Vol. 4, September 2016

MITCHELL INSTITUTE
Policy Papers

Key Points

Advancements in computing and network capabilities are empowering the ascent of information as a dominant factor in modern warfare.

Because of this trend, desired effects will increasingly be achieved through the interaction of multiple systems, each sharing information and empowering one another. It is a concept envisioned as a "combat cloud"—an operating paradigm where information, data management, connectivity, and command and control (C2) are core mission priorities.

The combat cloud will not only change the way we approach requirements, but more importantly, the way we think about C2 and operate C2 systems. A combat cloud could ultimately be strategically dislocating to any challenger, providing conventional deterrence to an unparalleled degree, and could enable simultaneous wartime operational dominance in multiple domains.

Evolving Technologies and Warfare in the 21st Century: Introducing the "Combat Cloud"

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

Abstract

The US and its allies are now at a critical point in history—at the center of an "information in war" revolution, where the speed of information, and advance of technology and organizational design are merging to change the execution of military operations. The 21st century demands a new, more agile, and integrated operational framework for the employment of allied military power, and to shift away from the structure of segregated land, air, and sea warfare.

We must move towards cross-domain synergy, embracing complementary vice merely additive employment of multi-domain capabilities that enhances effectiveness, and compensates for individual vulnerabilities. Desired military effects will increasingly be generated by the interaction of systems that share information and empower one another. This phenomenon is not restricted to an individual technology, nor is it isolated to a specific service, domain or task.

This concept can be envisioned as a "combat cloud"—an operating paradigm where information, data management, connectivity, and command and control (C2) are core mission priorities. The combat cloud treats every platform as a sensor, as well as an "effector," and will require a C2 paradigm enabling automatic linking, seamless data transfer capabilities, while being reliable, secure, and jam proof. The combat cloud inverts the paradigm of combined arms warfare— making information the focal point, not operational domains. This concept represents an evolution where individually networked platforms—in any domain—transform into a "system of systems" enterprise, integrated by domain and mission-agnostic linkages.

Introduction

Today, wireless connectivity, powerful personal computing devices, and cloud-based applications are integral to daily life. The ability to access, process, and disseminate mass volumes of information anywhere at anytime has revolutionized society's function.

This same development is also radically altering how the United States military projects power. Faster and more capable networks and computing capabilities are turning information into the dominant factor in modern warfare. As one Air Force commander recently remarked, we need to understand that "platforms like the F-22 are information machines far above and beyond being killing assets."[1] Recent operations over Syria as part of Operation Inherent Resolve (OIR) validate this assertion, with F-22s employed as information nodes in that campaign versus in their traditional air superiority role.

The US and its allies are at a critical juncture in history – at the center of an "information in war" revolution – where the speed of information, advance of technology, and designs of organizations are merging to change the way we operate.

Given this reality, it is critical to acknowledge that information and its management is just as important today as the traditional tools of hard military power— airplanes, satellites on orbit, infantry, amphibious elements, and warships at sea. Information and data is the force evolving all these tools from isolated instruments of power into a highly integrated enterprise where the exchange of information and data will determine success or failure in 21st century warfare.

This has major implications throughout the US military enterprise—shaping key focus areas like doctrine, organization, training, materiel acquisition, and sustainment, along with command and control (C2). Leaders and decision makers in the policy community also need to adjust to the new realities of information age combat. Paradigms dating back to the Second World War and the Cold War will simply fall short when considering how to build, sustain, and employ military power in the modern era.

The US and our allies are at a critical juncture in history – at the center of an "information in war" revolution -- where the speed of information, advance of technology, and designs of organizations are merging to change the way we operate.

This change has dramatically shortened decision and reaction times, and reduced the number of individual systems it takes to achieve desired effects in combat. During World War II, for example, the process of finding, identifying, tracking, targeting, engaging, and assessing a particular target could take two months or more. This process would often involve flying pre-strike reconnaissance missions to find and fix a target, dispatching strike aircraft or heavy bombers like the B-17 to put large numbers of weapons on target, then assessing the damage with more post-strike reconnaissance sorties by assets designed solely for this task. By the Vietnam War, this process had shrunk to just a few weeks, but often followed a similar pattern, utilizing pre-strike reconnaissance flights to fix and track targets, striking with assets like a B-52, then assessing damage with more reconnaissance flights. With the advent of modern sensors, networks, aircraft and other assets, this process has been compressed to mere minutes in today's wars. Where it used to take months and thousands of airmen and aircraft with separate functions to attack a single target, today we can find, fix, and finish a target from a single aircraft within minutes.

Ever since the introduction of modern mechanized warfare in the early twentieth century, the scale and scope of combat has been governed by industrial means of power projection. Advances in aircraft, ships, and ground vehicles increased speed, reach, and precision but still relied on mass to apply force. With the onset of the 20th century, military tasks, historically restricted to land and sea, expanded into the air, space, and underwater domains, and advancements in air and space power enabled global power projection. In the 21st century, we face another technology-driven inflec-

tion point that will again fundamentally reshape what it means to project military power.

Military power today is still mostly projected through platforms, such as aircraft, ground vehicles, or ships. But as the information age progresses, successful military operations will become more defined by more powerful networks than the capability of specific platforms. The need to use these networks to find and fix military targets in a timely manner will gain in importance, if not more so than finding a suitable platform to strike or engage them. Multi-function assets and aircraft, capable of performing strike, ISR, and other tasks, will steadily replace mission specific assets. Target engagement based around the need to "destroy" a given aim point will give way to effects-focused engagement, driven by improving capabilities such as cyber warfare tools. Massed, non-stealthy strike packages of manned aircraft will evolve into more distributed force packages, with greater low observable (LO) characteristics, and more use of automated systems. Individual precision weapons will give way to "volumetric weapons," such as directed energy. Data, information, and ISR gathering and analysis will evolve as knowledge management becomes even more important, as will predictive as opposed to reactive analysis. Even dogfighting, as understood in the 20th and early 21st century, will increasingly give way to "datafighting" – the need to secure information superiority as a prerequisite for success in any conflict.

… warfare is evolving as we transition out of the industrial age, and further into the information age. Advancements in computing and network capabilities are empowering the ascent of information as a dominant factor in warfare.

These trends highlighted show warfare is evolving as we transition out of the industrial age, and further into the information age. Advancements in computing and network capabilities are empowering the ascent of information as a dominant factor in warfare. It is now no longer sufficient to focus on just managing the physical elements of a conflict—such as planes, satellites in space, troops, amphibious elements or ships at sea. These individual platforms are evolving from a "stove piped," parochial service alignment, to a loosely federated "joint and combined" construct today, and eventually into a highly integrated enterprise that collaboratively leverages the broad exchange of information. Desired effects will increasingly be attained through the interaction of multiple systems, each one sharing information and empowering one another for a common purpose. This phenomenon is not restricted to an individual technology or system, nor is it isolated to a specific service, domain, or task.

It is a concept that can be envisioned as a "combat cloud"—an operating paradigm where information, data management, connectivity, and C2 are core mission priorities. Technology is now enabling the connection of aerospace systems with sea and land-based systems in ways that enhance their effectiveness, and compensate for the vulnerabilities of the individual components. A modern intelligence, surveillance, and reconnaissance (ISR) strike, maneuver, and sustainment complex could be described as a "combat cloud" that applies information age technology to conduct highly interconnected and distributed operations. This effectively inverts the paradigms of combined arms warfare, by making information the focal point vice traditional domains of operation (land, sea, and air).

While mechanical technology will continue to serve as a key factor in future military operations, the information empowering these systems will stand as the backbone for their potential. As the combat cloud is developed, it promises to afford an expansive, highly redundant defense complex with radically enhanced data gathering, processing, and dissemination capabilities. These attributes will offer actors at every level of war dramatically enhanced situational awareness by transforming masses of disparate data into decision-quality knowledge.

This development represents an evolution where individually networked platforms transform into a broader "system of systems" enterprise integrated through domain and mission agnostic infor-

While many militaries are evolving toward becoming informationized forces, the integration and assimilation of related capabilities is incomplete.

mation links. This approach will not only change the way we define new requirements, but more importantly, the way we think about C2 and operate the systems associated with this task. A distributed, self-forming, all-domain combat cloud that is self-healing and difficult to attack effectively significantly complicates an enemy's planning, and will compel them to dedicate more resources toward defense and offense. In its ultimate manifestation, the combat cloud will be strategically dislocating to any military challenger. A mature combat cloud will provide superior conventional deterrence to a degree previously only achieved by nuclear deterrence, and enable operational dominance in multiple domains.

Turning this vision into reality will require a significant effort. While many militaries are evolving toward becoming informationized forces, the integration and assimilation of related capabilities is incomplete. Militaries are still predominantly organized, trained, and equipped to fight a mechanized war—one in which information integration is a secondary support function.

Most bureaucratic organizations and current programs of record reflect the linear extrapolation on the development of combined arms warfare from the industrial age. Program oversight efforts within defense ministries and governments are also lagging—with antiquated industrial age governance impeding information-age endeavors. Any assessment of the likely landscape of future conflict must recognize that no matter what type of engagement should emerge, the outcome will increasingly be determined by which side is better equipped and organized to gather, process, disseminate, and control information.

The need to adapt to information age warfare is pressing. Modern technology and telecommunications are leveling traditional advantages enjoyed by the US and other sophisticated militaries, as threats grow more effective and proliferate. Resources are also declining. The US Air Force is increasingly reliant on high demand/low density (HD/LD) forces across several core mission areas. These missions include long-range strike (just 20 B-2s are augmented by legacy aircraft), air superiority (185 F-22s are currently augmented by only some F-35s and legacy fighters), C2 (20 E-3 AWACS are supplemented by combined air operations centers or CAOCs), and there are limited numbers of long range, survivable intelligence, surveillance, and reconnaissance (ISR) assets in the current inventory.[2] This shortfall is exacerbated because post-September 11, 2001 conflicts in Afghanistan and Iraq occurred in permissive environments, where information dominance and air superiority were never challenged, and thus immediate operational needs trumped long-term force structure concerns. It is a near guarantee future conflicts will not afford similar circumstances.

Furthermore, budget austerity appears to be the new normal. Militaries need to devise more effective and efficient means to secure desired effects with existing capabilities. If the US and our allies are going to win the next war, we need to gain persistent access to data networks while denying this same capability to any adversary. To be serious about this effort, military services need to embrace doctrinal and concept changes to how their forces are organized, trained, and equipped. Militaries have to innovate to secure desired effects in a more effective and efficient fashion, using technology to enable a new combat enterprise. The concept of the combat cloud stands as a framework to empower this vision.

The Future, Imagined: A Combat Cloud Scenario

Let's examine, for a moment, just how the combat cloud concept might actually unfold in a hypothetical scenario, set some time in the not-too-distant future.

In the opening phase, an amphibious force is escorted by Royal Air Force (RAF) F-35Bs, as the force carries out a raid against enemy anti-ship batteries to enable insertion of friendly forces. Upon reaching the objective, a V-22 Osprey carrying special operations forces is downed by the enemy. The

raid continues, though, and help is sent to extract the injured. As enemy air defenses begin to react, US Air Force F-22s guide missiles launched from an allied ship to hit two surface-to-air (SAM) missile sites, and team with Royal Norwegian Air Force F-35s to further suppress other threats.

Situational awareness tools are common across all platforms in this force. The F-22s and V-22s are able to detect and federate threat detection information so the force's limited weapons are employed against priority threats. The F-35s tap into the same picture, populated with other data, and broadcast the status of these threats. Both special operations, and general purpose air, land, and sea forces maintain an accurate intelligence, surveillance, and reconnaissance (ISR) picture of the opponent's defenses, gathered by friendly aircraft.

In the secure video debrief conducted five hours later, the strike commander credits his ability to see through the confusion—caused by the enemy's response to the strike—as the reason attack objectives were met. He adds that while three people died in the V-22 crash, none were lost during the actual attacks against enemy missile batteries. Injured personnel were evacuated, other losses were avoided, and new attacks were formulated by the real-time data available to the ground strike team. The F-35 and F-22 flight leads agreed that the real-time display of the status of opposing defenses, communications, and emissions allowed them to enhance their electronic warfare (EW) and kinetic attacks.

In the scenario outlined, every player had access to high quality, high confidence data that let them peer through the fog of war to see what was needed to save lives, keep the attack moving, and orchestrate follow-on actions to maximize success.

Space operators observed that stability of the command and control (C2) networks gave them the information needed to alter the view of satellites providing inputs to the F-22 and F-35 hunter-killer team. The RAF F-35 flight lead also described how he leveraged four Remote Piloted Aircraft (RPA) assigned to the team for the strike to improve their jamming techniques, and enhance the full motion video link to the maritime operations center. Lastly, cyber operators revealed they were forced to work through several challenges to network stability, caused by attacks from enemy cyber forces.

So, what is different in the above scenario from how we conduct the business of warfare today?

Clearly evident in the scenario is the sort of robust information connectivity that is largely aspirational today. In the scenario outlined, every player had access to high quality, high confidence data that let them peer through the fog of war to see what was needed to save lives, keep the attack moving, and orchestrate follow-on actions to maximize success. The problems associated with connectivity among surface platforms and low radar cross-section aircraft operating deep within enemy space were overcome. In the final scenario analysis, real-time data enabled real-time decision making, allowing every player to not only remain oriented in a highly confusing battle, but reorient, out think and proactively shut down opposing defenses.

The force in the scenario was enabled by a future vision of connectivity, of every combined task force player instantly forming together when in proximity to one another. However, this is not merely a recycled vision of "net-centric warfare." The combat cloud is a concept where every object and person in this future force is a component, a router, and a node in a real-time IP based constellation with low enough latency to enable accurate effects against priority targets. But what must be accomplished to allow us to do that? The focus of the remainder of this paper is on the first step to realize the vision of a combat cloud.

The Vision: Seeing Through the Fog of Modern War

To move towards achieving this reality, there first needs to be a common vision that all stakeholders and players in the defense community can understand, and accept as a desired way ahead. This is not about focusing on a particular system,

acquisition strategy, military service, or special organization. The United States requires the varied, separate, distinct capabilities inherent in our separate military services, and other government security organizations that make up the US and allied defense architectures.

However, we must be bound by a common appreciation for the value of sharing information as a critical element of national security operations. This is about a vision—aptly described as still using elements of the well-established notion of combined arms warfare, but moving beyond this approach to one of combined effects warfare. The kind of combined effects resident in unified ISR, strike, maneuver, and sustainment complex integrated across the electromagnetic spectrum.

This is the vision more descriptively labeled as a combat cloud. The concept has, as its basis, allied militaries linking information-age aerospace systems with cyber, sea, and land-based capabilities in ways that will enhance their combined effectiveness, while compensating for their individual vulnerabilities. The combat cloud concept is somewhat analogous to "cloud computing," which is based on using networks to rapidly share information across a highly distributed system of systems. However, instead of combining the computing power of multiple servers, a combat cloud will capitalize on the ubiquitous and seamless sharing of information among weapon systems in multiple domains to rapidly exchange data in order to act as a cohesive whole in warfare.

Current systems are largely expected to operate in a semi-autonomous fashion, with a basic level of collaborative engagement with other platforms. These shortcomings place pressure on individual assets to possess numerous internal capabilities.

If enabled by secure, jam-proof, and intrusion-proof connectivity, a combat cloud may be capable of employing fewer modern combat systems to achieve higher levels of effectiveness, across larger areas of influence in comparison to legacy operational concepts. For example, instead of relying on traditional approaches that mass fighters, bombers, and supporting aircraft into major strike packages to attack particular targets, a combat cloud could integrate complementary capabilities into a single, combined "weapons system" to conduct disaggregated, distributed operations over an entire operational area. The combat cloud requires treating every platform as a sensor as well as an "effector." It will require a C2 paradigm that enables automatic linking, as does cellular phone technology today. It will also need to transfer data securely, reliably, and seamlessly, without need for human interaction. While the overarching notion of actualizing a combat cloud with the degree of integration required to achieve a self-forming, self-healing complex is a new idea, many of the individual technological elements and capabilities required to manifest this vision already exist or are under development. But each was developed in the absence of an overarching, integrating vision. In fact, each component or platform comes with a somewhat different concept of operations (or CONOPS) that is unique to the particular system.

Modern US military networks and datalinks are a good example of this narrow approach to CONOPS at work. Some of these include Link-16, Intra-Flight Data Link (IFDL), Tactical Targeting Network Technology (TTNT), Multifunction Advanced Data Link (MADL), and the Joint Aerial Layer Network (JALN) concept.[3] While delivering distinctive capabilities, the services developed each of these in a stand-alone manner without an overarching construct to ensure joint or allied partner interoperability, much less interdependency. Establishing the combat cloud as the operational template for various linkages affords a basis of interoperability, and more importantly interdependency to normalize existing systems, to guide development on emerging programs, and establish common requirements.

Current systems are largely expected to operate in a semi-autonomous fashion, with a basic level of collaborative engagement with other platforms. These shortcomings place pressure on individual assets to possess numerous internal capabilities. The complexity inherent to this approach drives lengthy development cycles, which in turn leads to require-

ment creep, time and cost overruns, and delays in capability. In sharp contrast, the combat cloud will enable individual platforms to harvest a wide range of capabilities by sharing critical information, thereby negating the need to possess all functions internally. The goal is to align strategy, investment, and partnership capacity through a collaborative, responsive operational template. The goal will not be to share the same operating standard among US and allied assets, but for the operating concepts to at least be headed in the same direction—towards a combat cloud.

By affording numerous redundant functions options through participation in the combat cloud, individual platforms don't have to leverage as much from their internal attributes, nor do the services need to organize, train, and equip to operate "organically" to achieve self-sufficiency. Additionally, the combat cloud vision reduces the pressure to overload requirements on a given program, and allows individual platforms to evolve in a more cost-effective fashion. The result is that individual systems are freer to excel in specific areas where their capability can be maximized. For its part, the combat cloud supplements a broader array of capabilities, and ultimately serves as a more effective and efficient means to achieve the true intent of "jointness."

The combat cloud vision would allow us to take advantage of current and emerging technologies to develop plug-and-play systems that connect into a common information exchange.

The same holds true for allied interoperability. Partners around the world are modernizing their armed forces with new military capabilities that have the potential to enhance the effectiveness of a combat cloud-enabled force. Some of these systems include the F-35, the Eurofighter Typhoon, Aegis Weapons System-equipped ships,[4] the Royal Australian Air Force (RAAF) E-7A Wedgetail airborne early warning and control aircraft, the German Eurohawk RQ-4 high altitude long endurance ISR RPA, and others. Transforming these individual weapon systems into collaborative elements of an interdependent operational enterprise is what the combat cloud is all about. Whether discussing technical standards, common training standards, or established operational tactics, the potential afforded by individual allied systems will only be realized if they are harnessed in an organized, deliberate fashion.

The Way Ahead: Shaping the Combat Cloud

To describe the vision for the combat cloud, we must understand the physics of future combat platforms will likely not change significantly. But, how these systems operate within future battle networks must change to realize the potential of informationized warfare. In order for combat forces to freely access and distribute information during combat operations, some existing platforms will need modification, but more importantly the military services must develop gateways and relevant infrastructure to share information in a ubiquitous and seamless fashion. This has become "industry standard" for civil commerce, and it must become the new normal for the US military, and our allies. Networking will be key to the success of the combat cloud, but the concept is much larger than just networks—it is about automating shared knowledge, access, and employment of desired actions to achieve desired effects. In short, it will turn an entire area of responsibility (AOR) in a conflict into a CAOC.

To shape and grow the combat cloud into reality, focus must be kept on developing actionable knowledge and delivering combat effects across multiple domains, not just from a particular aircraft or platform. Platforms must become "cloud ready" in terms of communications and information management. Some platforms may require modifications, such as avionics bus structural improvements to permit greater data off boarding, and subscriptions to a variety of external data sources. All systems, eventually, would be able to feed data back into the combat cloud and pull information as required. The responsibility to track, identify, employ, and guide weapons would be shared across all platforms. For example, a B-21 could use sensor data to guide a submarine launched cruise missile

to target, or a ship-based radar could provide targeting data for an F-35.

The concepts of net-centric military operations, the Joint Information Environment (JIE) and the JALN attempt to address the needs mentioned above by establishing performance parameters for the acquisition of information technology systems. These performance requirements apply to any system capable of creating information, such as platforms, weapons, and even handheld devices. The combat cloud vision would allow us to take advantage of current and emerging technologies to develop plug-and-play systems that connect into a common information exchange. This would enable individual military tactical data links to join up with a coalition information network through multiple pathways, such as ground terminals or a JALN. The combat cloud would create a broad foundation to build such a network.

Rather than put value on just the weapons and platforms that launch them, commanders need to recognize the value of the effects they can create based on the seamless sharing of information.

Another approach is to create gateway-based solutions to connect currently fielded disparate networks, waveforms, and platforms. Yet another concept is to equip each platform with its own translator to accomplish the role of a few gateways thus contributing to the distributed and robust nature of a notional combat cloud.

To become a fully information-enabled force, all future capabilities will need the architecture and necessary protocols to connect through gateways with individual translators, or to existing networks. Ultimately, a plug-and-play concept may allow current disparate networks and systems to seamlessly share and access information. This does not mean every nation or service has to buy the same equipment—nor does it impose the unrealistic aim of a common operating standard. Experience, physics, tactics, or the combat environment may dictate that some systems should be uniquely designed not to operate with others. Nevertheless, normalizing data link frequencies, waveforms, and content format, or requiring unique systems to provide a gateway gives a combined force commander the flexibility to fully command battle networks and globally control distributed forces.

However, despite acknowledgment that future forces will need to operate and defend battle networks, progress toward building fully integrated battle networks has been sporadic and inconsistent, and without overarching vision. Currently, the US Department of Defense (DOD), other nations' defense ministries, and the US military services are bogged down with dozens of programs and concepts, each being developed independently and lacking a coherent effort that reconciles gaps or redundancies. Compounding the challenge of moving towards a combat cloud is the realization that since communication systems were primarily created to facilitate C2 and battlespace awareness, they have traditionally been viewed as supporting capabilities that simply enhance primary combat tasks. This has resulted in a piecemeal approach to fielding information systems and communication networks.

Conclusion: Making the Combat Cloud Reality

So how do we change this situation to best achieve information access and control?

The capability already exists for current battle networks to translate collected information into a common format so other systems are able to access and process the information. Future joint and combined force operations will need an even greater ability to establish multiple network paths that function across the electromagnetic spectrum. We must also assume that any operational environment will be contested, so solutions must be devised to achieve assured connectivity. This will be one of the toughest challenges in achieving the promise of the combat cloud, and therefore more effort needs to be focused on this task. Potential options may include the development of multiple and distributed pathways for low probability-of-intercept (LPI) communication networks, laser communications, multi-domain optical/radio frequency transfer technology, cryptographic security schemes, and others.[5]

In the current program-centric budgetary world of our defense organizations, narrow focus on individual platforms, sensors, and weapons is the norm. Absent a clear definitive vision, and without a strategy to realize that vision, the big picture is lost among a collection of disparate, disconnected systems often kluged together to pass as "joint." This is why vision is needed. Future combined and joint operations will require concepts and practices to show how to join together and perform C2 for desired effects; and to bring together distributed battle, intelligence, and surveillance networks.

Commanders must change the way they view networks and information systems. Rather than put value on just the weapons and platforms that launch them, commanders need to recognize the value of the effects they can create based on the seamless sharing of information. This shift in perspective will involve much more than simply material changes involving technology development. This approach is a completely different way of thinking about how we will use weapon systems in the future. Transitioning from industrial age, platform-centric methods of force employment to an interconnected, information-driven model will involve numerous challenges.

Becoming a fully informationized force will require leaders to recognize that information is a combat mission that must be controlled and protected by fielding weapon systems focused on this objective.

Transition will require a doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) approach to define a "template" that guides the modernization of related policy, acquisition, and concepts of operation. This will also require leaders and policy makers to seek collaborative solutions among the US military services, move from measures of merit that replace "cost per-unit" to "cost per-effect," eliminate stove-piping of kinetic and non-kinetic options, develop reliable and resilient data links, create sufficient diversity to avoid single points of failure, and realize automated multi-level security tools and procedures to ensure allied and coalition participation.

Becoming a fully informationized force will require leaders to recognize that information is a combat mission that must be controlled and protected by fielding weapon systems focused on this objective.

In an era of constrained resources and order of magnitude increases in warfighting capability such as the development of directed energy weapons, perhaps the best bet on achieving the ability to defeat modern threats is to move towards actualizing the combat cloud. This approach will not only change the way the US and its allies define new requirements, but also more importantly the way we think, command, control, and operate those systems. This is the essence of the combat cloud—it is not just the network, but also the entire enterprise of sensors, shooters, and connectors—all part of a cohesive, coherent whole that must extend across all operating domains.

The future calls for an agile operational framework for the integrated employment of allied military power. It means taking the next step in shifting away from a structure of segregated land, air, and sea warfare approaches to truly integrated operations.

The central idea is cross-domain synergy. The complementary employment of capabilities in different domains, instead of merely additive employment, is the goal—such that each one enhances the effectiveness of the whole, and compensates for the vulnerabilities of other assets. This combined effects approach will lead to integrating existing and future operations across all the domains with an agile operational framework guided by human understanding. Because of this, the combat cloud is more of an intellectual construct with technological infrastructure than the other way around, and requires dominance of the electromagnetic spectrum at the appropriate times and places.

The actualization of the combat cloud will not be easy, and it is sure to upset many well-established operational habits and cultures. But if we are not the first to embrace and act on this concept, our adversaries will. We have too much at risk to let that happen. ✪

Footnotes

1 Author's note: the commander of Air Combat Command, USAF Gen. Herbert "Hawk" Carlisle, has made this observation regarding fifth generation aircraft in multiple public speeches over the past two years; I included this anecdote in my testimony before the Senate Armed Services Committee in November 2015.

2 Air Force Magazine *2016 US Air Force Almanac*, "Equipment: Aircraft Total Active Inventory (TAI)," (Arlington, Virginia: Air Force Association), May 2015, 33.

3 George Seffers, "Joint Aerial Layer Network Moves Towards Reality," *Signal*, June 1, 2013, http://www.afcea.org/content/?q=joint-aerial-layer-network-vision-moves-toward-reality (accessed August, 2016).

4 For more information on the Aegis Weapons System, see the US Navy's fact sheet on its functions, and utility in targeting and C2 activities: http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=200&ct=2 (accessed August, 2016).

5 Godard Space Flight Center, NASA, "Laser Communications Relay Demonstration (LRCD) Overview." (Washington, D.C.), March 18, 2016, https://www.nasa.gov/mission_pages/tdm/lcrd/overview.html (accessed August, 2016).

About The Mitchell Institute

The Mitchell Institute educates about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Series

Mitchell Institute Policy Papers is a series of occasional papers presenting new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

About the Author

Lt Gen David Deptula, USAF (Ret.), is the dean of the Mitchell Institute for Aerospace Studies. A decorated military leader with decades of experience in both combat and leadership roles in major joint military operations, he has planned, flown, and commanded air operations ranging from disaster relief efforts to major theater war. Deptula served as the principal air attack planner for Operation Desert Storm in 1991; was a Joint Task Force commander in Iraq in 1998-1999; led the initial air campaign of Operation Enduring Freedom in late 2001, and led several other significant joint operations. Deptula retired in 2010 after 34 years on active duty, serving in his last assignment as the US Air Force's first deputy chief of staff for intelligence, surveillance, and reconnaissance. He is a prolific author and analyst on aerospace power, and thought leader on defense, strategy, and ISR.