# The Combat Cloud

## Enabling Multidomain Command and Control across the Range of Military Operations

Jacob Hess, Major, USAF
Aaron Kiser, Major, USAF
El Mostafa Bouhafa, Major, RMAF
Shawn Williams, DIA

Wright Flyer Papers

**Air University**
Steven L. Kwast, Lieutenant General, Commander and President

**Air Command and Staff College**
Brian E. Hastings, Colonel, Commandant
James W. Forsyth, PhD, Dean of Academic Affairs
Bart R. Kessler, PhD, Dean of Distance Learning
Paul J. Springer, PhD, Director of Research
Leon J. Perkowski, Colonel, PhD, Essay Advisor

**Selection Committee**
Sean Atkins, Major
Amy R. Baxter, PhD
Ann Mezzell, PhD
John Minney, PhD
John Terino, PhD
Jonathan Zartman, PhD, Committee Chair

Please send inquiries or comments to
Editor
The Wright Flyer Papers
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426
Tel: (334) 953-3558
Fax: (334) 953-2269
E-mail: acsc.der.researchorgmailbox@us.af.mil

**AIR UNIVERSITY**

**AIR COMMAND AND STAFF COLLEGE**

# The Combat Cloud

## *Enabling Multidomain Command and Control across the Range of Military Operations*

Jacob Hess, Major, USAF
Aaron Kiser, Major, USAF
El Mostafa Bouhafa, Major, Royal Moroccan Air Force
Shawn Williams, Defense Intelligence Agency

Wright Flyer Paper No. 65

Air University Press
Curtis E. LeMay Center for Doctrine Development and Education
Maxwell Air Force Base, Alabama

*Project Editor*
Jeanne K. Shamburger

*Copy Editor*
Carolyn Broadnax

*Cover Art, Book Design, and Illustrations*
Daniel Armstrong

*Composition and Prepress Production*
Jeanne K. Shamburger

AIR UNIVERSITY PRESS

*Director and Publisher*
Lt Col Darin Gregg

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6026
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Air University Press

Accepted by Air University Press March 2017
and published February 2019

## Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University Press, LeMay Center, Air University, United States Air Force, Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

This Wright Flyer and others in the series are available electronically at the AU Press website: https://www.airuniversity.af.edu/AUPress.

# Contents

# Foreword

It is my great pleasure to present another issue of the *Wright Flyer Papers*. Through this series, Air Command and Staff College presents a sampling of exemplary research produced by our residence and distance-learning students. This series has long showcased the kind of visionary thinking that drove the aspirations and activities of the earliest aviation pioneers. This year's selection of essays admirably extends that tradition. As the series title indicates, these papers aim to present cutting-edge, actionable knowledge—research that addresses some of the most complex security and defense challenges facing us today.

Recently, the *Wright Flyer Papers* transitioned to an exclusively electronic publication format. It is our hope that our migration from print editions to an electronic-only format will fire even greater intellectual debate among Airmen and fellow members of the profession of arms as the series reaches a growing global audience. By publishing these papers via the Air University Press website, ACSC hopes not only to reach more readers, but also to support Air Force–wide efforts to conserve resources. In this spirit, we invite you to peruse past and current issues of the *Wright Flyer Papers* at https://www.airuniversity.af.edu/AUPress/.

Thank you for supporting the *Wright Flyer Papers* and our efforts to disseminate outstanding ACSC student research for the benefit of our Air Force and war fighters everywhere. We trust that what follows will stimulate thinking; invite debate; and further encourage today's air, space, and cyber war fighters in their continuing search for innovative and improved ways to defend our nation and way of life.

BRIAN HASTINGS
Colonel, USAF
Commandant

# Abstract

In March 2016 the Air Force released an operating concept for the combat cloud, defined as "an overarching meshed network for data distribution and information sharing within a battlespace, where each authorized user, platform, or node transparently contributes and receives essential information and is able to utilize it across the full range of military operations." The combat cloud represents the intellectual construct necessary to unify Air Force and Department of Defense efforts in pursuit of decision superiority and multidomain command and control (MDC2). However, these goals require that the combat cloud and associated network exhibit critical attributes such as the ability to be self-forming, self-healing, gracefully degradable, and redundant. Under this construct, the ability to collect data and integrate it in an open, adaptive information system will significantly enhance C2 and operational agility for the United States and its allies across the range of military operations (ROMO).

The combat cloud can enhance specific mission concepts across the ROMO. For example, the cloud can potentially improve joint fires through better use of fire support coordination measures, augment close air support and personnel recovery missions, and refine interagency coordination and coalition war-fighting management. While the inherent advantages of the combat cloud are many, the challenges that surround its successful development and incorporation into modern warfare are equally numerous, including interoperability and security issues and ensuring decentralized execution at the tactical and operational levels. Despite these challenges, the ubiquitous nature of data will not allow arbitrary lines to be drawn between domains in the future, and C2 must no longer be confined by such terms. Going forward, information must be generated, synthesized, shared, and accessible by all, for all, and through all domains; the combat cloud is the instrument to do so.

## About the Authors

*Lt Col Jacob P. Hess* is the chief of Personnel Recovery Aviation, Headquarters United States Air Force, Directorate of Operations, Special Operations and Personnel Recovery Division. As the chief of PR Aviation he manages Air Force oversight of fixed- and rotary-wing rescue assets and integrates personnel recovery operations, policy, and doctrine across the staff. Colonel Hess is a 2004 distinguished graduate of the United States Air Force Academy and 2006 graduate of the John F. Kennedy School of Government at Harvard University. In 2007 Colonel Hess completed Undergraduate Pilot Training and was assigned to Air Combat Command to fly the HC-130P Combat King. As an HC-130 pilot he has flown missions in support of Combined Joint Task Force–Horn of Africa, Operation Enduring Freedom, Operation Unified Protector, and other overseas contingency operations. (Colonel Hess was a major attending ACSC at the time of this paper's writing.)

*Maj Aaron W. Kiser* is a 2005 graduate of the United States Air Force Academy. He completed Undergraduate Pilot Training in 2006 and has served as an instructor pilot in the T-38C and later in the F-15E. Major Kiser has flown missions in support of Combined Joint Task Force–Horn of Africa, Operation Enduring Freedom, Operation Inherent Resolve, and other contingency operations. He is currently a student at the School of Advanced Air and Space Studies.

*Mr. Shawn Williams* serves as chief, Manpower, Directorate of Intelligence, United States Southern Command, Miami. Prior to his current position, Mr. Williams was the chief, executive secretariat, and executive officer for the Directorate of Intelligence. His major responsibilities included strategic planning and workforce management for civilian and military personnel while also providing direct support to the director and deputy director for intelligence. Mr. Williams retired from the United States Air Force in 2005 and received a bachelor's degree in sports management from Ashford University and a master's degree in military operational art and science from the Air Command and Staff College, Maxwell AFB, Alabama, in 2017.

*Lt Col El Mostafa Bouhafa* is a helicopter squadron commander in the Royal Moroccan Air Force (RMAF). He entered the RMAF École Royale de l'Air (ERA) academy in September 1996 and after completion of his master's degree in aviation attended the RMAF helicopter school in Rabat, where he earned his Gazelle SA-342L attack helicopter pilot license. In 2009, after years as an operator, Colonel Bouhafa earned a master's degree in mechanical engineering from the ERA and worked as an aircraft maintenance manager before returning to the attack helicopter wing. In 2014–15 he attended the Moroccan staff college and graduated first in his RMAF class. He is also a 2017 graduate of the US Air Force Air Command and Staff College. Considering communication as a key foundation of culture, Colonel Bouhafa speaks a handful of languages including Arabic, French, Spanish, German, and English. (Colonel Bouhafa was a major attending ACSC at the time of this paper's writing.)

# Introduction

In March 2016 the Air Force published its vision for a future network of data distribution and information sharing known as the combat cloud.[1] As the lead major command in the combat cloud operating concept, Air Combat Command defines the combat cloud as "an overarching meshed network for data distribution and information sharing within a battlespace, where each authorized user, platform, or node transparently contributes and receives essential information and is able to utilize it across the full range of military operations."[2] The combat cloud is an intellectual framework that provides unity of effort in the acquisition and development of future networked capabilities across the Air Force, Department of Defense (DOD), and supporting government agencies. The concept is pertinent to advance the DOD beyond stovepiped capability development and service-specific networks that currently lack interoperability. The combat cloud will also enhance the tactical performance, decision making, and command and control (C2) of complementary combat platforms of sensors, shooters, and network nodes that share real-time tactical information that will be essential for future multidomain operations.

Gen David Goldfein, chief of staff of the Air Force (CSAF), highlighted multidomain command and control (MDC2) as one of three focus areas during his tenure as CSAF. He emphasizes that

> this evolution in our command-and-control capabilities requires new thinking, new training, and perhaps new technologies or new ways to use older technology. We will need to integrate real-time information from a variety of sources—some non-traditional—and evaluate that information as fast as systems can process it. If an enemy blocks actions in one domain, we quickly "call an audible" to change the play and attack or defend from another. Future multi-domain operations will be high velocity, agile, and joint by their very nature.[3]

The combat cloud architecture will enable MDC2 by increasing the interoperability of existing networks, creating a foundation for new networks, and allowing real-time information to flow rapidly to and from war fighters and decision makers in order to make decisions faster than the enemy.[4] The combat cloud has applications and offers connectivity across the range of military operations (ROMO) but brings with it many challenges as well, both technical and organizational. Ultimately however, the combat cloud represents a decisive component of MDC2 and must be developed for the military to ensure information dominance and decision superiority on the battlefields of the future.

## Information and Decision Superiority

Scholars and analysts have suggested a myriad of names for the current age: the computer age, digital age, space age, and postindustrial age—just to name a few.[5] While there may be no agreement as to which term best defines the current period, much more consensus exists around the idea that industrial-era concepts and organizational structures have become inadequate to deal with the problems of the future. These dated constructs particularly no longer apply to multi-domain operations in the realm of information sharing and C2. Retired Air Force lieutenant general David Deptula, dean of the Mitchell Institute of Airpower Studies, has gone so far as to predict that "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."[6]

Unfortunately, in terms of information sharing and C2, the joint force is still organized in an industrial-era confederation of stovepiped agencies more focused on consuming than sharing. This structure poses a significant risk for future operations. Decisions that used to take hours or even days are now expected to be made within the span of minutes, yet the information and intelligence needed to make them is bound by the constructs and protocols of a previous age. For multidomain operations to be successful in the future, commanders on the battlefield must have access to information at the same speed the rest of the world is operating at. Without this capability, C2 and intelligence will continue to lag behind the ever-mounting informational demands of combat, and joint commanders will increasingly find themselves outmaneuvered or "outdecided" by the enemy. To be successful in the future, the joint force commander must take advantage of superior information and be able to convert it to superior knowledge, enabling "better decisions arrived at and implemented faster than an opponent can react." Joint Vision 2020 refers to this process as *decision superiority*.[7] Decision superiority gives joint force commanders not only an increased quantity but also quality of information, allowing them the distinct advantage of being able to preempt the enemy with decisive action. In this light, the combat cloud stands out as the instrument of choice for attaining decision superiority, enabling MDC2, and preventing the force of the future from becoming paralyzed by an increasingly clever and postindustrial enemy.

## Attributes of the Combat Cloud

With the relevance of the combat cloud concept established, it is beneficial to examine specific attributes the future network must possess. Cloud computing in general allows users to access their applications from anywhere through any connected device. A user-centric interface makes the supporting cloud infrastructure transparent to users. The result is a network of massively scalable data centers where computational resources can be dynamically provisioned and shared to achieve economies of scale. A network such as this, however, requires certain attributes to ensure connectivity. According to the Air Force Operating Concept, the network must be self-forming, self-healing, gracefully degradable, and redundant.[8]

To demonstrate these attributes, the combat cloud can be compared with the network functionality of a modern cellular telephone data network.[9] In an uncontested environment, these networks display the same qualities that will be demanded of the combat cloud in a contested and degraded operating environment. For example, when a network user is at home with access to a wireless Internet connection, the network capability is maximized with high reliability and connectivity. The network is self-forming because multiple users can transfer information on the wireless network if they are within range of the signal. When the user leaves home, the data connection does not cease functioning but simply degrades to a lower level of connectivity, such as that of a Long-Term Evolution (LTE) network. As the user transitions out of the area of LTE coverage, the connectivity then degrades to a third-generation (3G) capability. Information transfer can still occur, albeit at slower speeds. Network connectivity is not like an on-off switch but degrades gracefully depending on the location or distance from nodes and available services. Multiple nodes in various locations provide redundancy in case any particular node becomes unavailable. Finally, the user arrives at a destination that also has full access to a wireless Internet connection. The network transitions out of 3G coverage and back to the high-speed data capability of the wireless signal when within range, demonstrating a "self-healing" capability to return from degraded to full functionality.[10] The combat cloud must share similar network attributes for individual users and systems while functioning in a highly contested electromagnetic spectrum (EMS).

Future combat cloud capabilities will resemble those of modern day cellular networks. Instead of cell phones, combat cloud users will log in with weapon systems, such as the F-35, that act as shooters, sensors, and network nodes that will automatically push and pull mission-relevant and timely information to assist the user. Present-day network capabilities represent the same functionality the F-35 and other network nodes will require of the combat cloud in a contested EMS. To provide operating platforms with a robust architecture that communicates with relevant players, operates at reduced levels of connectivity, and recovers to full operability under dynamic operating conditions, the combat cloud must be intentionally developed over time. It must link information and hardware from existing networks to future networks, and developers must pursue future capabilities under an overarching construct. These capabilities are already under development and include various gateways allowing communication among Link 16, Link 11, intra-flight data link (IFDL), and other data links, as well as data translation devices such as the Battlefield Airborne Communications Node (BACN) and pods like TALON HATE that enable fourth-to-fifth generation fighter data sharing.[11] However, future data links must be designed with interoperability among existing and future systems in mind, thus minimizing the need for patchwork connectivity fixes.

Beyond fighter data links, the combat cloud possesses serious advantages in terms of enabling MDC2. The ability to collect data and integrate it in an open, adaptive information system that mitigates all classification's burdens will significantly enhance C2 and operational agility for the United States and its allies.[12] The combat cloud represents a profound shift from viewing platforms as simply consumers of information to that of sensors and from a series of individually networked platforms to a broader "system of systems" integrated across all domains.[13] A concept such as this connects domains in a fully symbiotic manner. Information and C2 of the future become inherently multidomain as they will be constructed from the ground up by inputs and sensors that span the domains and enterprise. Thus, the commander can leverage the full benefits of MDC2 by rapidly generating multiple solutions for a given challenge with an ability to shift among them.[14] The combat cloud promises to alter the multidomain environment as we know it in an existential way. To quote General Deptula, "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."[15]

As a means of emphasizing the decisive advantages the combat cloud brings in shaping the environment and force of the future, the next section highlights specific capabilities and missions chosen to represent the spectrum of requirements that exist across the ROMO. These are joint fires and fire support coordination, close air support (CAS), personnel recovery (PR), interagency coordination, and multinational partnerships. The combat cloud stands at the intersection of these capabilities and can establish the common operating picture needed to achieve effective MDC2 and decision superiority leading into the future.

## The Combat Cloud across the Range of Military Operations

### Joint Fires and Fire Support Coordination

The combat cloud will enable more efficient joint fires through improving the flexibility and use of fire support coordination measures (FSCM). Joint doctrine defines a FSCM as "a measure employed by commanders to facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces."[16] At the operational level, FSCMs are intended to deconflict and harmonize fires from multiple domains to achieve joint force targeting efficiency. However, the lack of flexibility, improper application, and lengthy dissemination process of certain FSCMs, such as the location of the fire support coordination line (FSCL) or the status of a kill box, represent deficiencies in joint fires that present risks for future joint force operations. Through advancements enabled by the combat cloud, future joint fires will feature more flexible and timely FSCMs that foster multidomain targeting, enhance nonlinear battlefield operations, and reduce the risk of fratricide.

There are numerous FSCMs, but two of the most critical measures facilitating joint fires in large-scale operations are the FSCL and the kill box. The FSCL is defined as a FSCM "to support common objectives within an area of operation; beyond which all fires must be coordinated with affected commanders prior to engagement, and short of the line, all fires must be coordinated with the establishing commander prior to engagement."[17] FSCLs are placed on land a certain distance in front of friendly land or amphibious forces. They are useful during linear battlefield conditions when a distinct line can be drawn between friendly and enemy forces. The kill box is also essential in joint fires coordination and is defined as "a three-dimensional FSCM with an associated airspace control measure (ACM) used to facilitate the integration of fires."[18] Kill boxes are established by the supported commander—in coordination with supporting commanders—and can be opened, closed, or color coded depending on varying fires deconfliction requirements.[19] According to Joint Publication (JP) 3-03, *Joint Interdiction*, "The goal is to reduce the coordination required to fulfill support requirements with maximum flexibility . . . while preventing friendly fire incidents."[20] FSCLs and kill boxes can be used in concert, where kill boxes located short of the FSCL can be opened for air interdiction (AI) with the approval of the coalition forces land component commander (CFLCC). Examples illustrating the improper application, lack of flexibility, and slow dissemination of updates to these FSCMs are numerous in Operations Desert Storm (ODS) and Iraqi Freedom (OIF).

In his book with author Tom Clancy, *Every Man a Tiger,* Gen Chuck Horner pointed out several application problems with the placing of the FSCL. During the initial static phase of ODS that preceded the ground offensive, "the FSCL was the border between Saudi Arabia and Iraq-occupied Kuwait."[21] It was important to place the FSCL not only close to enemy forces during static phases to facilitate more extensive AI but also along a visually significant landmark from the air to assist in airborne identification.[22] The initial FSCL placement during the air campaign was ideal because there were no friendly troops yet in Kuwait, and the border itself was clearly visible from the air. However, as the ground maneuver phase was initiated on 24 February 1991, Army units failed to coordinate their new respective FSCLs with one another during their advance, so "their FSCLs looked like teeth on a saw blade."[23] This configuration caused confusion over fires deconfliction between air and artillery strikes in adjacent ground force lanes until the Army battlefield coordination element eventually arrived at a single integrated FSCL solution with Third Army.[24]

A major miscalculation in FSCL placement on the part of Third Army headquarters was also a factor during the withdrawal of Iraqi tanks and troops during the final hours of ODS.[25] On the morning of 27 February, the Army moved the line north of the Euphrates River to facilitate Apache helicopter attacks on the roads north of Basra.[26] Only a few attacks were carried out, but the move took away valuable airspace and ground area that abundant and unemployed AI aircraft could have used to target Iraqi forces escaping across the river.[27] At 1900L that evening, US Central Command finally clarified the FSCL to correct the situation but only after the FSCL "had been pushed back and forth as the two services sought maximum flexibility for their own forces."[28] As a result, the fleeing Iraqi forces benefited from an internal coalition FSCM dispute, as well as the inability to clearly disseminate changing FSCMs.

The flexibility and timely dissemination of FSCMs proved troublesome during the fast-paced ground phase of ODS, and air-to-surface fratricide was also a concern. Ground force commanders placed the FSCL well forward of advancing land forces to allow for greater maneuverability and to minimize the chance of fratricide. A RAND study of ODS air operations revealed, "Because of the speed of the Coalition advance, airborne control elements and forward air controllers (FACs) improvised to apprise pilots of the fast-moving

FSCLs, which tended to quickly outrun their planned positions disseminated in the daily Air Tasking Order (ATO)."[29] Basically, pilots responsible for AI in support of land forces were forced to be more cautious in employing fires due to rapid changes and uncertainty of current FSCMs. During the ground force advance, it was not always possible to place the FSCL along a visually significant landmark from the air. Poor weather and visibility also added to the fog and friction. The fast, nonlinear ground advance was also among factors contributing to fratricide during ODS; 35 of the 146 US personnel killed in action were the result of friendly fire.[30] Some of these casualties were the result of friendlies advancing beyond the FSCL unknowingly. Without the aid of the Global Positioning System (GPS), some ground units simply lost their way in the desert and found themselves behind Iraqi positions.[31]

Issues with FSCMs emerged again in 2003 during OIF. Due to the near-simultaneous initiation of air and ground attacks, air support to advancing ground units needed to be more flexible, and a new method of employing kill boxes in coordination with the FSCL was implemented. Kill boxes short of the FSCL were closed for AI except when the ground commander opened them, and kill boxes beyond the FSCL were open by default except when a ground commander coordinated to have it closed.[32] The kill box interdiction system used in OIF allowed more flexibility in joint fires on either side of the FSCL than during ODS, but the FSCL placement again hindered air-to-ground operations. The CFLCC delegated control of the FSCL to US Army V Corps and I Marine Expeditionary Force (MEF), and V Corps often placed the line 100 kilometers in front of advancing troops to increase its ability to use organic helicopter and artillery fire support without having to deconflict with fixed-wing AI assets.[33] This greater freedom for ground organic fires came at the expense of efficient AI operations and cost the Air Force a full night of interdiction strikes against fixed targets inside the FSCL on one occasion.[34] Furthermore, I MEF was not satisfied with the great distance between the forward line of own troops (FLOT) and FSCL, and it employed its own version of the FSCL, called the battlefield coordination line (BCL). The BCL was identical in function to the FSCL, but it was much closer to friendly ground forces and intended primarily for Marine air assets in support of Marine ground forces due to the increased air-ground coordination required. The Marine-specific BCL remains a FSCM in joint doctrine today, which reflects the ongoing interservice struggle over the appropriate use of FSCMs that enable joint fires.

Regarding incidents of fratricide during OIF, the commander of the 1st Marine Division, Maj Gen James Mattis said, "We've got to commit ourselves to getting the maximum use out of this air-ground team and not find ourselves in a position where we don't have the most technologically modern equipment."[35] Army lieutenant general David McKiernan thought the heart of the matter was more about correct procedures, observing that "what really makes all the difference in mitigating the risk of fratricide has nothing to do with technology. It has everything to do with the tactical discipline of units, of using the right fire support coordination measures, the right tactical graphics and the right weapons control status and discipline of formations."[36] Each of these leaders identified pieces of the solution, but measures to improve the effectiveness, efficiency, and safety of joint fires must harness technology in combination with correct procedures and doctrine to ensure successful multidomain fires in the future. To address these issues, the need for a combat cloud that enables MDC2 of joint fires is readily apparent.

The combat cloud will allow decisive and flexible FSCM placement that can be rapidly communicated to joint forces in all relevant domains. Ground force commanders must have greater visibility of friendly and enemy ground positions to smartly use FSCMs. All air, land, and sea-based shooters must have the ability to see a common operating picture that delivers full awareness of changing FSCMs to maximize MDC2 without losing efficiency or risking fratricide. An improved combat network capability directly addresses the FSCM deficiency because it is primarily a problem of information networking. The combat cloud will enable FSCMs that are rapidly adjusted to changing conditions and disseminated to relevant forces.

Improvements in the selection, flexibility, and distribution of FSCMs will synchronize multidomain operations in a future operating environment characterized by rapid change. The very idea of a linear FSCM, such as the FSCL, may often prove to be overly rigid for future military operations. When utilized, the FSCL must take into account the improvement and proliferation of long-range ground force organic capabilities because the range at which ground forces close for battle continues to increase. Unfortunately, this trend also conflicts with the air component's preference for a relatively close FSCL that allows a larger area for AI. FSCMs that can be updated rapidly with multidomain awareness will enable agility in MDC2. In the previous example from ODS, fleeing Iraqi forces capitalized on a C2 error in the placement of the FSCL for a 12-hour period that allowed them to escape untargeted to the north of the Euphrates River. Using a common operating picture enabled by the combat cloud, future CFLCCs will be able to make better decisions regarding FSCL placement with instantaneous displays of friendly ground units and available fixed-wing AI assets. When deciding to update the FSCL or change a kill box status, the CFLCC will no longer be limited to preplanned locations, geographic features, or delays associated with the ATO cycle.

Effective FSCMs require high-quality information to enable operational agility. With its foundation in robust fighter aircraft information networking, the combat cloud concept enables the connection of disparate information systems such as Link 16 and Blue Force Tracking to deliver battlefield situational awareness to operational decision makers and shooters. Effective MDC2 of FSCMs will allow agile force employment. In OIF, for example, supporting airpower allowed the 101st Airborne Division and 3rd Infantry Division to fight only with their organic division artilleries rather than with two reinforcing artillery brigades as in ODS.[37] Increased trust in multidomain fire support allowed the Army to trade mass for agility. While technology alone is not a substitute for the principle of mass in war, it can enable agile fires effects when accompanied by rapidly disseminated FSCMs. Combat cloud capabilities will also address FSCM-related fratricide issues. FSCMs can be communicated in real-time to land forces with GPS, which could receive network-generated warnings when approaching the battlefield FSCL. Updates to FSCMs and kill box status can be immediately transmitted and visible to fixed-wing AI operators as they confidently shape the battlefield in advance of friendly ground force maneuvers. These advances will become even more important in future operations against more capable adversaries. Despite significant challenges, such as integrating coalition partners and security concerns, the combat cloud provides an overarching way forward in improving joint fires through FSCMs.

### Close Air Support

Close air support consists of air action against "hostile targets that are in close proximity to friendly forces and requires detailed integration of each air mission with the fire and movement of those forces."[38] The C2, prioritization, and execution of CAS has historically been a source of tension among military services. However, the combat cloud allows development toward MDC2 and enables tactical possibilities that shift questions from "what service should control CAS assets?" and "what is the best CAS platform?" to "how can we optimize CAS effects and harmonize CAS and AI efforts with ground force movements?" CAS is a complex problem that represents more than a specific military service responsibility or aircraft platform, and a combat cloud architecture helps focus thought toward achieving efficient MDC2 and effects rather than focusing on platform-specific limitations. Mission-related information from a variety of sources that is relevant, timely, and presented in a usable format must be accessible to aircrew and C2 nodes on demand; voice communications represent a current time bottleneck in passing large quantities of information that could potentially be expressed digitally. Finally, present doctrine regarding digitally aided CAS (DACAS) reflects the infancy of the promising information systems approach to CAS, but future combat cloud DACAS capabilities must be appropriately interfaced with the human domain to create confidence and trust.

Much debate surrounds the viability of C2 methods, but CAS effects can be achieved by a variety of platforms with efficiency and speed through a combat cloud construct. Regarding C2, joint doctrine asserts that the coalition force air component commander tasks capabilities and forces made available for joint tasking through the combined air operations center (CAOC) and appropriate service component C2 systems.[39] In the event that joint ground forces do not have an established command relationship, these forces use their respective C2 systems to submit CAS requests directly to the CAOC.[40] The requirement to use separate service component C2 systems provides ground forces with trust and familiarity with the process but does not represent the most efficient method. There is a historical tension between CAS efficiency (an air-centric perspective) and CAS effectiveness/response time (a land-centric perspective) when viewing the mission from a C2 perspective, and the combat cloud could bridge this divide. While centralized control and decentralized execution is paramount, no single C2 construct currently exists for CAS operations in multinational environments.[41] Considering the future will likely involve coalition warfare to a greater extent, the combat cloud has the ability to integrate service component C2 systems and coalition partners into an effects-based system with greater visibility and responsiveness. When it comes to integrating CAS C2 in support of ground troops, the heart of the matter is trust. Military services and coalition partners will resist centralized control and be more hesitant to make significant advances on the ground if they do not trust the CAS system to protect their forces. The combat cloud can offer greater process visibility, such as digital tracking and status updates of CAS requests to aid in overall battlespace awareness. With increased transparency and effectiveness of the C2 process, interservice and coalition trust will naturally evolve.

The speed of response to CAS requests is a critical factor in determining success on the ground, as illustrated during the Vietnam War. In November 1970, an Air Force report revealed the average Tactical Air Command (fighter-bomber) response time to CAS requests of 39.3 minutes exceeded the average battle duration of only 32.3 minutes for small unit engagements.[42] The introduction of armed OV-10s in a forward air controller (airborne) role reduced the CAS response time to only 8.1 minutes and resulted in a greater probability of friendly force victory and a lower probability of friendly casualties.[43]

With air superiority established, lighter platforms with increased loiter capabilities can orbit freely with weapons on call. Today, increased loiter times of the MQ-1 and MQ-9 in Iraq and Afghanistan offer similar effects.

Ground forces are conditioned to expect rapid effects that are enabled primarily by air superiority. However, future ground forces may require immediate CAS in contested and degraded air environments where persistent airborne weapon platforms are unable to loiter. Under these conditions, the response time for immediate CAS requests may increase, but the combat cloud can create efficiencies. For example, joint terminal attack controllers (JTAC) could use a tablet device to enter support requests into a cloud-based system, which is instantly observed by the air support operations center (ASOC) and CAOC. Requests would flow from the ASOC to the CAOC, where assets would then be tasked, alerted, or diverted to respond. The process is transparent, and the request status is immediately visible to all players at each level in the theater air control system. The JTAC can also input the ground commander's intent, desired effect, and targeting data that can be pushed to the applicable data link of the supporting platform. These capabilities eliminate critical minutes in the kill chain and push pertinent data to supporting platforms to maximize situational awareness.

Regarding the flow of information between ground and air assets, voice communications currently represent a bottleneck that can delay the ability to provide CAS effects. Voice aircraft check-in briefings, situation updates, and handoffs from on-station to inbound aircraft formations are time-consuming processes. Joint doctrine acknowledges that "DACAS has the potential to increase tempo, expedite the kill-chain timeline, minimize human error in information transfer, and reduce the risk of friendly fire."[44] However, DACAS is still cumbersome and requires extensive pre-mission planning to ensure that various data links and nodes are compatible. Each supporting CAS platform has varying DACAS capabilities with which JTACs and aircrew must be familiar to use effectively. As DACAS capabilities are refined, the interface of data presentation to human operators must be a key area of focus. The Joint Helmet-Mounted Cueing System and other helmet-mounted capabilities reach their full potential when pertinent data appears at the right time and in the right place. For example, when a JTAC establishes a new airspace control measure to help deconflict assets and joint fires, it can be visually displayed through helmet information systems to enhance spatial awareness. Digital targeting information displayed in the helmet complements the visual lookout and aids with an aircrew member's composite crosscheck inside and outside the cockpit. Networked CAS capabilities can also place more control of airborne sensors and weapons into the hands of ground personnel if necessary.

The Defense Advanced Research Projects Agency (DARPA) initiated a program called Persistent Close Air Support (PCAS) in 2010, with the intent to increase the ability of ground forces to control remotely piloted aircraft (RPA) and weapons. The program evolved to include multiple weapon systems like the USAF A-10C, Army AH-64 Apache, USMC MV-22, and unmanned systems.

PCAS takes advantage of commercial Android tablets given to JTACs and aircrew to reduce costs of upgrades to specific platforms, and the Marine Corps now deploys hundreds of tablets that run the operational app KILSWITCH (Kinetic Integrated Low-cost Software Integrated Tactical Combat Handheld). KILSWITCH allows aircrew and ground personnel to share common reference maps for any region in which they are operating and allows JTACs on the ground to pass digital 9-lines, display real-time collateral damage estimates, and even control sensor slewing and fire weapons from remotely piloted platforms.[45] The intent of the program is to use a "system of systems" approach for developing plug-and-play capabilities that are not platform-centric but provide tactical flexibility and timely effects.[46] While the Marine Corps is leading the charge in this program, its implementation may be slowed in the Air Force because these systems may prove more difficult to incorporate onto fighter aircraft (it would not be wise to ask single-seat pilots to operate tablets) and would likely remain separate from platform-specific operational flight programs (OFP). However, the approach reflects an innovative mind-set for pursuing DACAS precisely because of its plug-and-play nature and ability to be more flexible than aircraft OFPs. With joint force concurrence, there is also room to expand the program into the previously mentioned digital C2 network. Combat cloud connectivity can expand the PCAS program and assist with its integration into the previously described digital CAS request and approval network concept.

As CAS-related combat cloud capabilities are envisioned and refined, the importance of a proper interface for human data consumption cannot be overstated. Current doctrine recognizes that DACAS capabilities "do not replace the need for the verbal give-and-take that typically completes the tactical situation picture developed by aircrew and JTACs."[47] The underlying principle behind this thought returns to the themes of trust and the human domain. The efficiency and effectiveness of DACAS systems can be undermined because these methods of communication are unable to convey emotional information. A confident and reassuring tone of voice from an airborne operator on the radio instills trust in ground personnel in a way that digital information cannot. A methodical voice talk-on to a target with verbal confirmation from the shooter also builds trust. There is a tendency for Airmen to rely on technological solutions and to underemphasize the human elements of complex problems like CAS. In the pursuit of better CAS, combat cloud capabilities must be appropriately interfaced with human war fighters to maximize trust and realize the system to its fullest potential.

## Personnel Recovery

To gain decision superiority, the military must continue to seek applications for the combat cloud across the ROMO beyond just its offensive combat capabilities. One mission, unique to ACC and truly the Air Force as a whole, is that of dedicated personnel recovery. The Air Force is the only service to train and equip a dedicated PR force. Traditionally used for combat search and rescue (CSAR), these forces perform a host of other missions such as civil search and rescue, noncombatant evacuation operations, casualty evacuation (CASEVAC), mass casualty operations, infill and exfill of special operations or pararescue forces, and a multitude of other humanitarian assistance and disaster relief missions.[48] The spontaneous nature of many of these missions and the need for constantly updated information and dynamic connectivity present a truly valuable opportunity to leverage technologies such as the combat cloud to decrease the fog and friction inherent in any rescue mission.

The Air Force above all can benefit from a robust combat cloud capability within the PR arena due to the unique fact that the Air Force is the only service to have a dedicated and exclusively trained PR force. The reason for this is simple; within the Army, Navy, and Marines if there is an accident requiring search and rescue assistance, the event itself (in most cases) takes place in the domain in which these respective services are trained and equipped to operate. In other words, if a Sailor is lost at sea, the naval forces dispatched to search for that individual are already trained to operate in the sea domain. The same goes for the land forces; if a Soldier or Marine goes missing, the forces dispatched will be operating in their primary domain as well. For the Air Force, it is quite the opposite. Airmen are trained to operate in the air domain. However, in the case of a PR event, the isolated personnel (IP) by nature of having crashed or been lost are no longer operating within the air domain. Thus, USAF rescue forces must be equipped to operate across all three primary domains (air, land, and sea). This capability requires a much higher level of training and readiness and presents a valuable opportunity to leverage MDC2 through networking technologies such as the combat cloud.[49]

The challenges of operating in a multidomain environment are often exacerbated by the contested and high-risk settings in which many PR events such as CSAR occur. This situation is heightened by the fact that in many cases crews may have little to no time to plan the mission before being dispatched. As an example, the typical response time for USAF rescue crews executing a CASEVAC mission is measured in minutes from notification to launch versus hours or even days for more traditional Air Force missions. It is not uncommon for a crew to take off without knowing its final destination or to be retasked multiple times throughout an ongoing mission. Add to all this the need for diverse communication links with agencies ranging from an AWACS to Navy ships to PRC-112 survival radios, and the vital need for a common platform for information and communication sharing becomes decisive. This is precisely where the combat cloud can provide its greatest contribution to PR.

The combat cloud's ability to create an operating picture that is not only accessible to all, but built using all available assets is critical within the PR community. Often, a non-rescue-trained aircraft will be the initial on-scene commander during a PR event, whether it be a downed aircraft's wingman or an asset that happened to be nearby. When the first rescue aircraft arrives and takes over as rescue mission commander (RMC), the handoff of information is vital. The RMCs are typically A-10 "Sandy" pilots, highly trained at coordinating the flow and execution of rescue missions, but the initial handoff of information with non-rescue-trained forces can be cumbersome. This process is usually done via voice communications over the aircraft radios in a relatively unsecure fashion. The combat cloud represents a critical opportunity to exponentially increase the ability to pass accurate, in-depth, up-to-date information in a reliable and secure fashion. Additionally, it would give the RMC a platform to pass real-time threat updates and changes to the mission at one time to all assets involved, both rescue and support. Having this capability, as well as the ability to include RPA overhead imagery in the flow of real-time information, would fundamentally enhance the decision-making abilities of the rescue forces involved and mitigate a great deal of the fog and friction that make these interdomain missions so challenging. According to General Deptula, the "Combat Cloud will capitalize on the ubiquitous and seamless sharing of information among multi-domain weapon systems to rapidly exchange data between sensors and shooters to act as a cohesive whole."[50]

Other possibilities within PR where the combat cloud can provide fidelity and synchronization of C2 is between the rescue assets themselves. Air Force "rescue," as it is commonly referred to, is actually a combination of three unique weapon systems: fixed-wing HC-130s, rotary-wing HH-60s, and the pararescue Guardian Angel (GA) teams. These assets collectively form the rescue triad. For any given PR mission some variant of these three teams will operate in concert, parallel, or support, and coordination often becomes the most challenging aspect. As an example, an HC-130 may fly directly to an IP and insert a GA team to provide immediate security and medical treatment; meanwhile, the HH-60 will also be en route to recover the IP and team but along the way will need an aerial refueling from the HC-130. Sometimes these refueling tracks are precoordinated, but oftentimes due to the dynamic nature of a rescue mission as well as threats in the area, the refueling operations are coordinated ad hoc. The aircraft are frequently unable to communicate unless within radio range of each other; thus, coordination can become perilous if an HH-60 nears minimum fuel status and the HC-130 is still too far to coordinate a refueling. Likewise, once the HC-130 reaches the IP and deploys the pararescue teams, it may be forced to immediately return to provide critical fuel for the HH-60. The HC-130 crew also has a limited ability to glean information from the RMC to pass back to the helicopter and GA crews and help them form an operating picture of what awaits them. All of this could be mitigated with a common operating platform that would allow the HC-130, HH-60, and GA teams to communicate in real time, using each other as sensors to paint a vivid, real-time picture of the objective while coordinating their efforts in a much more synchronized manner.

The Air Force PR mission is a unique one. It is characterized by the ad hoc and spontaneous nature of the events that typically require a rescue. It is further compounded by the likelihood that any given mission will require operating in multiple domains. As such, the need for MDC2 and precise, real-time, holistic data becomes just as relevant as the traditional combat air forces (CAF) missions spanning the ROMO. The combat cloud represents a valuable tool in collecting and distilling the disparate pieces of information required to execute a complex rescue scenario. At the same time, the cloud is increasing communication among other valuable assets and leveraging their sensors as information nodes to further eliminate fog and friction. For a mission where every second matters, decision superiority can literally be a life-or-death matter. The combat cloud has the ability to allow decision makers to "be in more places than before" and gives them a decisive edge in gaining decision superiority.[51]

## Interagency Coordination

A policy paper published by the Mitchell Institute stated, "The 21st century demands a new, more agile, and integrated operational framework for the employment of military power, and a shift away from the domain focused structure of segregated land, air, and sea warfare."[52] By treating every platform as a sensor, the combat cloud MDC2 paradigm will give decision makers a reliable, secure, and dynamic system that ensures the effects are the focus, versus the actual platform utilized. The days of extensive stovepiping of information by various organizations within the defense enterprise, such as the intelligence community (notorious in compartmentalizing information), must be fundamentally restructured around a concept of information sharing, not hoarding. If the first part of the twenty-first century has taught us anything, it is that the days of interagency competition must be replaced with cooperation if the US defense enterprise is to remain relevant and efficient in the postindustrial age. The combat cloud provides just such an architecture to operationalize this concept.

When looking at the operability of the combat cloud in concert with agencies both within and outside the DOD, the Air Force can lead the way in providing the framework to ensure advances in C2 and intelligence, surveillance, and reconnaissance (ISR) are available to be shared with all relevant agencies. The sharing of information on these platforms is beneficial and critical in exploiting the disparate pieces of intelligence required to defeat the enemies of the twenty-first century, both state and nonstate. In the fight against violent extremist organizations, real-time communication and C2 within multiple domains are critical to effective control of the battlespace, and the combat cloud precisely enables this effect. Leveraging the advances in communication and information-sharing technologies that have come to fruition over the last 10 years, such as the combat cloud, will keep the United States ahead of potential adversaries like China and Russia.

Take, for instance, an organization such as the US intelligence community (IC). In most matters of information storage and sharing, the IC is still operating in an industrial-era mind-set. Information is typically stored on in-house secured networks; passing information to another agency requires a lengthy process of downloading, vetting, and often transcribing. The combat cloud will enable users within the IC (and truly the defense enterprise as a whole) to develop an information technology infrastructure that is fully functional with outside agencies, allowing the consolidation of data and information on secure yet accessible networks and ultimately reducing the time necessary to retrieve and pass vital information. Doing so will of course require complex algorithms capable of filtering, sorting, and archiving data in a way that is relevant and retrievable. But making data accessible across the interagency enterprise increases the number of highly trained analysts required to interpret and examine it. Analysis will also be aided by advances in metadata processing—a field that will continue to be more critical to efficiency and success in the information age. Heavy manpower will continue to be required to ensure efficient processing, exploitation, and dissemination of data. In 2014 alone, Air Force units generated approximately 1,600 hours of video per day, and the number of humans required to process, exploit, and disseminate this data is upwards of 100,000.[53] Sophisticated algorithms used in conjunction with the combat cloud will be pivotal in sorting through the masses of data but will give agencies the ability to share relevant information, reduce redundancies, and enable decision superiority across the DOD.

## Multinational Partnerships

Information and decision superiority cannot be achieved by a nation unilaterally. If the outcome of wars and battles is decided by the way a commander applies the "right type of force to the right targets at the right time with a rapidity the enemy cannot match," then in today's environment of multinational coalition building, the difficulty lies in optimizing MDC2 among partner nations.[54] In line with the principle of unity of effort, the more military efforts are coordinated, the more decisive and better those actions will be. Today's increasingly dynamic operational environment requires a full spectrum of multinational capabilities that span the domains—especially those that are typically coalition heavy, such as peacekeeping missions and humanitarian assistance. In that light, the US military will continue to find itself operating in close coordination with a wide range of coalition partners. These partners may include traditional allies such as North Atlantic Treaty Organization (NATO) partners, newer allies such as former Warsaw Pact members, developed and emergent states, or even ad hoc coalition partners during a natural disaster. This diversity requires coalition members to become part of a dynamic information-sharing environment and a specific C2 network. A transition to network-centric operations through a combined combat cloud that overcomes differences in tactics, training, and procedures (TTPs) will enhance unity of effort and ultimately lead to decision superiority in both US- and coalition-led engagements of the future.

It is critical that US partners be linked in both infrastructure and access to the combat cloud from the early phases of its creation and implementation. Doing so will assist in identifying and overcoming the inevitable shortfalls in hardware and software that can hinder operationalization. Furthermore, it will institute the framework whereby unity of effort can be streamlined through a timely, accurate, and relevant responsiveness that flows from the rapid, agile, and appropriate collection and dissemination of information and orders.[55] The concept of "every platform a sensor" is multiplied by the inclusion of coalition partners. Current systems, such as Link 16, provide only a small glimpse into the interoperability potential of coalition partners. Based on nodes in aircraft, vehicles, satellites, combatants, sensors, and terminals, the combat cloud will not be limited just to exchanging tactical data. It will also increase situational awareness and intelligence sharing, enhance MDC2, and intensify the effects each coalition partner brings to the operation.[56]

The combat cloud enables flexibility at the tactical, operational, and strategic levels. This capability will allow partner nations to efficiently adhere to the MDC2 systems and concepts used by the United States in a much more streamlined fashion.[57] A common system will allow any partner nation to quickly join or quit the network without any required configuration, reconfiguration, or additional and complicated settings or modifications to its own national systems. Seen in this light, coalition partners will begin to see the combat cloud as a solution to the problems of interconnectedness as opposed to simply another hurdle. By harnessing this dynamic information-sharing capability, MDC2 becomes streamlined at all levels whether it be a small collection of organic assets undertaking a joint operation or a large-scale heterogeneous coalition comprising many types of resources.[58] To that end, the combat cloud can enable the interconnected and resilient C2 systems required in the future and permit the United States and its partners to achieve information and decision superiority.

For the combat cloud to be effective, it must exist in a common computing environment that permits the United States and its coalition partners to share data and collaborate on, plan, prepare, and execute operations using shared security classification levels. Security is paramount. Coalition partners will be reluctant to adhere to a C2-centric network not adequately strengthened against the inherent vulnerabilities of interconnectedness. The system must be appropriately robust, effectively protected, and defended to prevent risks such as single-point and collective combat failure.[59] Moreover, the combat cloud's risks do not stem only from external sources; many of the most critical challenges may arise from within, especially in terms of specific partner nations. Pakistan, for example, is a key US ally in the fight against terrorism in Afghanistan and at the same time a key ally of China. In this light, not all members of a US-led coalition can necessarily be considered universal allies, and proper protocols must be instilled to ensure access is limited accordingly.

Interoperability is also required for a combined combat cloud. In the absence of compatible systems, laborious and inefficient workarounds have to be devised, often at some cost in coalition force effectiveness.[60] A familiar example of interoperability challenges that currently exists is the incompatibility of software for force-level planning used by the United States and NATO, known as the Contingency Theater Air Planning System (CTAPS) and the Interim CAOC Capability (ICC), respectively. To date, the only solution has been to manually redefine ATO messaging standards for communicating between the two systems, which is an incredibly cumbersome process.[61] Moreover, within the CAF the huge disparity in assets operated by the United States and its partners such as the F-35, Eurofighter, Typhoon, Rafale, E-7A Wedgetail AWACS, Eurohawk RQ-4, and other platforms shows that interoperability will continue to present significant challenges. Transforming all these individual weapon systems into collaborative elements of an interdependent coalition is precisely what the combat cloud can accomplish and is a prerequisite to achieving information and decision superiority.

A final key requirement for successful integration of coalition partners in a combined combat cloud is an increase in common training standards and operational tactics amongst partner nations. Requirements and TTPs must be agreed upon and formalized through inter- military agreements and training exercises in a highly deliberate fashion.[62] Well-defined standards and procedures will enable rapid and efficient implementation of the combat cloud and increase its utility for all involved throughout the ROMO.

## Challenges of Realizing the Combat Cloud

While the inherent advantages of the combat cloud are many, the challenges that surround its successful development and incorporation into modern warfare are equally numerous. As General Goldfein stated, "Linking operations moving at the speed of light with operations moving at the speed of sound requires we bring it all together: the skills of our Airmen, the vision of our leaders, and the audacity and technical innovation found throughout history."[63] The combat cloud stands as a potentially decisive medium for enhancing MDC2 in the future, but poses serious technical, security, strategic and cognitive challenges that must be overcome if the U.S. is to maintain information and decision superiority into the twenty-first century.

The first and most tactile challenge of the combat cloud is that of technology—specifically, interoperability between platforms. Due to a myriad of historic, bureaucratic, and political influences, the defense acquisition system has resulted in a wide disparity in C2 technology and interoperability across the military. Current Air Force systems such as the situation awareness data link (SADL), Link 16, IFDL, and multifunction advanced data link (MADL) do not offer full interoperability among Air Force aircraft without a variety of gateways—let alone full functionality with data networks of other services.

Meanwhile, the Army, Navy, and Marines are developing their own hardware and software combinations with no guarantee they will be compatible with any future network architecture. As Gen Hawk Carlisle, former US Pacific Air Forces (PACAF) commander, noted at a recent Air Force Association (AFA) convention,

> The Navy and the Air Force aren't necessarily on the same sheet of music when it comes to network collaboration and advanced tactical datalinks. . . . the Navy with NIFC-CA [Naval Integrated Fire Control–Counter Air] and the TTNT [tactical targeting network technology] and where they're headed, the Air Force in an LPI/LPD [low probably of intercept/low probability of detection] mind-set with MADL and IFDL, and then the network connectivity through gateways. . . . [This is] going to be a way of the future, but we've got to think about how we get to the next level, and we're not there yet.[64]

For MDC2 and the combat cloud to become a reality, connectivity must become as ubiquitous as electricity. Archaic and industrial-era acquisition processes must be fundamentally revamped to ensure interoperability is put at a premium and placed above other current and competing institutional agendas.

A key challenge that comes from ubiquity is security. Just as electricity requires the right kind of plug to access the electricity grid and keep its users safe, the combat cloud must too have protected access points focused on security. The challenge with this cannot be understated and requires a fundamental shift in the mentality of network administrators and architects. There must be an organizational pivot from networks that focus on "keeping the bad out" to ones that emphasize "letting the good in."[65] This becomes especially heightened in light of the ever increasing reliance on multinational coalition operations. Not only must the United States be able to communicate among its own assets and agencies, but it must have an ability to seamlessly and securely link with partner nations. Doing so requires a universally accessible but uniquely secure network that offers access to host and partner nations alike, while at the same time ensuring that access is tailored to the specific user at hand.

To that end, once the system has been designed to ensure only the right users "get in," there are two additional key considerations to avoid potential threats. First, the information must be attributable and users held responsible even down to the most basic level. Second, checks must be in place to ensure that designated users do not exploit their own legitimate access for illicit reasons. The former highlights one of the positive aspects of the combat cloud in that by cutting down on the stovepiping of information, data sharing between agencies, war fighters, and commanders becomes easier. However, to make this information sharing easier, individuals at the basic user level will be able to input information in real time that could immediately affect a war fighter's tactical decisions. This level of connectivity between the analyst and the war fighter has never existed in such a symbiotic manner, and thus new standards of accountability must be in place for the information uploaded. The accountability aspect of the combat cloud will be a challenge that must be infused early in development of the MDC2 culture to ensure efficient posting of information while also minimizing situations of incomplete or incorrect data being given to the war fighter.

The second challenge above deals with the exploitation of legitimate access. Kevin Haley, director of security for the leading software security firm Symantec, elucidated at a recent cyber security conference that

> a lot of the focus tends to be on very high-level vulnerabilities, but as we focus on more high-tech hacking and solutions, we tend to lose sight of the simplest avenues, such as stealing log-in details. . . . If I can get your log-in details, I don't have to worry about whatever security system the cloud provider has implemented. So if your data is in the cloud, you not only have to worry about vetting your employees who have access, but also the cloud providers' employees.[66]

Ultimately, this factor may prove to be the biggest challenge to MDC2 in the future, specifically in relation to coalition operations. Often, the United States pairs with partner nations that may not share or embrace US definitions of sensitive information. Yet, once granted access to a part of the combat cloud, a user potentially has access to *all* of the combat cloud. The amounts of data accessible would be nearly incomprehensible. Information and data have become the eyes, ears, and mouth of the Air Force and truly the military as a whole. These massive quantities of data are only going to increase, and as such, the combat cloud may well be the ultimate center of gravity of US and coalition military operations in the future. As the saying goes, if you put all your eggs in one basket, it becomes a target. However, a dispersed and defended C2 network certainly presents a more difficult target than the current physical C2 hub of the CAOC. Still, preventing user exploitation or espionage through legitimate access portals to the combat cloud will require a new level of vigilance and vetting, beyond even today's standards, for both US and partner nations.

Finally, one of the more metaphysical challenges associated with the combat cloud is that of information and permission "drunkenness."[67] Today's Air Force is often criticized as having strayed from its roots of centralized control and decentralized execution to one more akin to centralized control *and* execution. Increased connectivity has created a new level of interference in the execution of orders on the battlefield and led commanders on the front lines to feel the need to seek approval during critical portions of tactical execution. In fact, there is little debate that this phenomenon has occurred, but in light of MDC2 and the combat cloud the potential exists for it to be exacerbated. In pursuit of information superiority, commanders at the highest levels must resist the urge to insert themselves into minute tactical decisions; in doing so they will ultimately be at odds with decision superiority. If anything, the combat cloud represents an opportunity to break away from permission drunkenness by adding information to connectedness. Thus, the war fighter on the battlefield has access to exactly the same information as the commander in the operations center and enables that commander to once again trust his or her subordinates to execute their orders appropriately. Achieving this end, though, requires a cognitive break from the current trend toward centralized execution. Commanders at all levels must leverage connectivity as a means of passing information down, not simply pulling decisions up. This transaction is not risk free. Mistakes will be made, but the overall increase in decision superiority will be a key factor in successful integration of MDC2 and must be fostered and developed as a means of reaching a decisive edge over enemies of the future.

## Conclusion

Returning to General Goldfein's 2017 focus area paper, "To execute multidomain operations, commanders need an enhanced C2 system . . . one that refines our thinking about situational awareness, decision-making, and direction of forces."[68] The combat cloud stands out as a decisive enabler for MDC2 and will provide the common operating picture needed to achieve information dominance and decision superiority for the force of the future. This technology must be harnessed and ushered from concept to reality as it represents the type of multidomain thinking and collaboration required in the postindustrial age across the ROMO. The challenges are many and range from the technical to the organizational, but to remain a viable power into the future, the joint force must fundamentally alter its mind-set accordingly. Agencies must transition from an attitude of simply "keeping the bad out" to one that emphasizes "letting the good in." The ubiquitous nature of data will not allow arbitrary lines to be drawn between domains in the future, and C2 should no longer be confined by such terms. Going forward, information must be generated, synthesized, shared, and accessible by all, for all, and through all domains; the combat cloud is the instrument to do so.

## Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Lester and Vieira, "Combat Cloud Operating Concept," 3.

2. Ibid.

3. Goldfein, "Multi-Domain Command and Control," 1–2.

4. Lester and Vieira, "Combat Cloud Operating Concept," 4.

5. Geraghty, "Postmodern Warfare," 20–23. In his paper, Major Geraghty clearly distinguishes the concepts of postmodernism, postnationalism, and postindustrialism. The latter primary has to do with technology and its role in human affairs in the current era. As such, it is the term we have chosen to represent the current age throughout this paper.

6. Deptula, "Evolving Technologies," 4.

7. Department of Defense, "Joint Vision 2020," 62.

8. Lester and Vieira, "Combat Cloud Operating Concept," 23–24.

9. Russell Vieira (associate, Booz Allen Hamilton in support of ACC/A3C), phone interview with the authors, 15 December 2016.

10. Ibid.

11. Lester and Vieira, "Combat Cloud Operating Concept," 52.

12. Ibid., 20.

13. Deptula, "Evolving Technologies," 3.

14. Lester and Vieira, "Combat Cloud Operating Concept," 20.

15. Deptula, "Evolving Technologies," 9.

16. JP 1-02, *DOD Dictionary*, 87.

17. Ibid., 86–87.

18. JP 3-09, *Joint Fire Support*, A-9.

19. Ibid.

20. JP 3-03, *Joint Interdiction*, V-7.

21. Clancy and Horner, *Every Man a Tiger*, 491.

22. Ibid., 492.

23. Ibid.

24. Ibid., 493.

25. Ibid.

26. Gordon, *Generals' War*, 411–12.

27. Ibid., 412.

28. Ibid., 412–13.

29. Winnefeld, *League of Airmen*, 154.

30. Ibid., 155.

31. Ibid., 156.

32. Koscheski, "Counterforce Attack," 71.

33. Ibid., 76.

34. Ibid., 77.

35. Keeter, "Fratricide Mars U.S. Successes," 8.

36. Ibid., 10.

37. United States Marine Corps, *Army Field Artillery Relevance*, 8.

38. JP 3-09.3, *Close Air Support*, xi.

39. Ibid., II-1.

40. Ibid., II-4.

41. Ibid.

42. Sandborn, "Effect of Armed FAC," 56.

43. Ibid.

44. JP 3-09.3, *Close Air Support*, III-110.

45. Warwick, "DARPA Demonstrates All-Digital," 48–50.

46. Ibid.

47. JP 3-09.3, *Close Air Support*, III-112.

48. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-50, Personnel Recovery."

49. For a more in-depth discussion on the advent of PR as a service core function for the USAF, see Todorov and Hecht, "Air Force Personnel Recovery," 7–12.

50. Deptula, "Combat Cloud," 2–3.

51. Schanz, "Combat Cloud," 40.

52. Deptula, "Evolving Technologies," 1.

53. Maj Gen Linda Urrutia-Varhall, remarks, Air Force Association, "21st Century Warfare" Panel.

54. Otto, "Battlespace Networking," 2.

55. Ibid.

56. Ibid., 5.

57. Lester and Vieira, "Combat Cloud Operating Concept," 4.

58. Albert and Hayes, *Understanding Command and Control*, 34.

59. Lester and Vieira, "Combat Cloud Operating Concept," 4.

60. Hura et al., *Interoperability*, 49.

61. Ibid., 48.

62. Deptula, "Evolving Technologies," 7.

63. Goldfein, "Enhancing Multi-Domain Command and Control," 1.

64. Gen Herbert J. Carlisle, remarks, Air Force Association, "21st Century Warfare" Panel.

65. Pope, "Cyberspace."

66. Haley, remarks, "Security and Privacy in the Cloud" Panel.

67. Deptula, remarks, "Tomorrow's Future Wars" Panel.

68. Goldfein, "Enhancing Multi-domain Command and Control."

## Abbreviations

| | |
|---|---|
| ACM | airspace control measure |
| AFA | Air Force Association |
| AI | air interdiction |
| ASOC | air support operations center |
| ATO | air tasking order |
| BACN | Battlefield Airborne Communications Node |
| BCL | battlefield coordination line |
| CAF | combat air forces |
| CAOC | combined air operations center |
| CAS | close air support |
| CASEVAC | casualty evacuation |
| CFLCC | combined forces land component commander |
| CSAR | combat search and rescue |
| CTAPS | Contingency Theater Air Planning System |
| C2 | command and control |
| DACAS | digitally aided close air support |
| DARPA | Defense Advanced Research Projects Agency |
| DOD | Department of Defense |
| EMS | electromagnetic spectrum |
| FAC | forward air controller |
| FLOT | forward line of own troops |
| FSCL | fire support coordination line |
| FSCM | fire support coordination measure |
| GPS | Global Positioning System |
| IC | intelligence community |
| ICC | Interim CAOC Capability |
| IFDL | intra-flight datalink |
| IP | isolated personnel |
| ISR | intelligence, surveillance, and reconnaissance |
| JHMC | Joint Helmet-Mounted Cueing System |
| JTAC | joint terminal attack controller |
| LPI/LPD | low probability of intercept/low probability of detection |
| LTE | Long-Term Evolution |
| MADL | multifunction advanced data link |
| MDC2 | multidomain command and control |
| MEF | Marine expeditionary force |
| NATO | North Atlantic Treaty Organization |
| NIFCA-CA | Naval Integrated Fire Control–Counter Air |

| | |
|---|---|
| ODS | Operation Desert Storm |
| OFP | operational flight program |
| OIF | Operation Iraqi Freedom |
| PACAF | Pacific Air Forces |
| PCAS | Persistent Close Air Support |
| PR | personnel recovery |
| RMC | rescue mission commander |
| ROMO | range of military operations |
| RPA | remotely piloted aircraft |
| SADL | situation awareness data link |
| 3G | third generation |
| TTNT | tactical targeting network technology |
| TTP | tactics, techniques, and procedures |

## Bibliography

Air Force Association. “21st Century Warfare: The Combat Cloud” Panel. Air and Space Conference and Technology Exposition. National Harbor, MD, 15 September 2014. https://www.af.mil/Portals/1/documents/af%20events/Speeches/15SEP2014-AFA-CombatCloud-Carlisle-Hostage-UrrutiaVarhall-Fahrenkrug.pdf.

Alberts, David S., and Richard E. Hayes. *Understanding Command and Control*. Washington, DC: Command and Control Research Program (CCRP), 2006. http://www.dodccrp.org/files/Alberts_UC2.pdf.

Clancy, Tom, and General Chuck Horner. *Every Man a Tiger*. New York: G. P. Putnam’s Sons, 1999.

Curtis E. LeMay Center for Doctrine Development and Education. “Annex 3-50, Personnel Recovery,” 23 October 2017. https://www.doctrine.af.mil/Portals/61/documents/Annex_3-50/3-50-Annex-Personnel-Recovery.pdf.

Department of Defense. “Joint Vision 2020: America’s Military—Preparing for Tomorrow.” *Joint Force Quarterly* 25 (Summer 2000): 57–76.

Deptula, David A. “Evolving Technologies and Warfare in the 21st Century: Introducing the ‘Combat Cloud.’ ” Mitchell Institute Policy Papers 4, September 2016. http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

———. Remarks. “Tomorrow’s Future Wars” Panel. Air Command and Staff College, Maxwell AFB, AL, 12 December 2016.

———. “The Combat Cloud: A Vision of 21st Century Warfare.” Keynote address. Association of Old Crows, Washington, DC, 1 December 2015. http://media.wix.com/ugd/a2dd91_1550c5f873934b068afa8be3ad4ddd54.pdf.

Geraghty, Maj Jeff. “Postmodern Warfare: Beyond the Horizon.” Master’s thesis, School of Advanced Air and Space Studies, June 2013.

Goldfein, Gen David, CSAF. Letter to Airmen. CSAF Focus Area Paper no. 3. “Enhancing Multi-Domain Command and Control,” 10 March 2017. https://www.af.mil/News/Article-Display/Article/1108931/csaf-letter-to-airmen/.

Gordon, Michael R., and Gen Bernard E. Trainor. *The Generals’ War: The Inside Story of the Conflict in the Gulf*. New York: Little, Brown and Company, 1995.

Haley, Kevin. Remarks. “Security and Privacy in the Cloud” Panel. Digital Growth Summit, Los Angeles, 6 May 2016.

Hura, Myron, Gary W. McLeod, Eric V. Larson, James Schneider, Dan Gonzales, Daniel M. Norton, and Jody Jacobs et al. *Interoperability: A Continu-*

*ing Challenge in Coalition Air Operations*. RAND Report MR-1235-AF. Santa Monica, CA: RAND Corporation, 2000. https://www.rand.org/pubs/monograph_reports/MR1235.html.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as Amended through 15 February 2016).

Joint Publication 3-03. *Joint Interdiction*, 9 September 2016.

Joint Publication 3-09. *Joint Fire Support*, 12 December 2014.

Joint Publication 3-09.3. *Close Air Support*, 25 November 2014.

Keeter, Hunter C. "Fratricide Mars U.S. Successes in Iraqi Freedom Conflict." *Sea Power* 46, no. 9 (September 2003): 8, 10.

Koscheski, Michael G. "Counterforce Attack: Closing the Doctrinal Gap between AI and CAS in Air Force Counterland Operations." Master's thesis, School of Advanced Air and Space Studies, June 2006.

Lester, Jim, and Russell Vieira. "United States Air Force Combat Cloud Operating Concept." Langley AFB: Air Combat Command, March 2016.

Otto, Lt Gen Robert P., deputy chief of staff, intelligence, surveillance and reconnaissance, Headquarters United States Air Force. "Battlespace Networking: An ISR Horizons Future Vision." Staff Study, January 2015.

Sandborn, Richard T. "The Effect of Armed FAC (OV-10A) and TAC Air Close Air Support on Small Unit Ground Actions." OA Paper 70-9. Washington, DC: Headquarters USAF, November 1970.

Schanz, Mark V. "The Combat Cloud." *Air Force Magazine* 97, no. 7 (July 2014): 38–41. http://www.airforcemag.com/MagazineArchive/Magazine/2014/0714fullissue.pdf.

Todorov, Brig Gen Kenneth E., and Col Glenn H. Hecht. "Air Force Personnel Recovery as a Service Core Function: It's Not Your Father's Combat Search and Rescue." *Air and Space Power Journal* 25, no. 3 (Fall 2011): 7–12.

United States Marine Corps. *U.S. Army Field Artillery Relevance on the Modern Battlefield.* Quantico, VA: Marine Corps University, 2004. http://www.dtic.mil/dtic/tr/fulltext/u2/a494044.pdf.

Warwick, Graham. "DARPA Demonstrates All-Digital Persistent Close Air Support." *Aviation Week and Space Technology* 177, no. 25 (23 November 2015): 48–50.

Winnefeld, James A., Preston Niblack, and Dana J. Johnson. *A League of Airmen: U.S. Air Power in the Gulf War.* Santa Monica, CA: RAND, 1994.

AIR UNIVERSITY

INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE

AUP

AIR UNIVERSITY PRESS

https://www.airuniversity.af.edu/AUPress/