S. military loses force capacity vis-a-vis the PLA, the capability and performance gap of systems such as combat aircraft and weapons continues to shrink. For an exploration of the current U.S.-China military balance see: Eric Heginbotham, Michael Nixon, et. al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: The RAND Corporation, 2015), https://www.rand.org/pubs/research_reports/RR392.html.

83 Authors' note: China, in particular, has long discussed targeting U.S. communications, logistics, basing, and space systems in order to hold American military assets at risk. See: Cliff, et al., *Entering the Dragon's Lair*, 51-64.

84 Eric J. Mehrtens, "Tackling Tomorrow's High-Value Airborne Assets Anti-Access/Area-Denial Problem--Part One," *Over The Horizon Journal*, July 8, 2019, https://othjournal.com/2019/07/08/tackling-tomorrows-high-value-airborne-assets-anti-access-area-denial-problem-part-one/.

85 Dougherty, *Why America Needs a New Way of War*, 20.

86 Lani Kass, "U.S. Airpower: The Imperative for Modernization (Buy the F-35)," *Breaking Defense*, March 18, 2019, https://breakingdefense.com/2019/03/us-air-power-the-imperative-for-modernization-buy-the-f-35/.

87 Schwartz, *Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process*.

88 Buck, et al., "Light Combat Aircraft," 7-9.

89 Authors' note: In addition to combat aircraft, U.S. joint combat operations concepts currently rely heavily on fourth-generation airborne command and control and intelligence, surveillance, and reconnaissance (C2ISR) airplanes, such as the RC-135 Rivet Joint, E-8 JSTARS, and E-3 Sentry, which are particularly at risk in A2/AD environments. For more on this, see: Mehrtens, "Tackling Tomorrow's High-Value Airborne Assets Anti-Access/Area-Denial Problem–-Part One."

90 DOD, *Summary of the 2018 National Defense Strategy of the United States of America.*

91 Authors' note: Many of these questions about future disaggregated combat architectures and operations are explored in Deptula's writings on the "combat cloud." See: Deptula, "Evolving Technologies and Warfare in the 21st Century: Introducing the Combat Cloud," *Mitchell Institute Policy Papers*, 4 (Arlington, VA: Mitchell Institute for Aerospace Studies, 2016), http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

92 John R. Boyd, "The Essence of Winning and Losing," ed. Chet Richards and Chuck Spinney, *Defense and the National Interest* (a now-defunct blog), Project on Government Oversight, August 2010, http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf.

93 Authors' note: For a comprehensive discussion of this OODA process in the European theater, see Charles W. McArthur, *Operations Analysis in the U.S. Army Eighth Air Force in World War II*, (Providence, RI: American Mathematical Society, 1990); and Robert S. Ehlers Jr., *Targeting the Third Reich: Air Intelligence and the Allied Bombing Campaigns*, (Lawrence, KS: University Press of Kansas, 2009).

94 Authors' original diagram, Mitchell Institute for Aerospace Studies, August 16, 2019.

95 Authors' original diagram, Mitchell Institute for Aerospace Studies, July 10, 2019.

96 Ibid.

97 "Mosaic Workshop: A Future Force Design," Mitchell Institute for Aerospace Studies, July 17, 2019.

98 Ibid.

99 Authors' note: The military advantages of disaggregated, distributed combat operations in this context are highlighted in: Deptula, "Evolving Technologies and Warfare in the 21st Century: Introducing the Combat Cloud," 6.

100 SrA Colville McFee, USAF, "Opening doors to the future: 427th Reconnaissance Squadron ribbon-cutting ceremony," 9th Reconnaissance Wing Public Affairs, April 26, 2019, https://www.25af.af.mil/News/Article-Display/Article/1829710/opening-doors-to-the-future-427th-reconnaissance-squadron-ribbon-cutting-ceremo/.

101 Pat Host, "Air Force, Contractors Working Together On Common Mission Control Center," *Defense Daily,* June 21, 2016, https://www.defensedaily.com/air-force-contractors-working-together-on-common-mission-control-center/air-force/.

102 Kris Osborn, "The Air Force is Creating a System to Manage the Military's Forces in War," *The National Interest,* March 1, 2018, https://nationalinterest.org/blog/the-buzz/the-air-force-creating-system-manage-the-militarys-forces-24701. Authors' note: Osborn states: "ABMS seeks to harvest the latest ISR-oriented technologies from current and emerging systems as a way to take a very large step forward—and connect satellites, drones, ground sensors, and manned surveillance aircraft seamlessly in real time across a fast-changing, dispersed combat area of operations."

103 Secretary of the Air Force Public Affairs, Robins Air Force Base Public Affairs, "Robins to host Advanced Battle Management System," June 6, 2018, https://www.robins.af.mil/News/Article-Display/Article/1542887/robins-to-host-advanced-battle-management-system/.

104 Lt Col Dan Javorsek, USAF (program manager, DARPA Strategic Technology Office), "Adapting Cross-Domain Kill-Webs (ACK)," Defense Advanced Research Projects Agency, July 24, 2019, https://www.darpa.mil/program/adapting-cross-domain-kill-webs.

105 Lt Col Jimmy Jones, USAF (program manager, DARPA Strategic Technology Office), "Distributed Battle Management (DBM)," Defense Advanced Research Projects Agency, July 24, 2019, https://www.darpa.mil/program/distributed-battle-management.

106 Khine Latt, "Dynamic Network Adaptation for Mission Optimization (DyNAMO)," Defense Advanced Research Projects Agency, https://www.darpa.mil/program/dynamic-network-adaptation-for-mission-optimization. Authors' note: DARPA states that the DyNAMO program is "developing and testing technologies that enable adaptive, mission-responsive networking among diverse airborne platforms in contested environments." Further, DyNAMO is "developing information-centric approaches to bridge disparate networks and to adaptively configure and control networks and networks of networks for operation in dynamic and contested environments." And, it is "addressing optimization within legacy and future military networks, interactions between networks, and availability of necessary network services to support mission success."

107 Jones, "Resilient Synchronized Planning and Assessment for the Contested Environment (RSPACE)," Defense Advanced Research Projects Agency, July 24, 2019, https://www.darpa.mil/program/resilient-synchronized-planning-and-assessment-for-the-contested-environment.

108 Kathleen Hicks, "Bad Idea: Arguing Over Capabilities- vs. Threat-based Planning," *Defense 360*, December 4, 2017, https://defense360.csis.org/bad-idea-arguing-capabilities-vs-threat-based-planning/.

109 Jones, "System of Systems Integration Technology and Experimentation," Defense Advanced Research Projects Agency, August 5, 2019, https://www.darpa.mil/program/system-of-systems-integration-technology-and-experimentation; and Mariana Iriarte, "Skunk Works, DARPA team demo key capabilities in SoSITE program," Military Embedded Systems, August 3, 2019, http://mil-embedded.com/news/skunk-works-darpa-team-demo-key-capabilities-in-sosite-program/.

An Affiliate of the Air Force Association | www.mitchellaerospacepower.org