STATEMENT BEFORE THE SENATE ARMED SERVICES

SUBCOMMITTEE ON AIRLAND

The Future of All Arms Warfare in the 21st Century

David A. Deptula, Lt Gen, USAF (Ret)

Dean, The Mitchell Institute for Aerospace Studies

March 15, 2017

STATEMENT BEFORE THE SENATE ARMED SERVICES SUBCOMMITTEE ON AIRLAND: THE FUTURE OF ALL ARMS WARFARE IN THE 21ST CENTURY

March 15, 2017

Statement by David A. Deptula, Lt Gen, USAF (Ret)

Dean, The Mitchell Institute for Aerospace Studies

Introduction

Chairman Cotton, Senator King, and members of the Subcommittee, thank you for inviting me to present my thoughts on the critical issue of the future of all arms warfare in the 21st century. Our air and land forces have an extensive history of operating in conjunction with one another to accomplish military objectives. WWII and the Cold War posed some very significant challenges for the members of the greatest generation. As a result of their efforts, the United States prevailed against incredible challenges. It is now up to us to confront our own unique set of circumstances.

Our military situation today is stark. The United States faces a burgeoning number, and a greater spectrum of threats around the globe. At the same time we have declining resources allocated to meeting these threats. To successfully confront this dynamic array of dangers, we must optimize our military organizations and concepts of operation. We must evolve service relationships from ones of *interoperability*—a goal of the Goldwater-Nichols Act, to ones of full integration and *interdependency*. This is the next step in the evolution of our military.

A dollar spent on duplicative capability comes at the expense of essential capacity or capability elsewhere. Confused organizational structures lead to sub-optimal employment of forces already stretched too thin. Outdated service roles, missions, and concepts of operation yield costly, inefficient acquisition programs. Clearly, things have to change—security circumstances and fiscal pressures will no longer tolerate such conditions. We are not going to be able to blast or buy our way out of these challenges—we are going to have to think our way out of them.

I believe that if the United States is to succeed in protecting its core interests around the globe and deter aggression, we must have the strongest Army, Navy, Marine Corps, and Air Force in the world. However, fiscal realities dictate that the military must make difficult choices in balancing near-term operational readiness with longer-term needs. This demands much more clarity regarding goals and desired outcomes, with special emphasis on how we can best project effective, prudent power to negate threats that would oppose us in the 21st century.

Our Department of Defense and military services are conservative institutions. While highly capable they are slow to change, but to operate effectively in the information age, we must develop and capitalize on the new concepts of operation and organizations that new technologies enable. Dr. Thomas Kuhn, renowned American physicist, historian and philosopher, noted institutions only accept new paradigms when: 1) there is a paradigm crisis; 2) the old people of a given paradigm die off; or 3) change is forced from the outside.[1] We want to change before a crisis occurs, and cannot afford to wait for the "old-guard" to depart.

[1] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, University of Chicago Press, 1962.

In 1986 Congress was the outside institution that forced much needed change in the Department of Defense with the Goldwater-Nichols Act. It may be time to consider such action again. I commend Chairman Cotton, Senator King, and the rest of the Airland Subcommittee for beginning this conversation and initiating this series of hearings regarding the future of all arms warfare in the 21st century. It is a much-needed start.

I believe the biggest challenge our defense establishment faces is one of institutional inertia. We are well into the information age, yet our systems, organizations, and concepts of operations remain rooted in the industrial age of warfare. Our diplomatic, economic, and informational elements of our national security enterprise are also largely unchanged since the mid 20th century, and require more integration than ever before. We can no longer afford this misalignment—not only is it costly, but it also poses undue risk.

Change with respect to the military involves four principal factors—advanced technologies, new concepts of operation, organizational change, and the human dimension. *Advanced technologies* and the new capabilities they yield, enable *new concepts of operation* that produce order-of-magnitude increases in our ability to achieve desired military effects. *Organizational change* codifies changes and enhances our ability to execute our national security strategy. The final and essential element to progress is the *human dimension.* People are fundamental to everything we do, especially when it comes to leadership.

The 21st Century Security Environment

First, our defense strategy must contend with non-state and transnational actors; a rising economic and military powerhouse in China; a resurgent Russia; declining states—some with nuclear weapons; the increasing likelihood of nuclear weapons proliferation; evil actors of the most despicable nature; and a dynamic web of terrorism.

Second, the pace and tenor of our lives has been irrevocably altered by the acceleration of change. Global trade, travel, and telecommunications have produced major shifts in the way we live. Such developments are not isolated. Speed and complexity have merged, and now *permeate* the conduct of warfare. Consequently, one implication for future air and land warfare operations is that they *must* be able to respond rapidly and decisively anywhere on the globe at any time. As recent events have demonstrated, key security events now unfold in a matter of hours and days, not months or years. The window to influence such circumstances is increasingly fleeting.

Third, we have to contend with increasing personnel and procurement costs at a time when defense budgets are decreasing. Therefore, *the provision of flexibility of response across a wide spectrum of circumstances* should be foremost among the decision criteria we apply to our future military.

Fourth, we should acknowledge that deploying large numbers of American military forces onto foreign soil to nation-build vice accomplishing a defined mission and then leaving is counter-productive to securing our goals. Strategies centered upon occupation expose American vulnerabilities, often result in anti-American backlash and domestic disapproval, and create destabilizing effects within the very state or region they are intended to secure.

Fifth, we must actively pursue and invest in options we can use to counter the increasingly advanced anti-access strategies and technologies our adversaries are developing.

Precision weapons and stealth projected incredible lethality at the end of the Cold War. Those capabilities proliferated, and our adversaries are now equipping themselves with these systems, and seeking greater advancements. One quarter of a century later, it is foolhardy to assume U.S. forces will be afforded freedom of action in future engagements. Our strategies, planning assumptions, acquisition programs, and training need to account for more capable enemies.

Sixth, we need to challenge our adversaries' domination of public perception. We have to learn how to use the application of accurate, compelling information as a core element of our security apparatus. We are woefully inept at strategic communications and too often put ourselves in a reactionary versus proactive position in struggling to gain domestic and international public support.

Finally, information's value also extends past the media. Just as wireless connectivity, personal computing devices, and cloud-based applications are revolutionizing life in the civilian sector; these trends are also altering how our military forces project power. Faster and more capable networks and computing capabilities are turning information into the dominant factor in modern warfare. We need to understand that aircraft like the F-22 and F-35 are information systems far above and beyond being fighters that shoot missiles and drop bombs—they are sensor-shooters. F-22 operations over Syria validate this statement. Given this reality, we must now acknowledge that information and its management are just as important today as the traditional tools of hard military power—airplanes, satellites, infantry, warships. Information is the force evolving all weapon systems from isolated instruments of power into a highly integrated enterprise where the exchange of information and data will determine success or failure in the 21st century.

These facts have major implications throughout the military enterprise, particularly air and land operations—shaping key areas like doctrine, organization, training, materiel acquisition and sustainment, along with command and control. Top leaders in the policy community must adjust to the new realities of information age combat operations. Cold War and counterinsurgency paradigms will fall short when building, sustaining and employing military power in the modern era.

These trends provide a starting point for anticipating the future with which we will have to contend. Bluntly stated, all the services, Department of Defense (DOD) agencies, and the other elements of our national security architecture have been slow to recognize the emerging new security environment. Our focus has remained on traditional weapons platforms. We still have institutions and processes that were designed in the middle of the last century to accommodate what we now view—in retrospect—as a rather simple world of kinetics and traditional domains that characterized the Cold War. While nuclear threats have not gone away, we need to supplement our traditional focus on combined arms warfare with a broader "lens" that exploits non-kinetic tools and the cyber domain. Excessive emphasis on traditional weapon platforms associated with combined arms warfare runs the danger of under-investing in emerging non-kinetic instruments. We cannot relive the era of battleship admirals and cavalry generals that dismissed aviation as a passing fad.

Summarizing, the proliferation of technology, information flow, and the associated empowerment of nation-states, organizations, as well as individuals, presents one of the most daunting challenges our military has ever faced.

The Cornerstones of the U.S. Military: Services and Combatant Commands

Interservice rivalry is a vivid part of American military history stretching forward from the earliest days of our Republic. The most intense period of competition occurred at the close of World War II. Drawing on the lessons of that war and seeking to address years of agonizing political turmoil fueled by service rivalries, President Truman prodded Congress to pass the National Security Act of 1947 and its first amendment in 1949. This legislation established the fundamental postwar defense organization for the United States. They created, among other entities, a new Department of Defense (DOD), intended to unify the earlier separate Departments of War and Navy, and an independent air force as a third military department within DOD.

In 1958, additional legislation created the unified combatant commands that were designated as the headquarters for the conduct of actual warfare. However, this objective remained theoretical for many years, with the services remaining dominant in all aspects of organization, training, equipping, and planning. Land, sea, and air forces tended to operate autonomously. A service would develop weapons and equipment without regard to their compatibility with that of the other services. Army and Navy communications systems could not talk to one another; equipment was acquired by the Army and Navy that could not be loaded into Air Force cargo planes; and each service had its own doctrine for employing aircraft. This did not change until the Goldwater-Nichols Act of 1986. Its passage was prompted when years of interservice dysfunctionality manifested tragic results during the 1980 Iranian hostage rescue mission and the less than optimal invasion of Grenada three years later.

The Goldwater-Nichols Act was not intended to erase the differences in service philosophies and cultures. However, it was hoped that the unique characteristics and strengths of each service could be molded to complement one another so the whole would be greater than the sum of its parts. Jointness became the mantra of the Armed Forces after passage of the Goldwater-Nichols in 1986. So just what did the Goldwater-Nichols act do? And what is the proper meaning of jointness?

Here are the basics of the Goldwater-Nichols Act. First, no longer do the individual services fight our nation's wars as separate entities—the unified combatant commands do the fighting. The services organize, train, and equip what are called service *component* forces. These are then assigned to the unified combatant commands to actually conduct operations under a joint task force commander. The way America fights essentially boils down to this: individual services organize, train, and equip to master their principal domains of operation. The combatant commands assemble service and functional components to fight under the unifying vision of a joint force commander. It does not mean four separate services deploy to a fight and simply align under a single commander. It does not mean, "going along to get along." Nor does jointness mean everybody necessarily gets an equal share of the action. Jointness does not mean homogeneity. Jointness means using the right force, at the right place, at the right time—not an equal apportionment of all services.

Joint operations are often misunderstood. The strength in joint operations resides in the *separateness* of the services. Joint force operations create synergies because they capitalize on each services' core functions—skill sets that require much time, effort, and focus to cultivate. It takes 20-25 years to develop a competent division commander, a surface action group

commander, a Marine Expeditionary Force commander, or an air and space expeditionary force commander.

The beauty of the joint approach to warfare is that because every contingency will be different, a joint approach allows a joint task force commander to tailor-make a force optimal and unique to the particular contingency at hand. The service component force make-up for Operation Desert Storm (or the first Gulf War) was very much different than that required for Operation Allied Force (the air war over Kosovo and Serbia); which was very much different than that required for Operation Unified Assistance (the South Asia Tsunami relief); which is very much different than that required for Operation Inherent Resolve (the current counter Islamic State operation); and so it will be in the future.

Since the passage of the Goldwater-Nichols Act, a joint approach was first intended to move contingency organizations and operations from independent, de-conflicted, service approaches, to sustained *interoperability*. Today, we need to move beyond interoperability to *interdependency*, which means the service components rely on capabilities brought to the joint fight by other service components. The services must shed their historical predilection for self-sufficiency, or "owning" everything required to fight and win independently. The reason joint task force operations create synergies is because an *interdependent* approach allows each service to focus on, hone, and offer *its* core competencies. Services trying to control everything is unsustainable from a resource perspective and yields sub-optimized, compromised capabilities. Control of all the capabilities in a fight is the role of the combatant commanders when employing forces. It is far better for the services to invest and excel in their respective domains.

This idea is similar to doctors concentrating on healing the sick, and firemen focusing on rescuing people from burning buildings. Drawing out this analogy, such an approach means joint task force operations have at their disposal the abilities to both put out fires, and to cure sick people, no matter which is needed where—and both of these important tasks are being performed by specialists in their fields. The unfavorable alternative to interdependence is to have firemen also attempting surgical procedures, and physicians darting in and out of blazing structures between seeing patients.

Effective jointness relies upon having *separate* services; it is an *imperative* that service members understand how to best exploit the advantages of operating in their domains. Articulating the virtues and values of a member's service is being "joint." However, when a single service attempts to achieve warfighting *independence* instead of embracing *interdependence*, "jointness" unravels, trust is lessened, warfighting effectiveness is reduced, and costly redundancies and gaps will likely increase. We do not want to reduce the effectiveness of Goldwater-Nichols by allowing services to develop redundant "organic" capabilities, thereby rejecting the premise of joint warfighting.

With a common context of the challenges of the future security environment; the rapid advance of technology and information flow; and a proper understanding of joint operations, I now address the four specific requests for comment by the Subcommittee on the future of all arms warfare in the 21st century, and specifically air-ground operations.

1. An Assessment of the Future of Joint Force Air-Ground Combat Operations Against Peer And Near-Peer Competitors.

Beginning with Operation Desert Storm in 1991, in operations over the next decade, and into the beginning of the 21st Century, nascent joint force operations, combined with advanced

technologies and innovative concepts of operations aimed at achieving desired effects, have dominated conventional warfare. As a result, our adversaries and potential peer and near-peer competitors have watched and learned the lessons of what happens if the U.S. is allowed to project power into a region of interest. They have used this time to develop systems, concepts, and organizations to attempt to deny us in the future the advantages that our military has relied upon for success in the past.

One of the most significant changes in the evolution of modern warfare is the result of the impact of the combination of three technological changes: 1) modern intelligence, reconnaissance, and surveillance (ISR) yielding persistent multi-spectral ISR; 2) the normalization of the use of precision weapons; and 3) the dramatic improvement of system survivability (stealth). This combination has resulted in the reversal of the traditional paradigm of the use of air and ground forces to defeat adversary forces. The traditional warfighting paradigm of ground forces leading the fight supported by air forces has been supplanted by a construct where air forces supported by ground forces is often a much more responsive, effective, efficient, and less costly—in terms of both lives and dollars—manner in which to conduct warfare.[2] Validating this observation, a platoon leader during Operation Iraqi Freedom (Iraq 2003) at the leading edge of the push to Baghdad by the 1st Marine Expeditionary Force, wrote: "For the next hundred miles, all the way to the gates of Baghdad, every palm grove hid Iraqi armor, every field an artillery battery, and every alley an antiaircraft gun or surface-to-air missile launcher. But we never fired a shot. We saw the full effect of American air power. Every one of those fearsome weapons was a blackened hulk."[3]

In the context of this hearing, the point of raising this realization is not to start a doctrinal roles and functions fight between the Army and the Air Force, but rather to highlight the fact that capabilities change over time and the fundamental causes should be exploited to our Nation's warfighting advantage. This is particularly true in an era where near-peer adversaries are working hard to negate the warfighting advantages we have exhibited over the past quarter of a century.

To best meet the challenges of future peer and near-peer adversaries we must continue to exploit modern ISR, routine precision strike, improvements in survivability, and maneuver by focusing on two key essential actions. First, unshackle the service-based organizational paradigms of the past and embrace more functional joint organizational constructs that can be achieved by greater integration of these elements. Second, rapidly capitalize on the capabilities of the information age to actualize the ubiquitous and seamless sharing of information across systems in every domain as a vision of the Department of Defense.

We are at a critical juncture in history. We are 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 weapon systems needed to achieve desired effects. In World War II it took months of time, thousands of Airmen, and hundreds of aircraft to neutralize a single target. Today we can find, fix, and successfully engage multiple targets with a single aircraft within minutes.

---

[2] For a comprehensive treatment on this phenomena see, *The Urgent Necessity to Reverse Service AirLand Roles,* by Price T. Bingham, Joint Forces Quarterly 84, 1st Quarter 2017.

[3] Nathaniel Fick, *One Bullet Away: The Making of a Marine Officer* (New York: Houghton Mifflin, 2005), p. 289.

Since the introduction of mechanized technology 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 "mass" remained an essential aspect of force application. In the last century, military missions, historically restricted to land and sea, expanded into the air, space, and underwater domains. However, the ability to project power globally was wholly dependent upon mechanized technology.

In the 21st century, we face another technology-driven inflection point that will fundamentally reshape what it means to project power. Advancements in computing and network capabilities are empowering information's ascent as a dominant factor in warfare. No longer will it be sufficient to focus on simply managing the physical elements of a conflict—planes, satellites in space, tanks, amphibious elements or ships at sea. These individual platforms have evolved from a stove-piped, parochial service alignment to a loosely federated "joint and combined" construct today. To be effective in the future, these same forces must become a highly integrated enterprise collaboratively leveraged through the broad exchange of information.

Said another way, desired effects of military operations 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 command and control are core mission priorities.

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 maximizing 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, and in every service component, dramatically enhanced situational awareness by transforming masses of disparate data into decision-quality knowledge. This represents an evolution whereby individually networked platforms transform into a broader system of systems enterprise integrated through domain and mission agnostic information linkages.

This approach will not only change the way we define new requirements, but also more importantly, the way we think about; operations; intelligence; command and control; and support. A distributed, self-forming, all-domain Combat Cloud that is difficult to attack and self-healing when attacked, significantly complicates an enemy's planning and will compel enemies to dedicate more resources toward its defense and offense. In its ultimate instantiation, Combat Cloud will be: 1) strategically dislocating to any challenger; 2) provide conventional deterrence to a degree heretofore only achieved by nuclear weapons; and 3) will enable operational dominance in multiple domains.

Turning this vision into reality will require a significant effort. While many militaries are evolving toward informationized forces, the integration and assimilation of related capabilities is incomplete. Forces 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 of combined arms warfare construct developed in the industrial age of warfare. Program oversight

efforts within the DOD are also lagging—with antiquated industrial age governance impeding information-age endeavors.

Any assessment of the likely landscape of future conflict with peer and near peer adversaries must recognize that no matter what type of engagement occurs, the outcome will increasingly be determined by which side is better equipped and organized to collect, process, disseminate, understand, and control information. Furthermore, with budget austerity as the new normal our military needs to devise more effective and efficient means to secure desired effects with existing capabilities. The Combat Cloud concept is a paradigm that allows us to do this.

If we, along with 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. The concept of the Combat Cloud stands as a framework to empower this vision.

In the current program-centric budgetary world of DOD, 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 that are often kluged-together to pass as "joint." This is why DOD needs to embrace the vision of attaining a joint and combined Combat Cloud. Future combined and joint operations will require new concepts and practices for how to join together and command and control desired effects; and distributed battle, intelligence, and surveillance networks.

Commanders must change the way they view networks and information systems. Rather than value only 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. Indeed this 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 involves numerous challenges. It will require a review of, and appropriate changes to doctrine, organization, training, material, leadership, personnel and education, facilities, and policy to define a "template" to guide modernizing policy, acquisition, and concepts of operation; seeking collaborative solutions among the services; moving from measures of merit that replace cost per-unit to cost per-desired effect; eliminating stove-piping of kinetic and non-kinetic options; developing reliable, robust, and anti-jam data links; creating sufficient diversity of employment approach to avoid single points of failure; and realizing automated multi-level security to ensure coalition participation.

2. The Conduct of Offensive Operations Against Adversaries in Anti-Access, Area Denial Environments.

Over the last quarter-century that the U.S. has dominated military operations, our air forces have been fighting in relatively permissive airspace. Similarly, our ground forces have been engaged in counterinsurgency and counterterrorism fights with little exposure to modern high-tech threats. Combat operations against peer and near-peer competitors in anti-access, area denial environments will demand a new, more agile, and integrated operational framework for the employment of U.S. military power to succeed. While terrorism and insurgencies have proliferated more than traditional conventional combat since 9/11, a failure to be ready for state

on state warfare would be catastrophic. We must be ready to engage and succeed across the entire spectrum of conflict.

Warfare against an adversary in an anti-access, area denial environment of the future will be very different than the experience of the members of the U.S. military today.[4] Heavy armor; barrages of theater ballistic missiles; rear areas under attack; surface to air missiles ranging hundreds of miles; smart mines; quiet submarines interdicting friendly shipping; anti-satellite capabilities shutting down GPS; non-stealthy friendly drones falling from the sky like rain—are all more likely to characterize warfare in the future than will the treatises of the recent past on sharing "three cups of tea," and "eating soup with a knife."[5]

Furthermore, if we are to succeed in fighting in anti-access and area denial environments, critical areas that require serious attention are not getting it. Potential opponents capable of creating an anti-access, area denial environment are capitalizing on electronic warfare (EW) tools and techniques to do so. The proliferation of high-end electronics has made offensive cyber operations and EW the modern military equalizers. Russia is now routinely attacking Ukraine and the Baltic states via the net. As a nation we are losing hundreds of billion dollars a year of commercial/military value due to Internet thefts. Many of China's newest weapons systems look eerily familiar to U.S. systems—they should, they stole our designs. However, in the DOD, getting traction for electronic warfare requirements and investment is painfully slow, and inadequate to properly prepare us for the future. Here is what the DOD electronic warfare strategy states in its introduction, "...our EW work force is currently fragmented and ill-equipped to dominate a pacing competitor."[6] In 2014 the Defense Science Board highlighted the insufficient attention paid to electronic warfare by all Services, and recommended a 75 percent markup in electronic warfare investments over the next 5 years—from $3 billion a year to over $5 billion a year. Electronic warfare is no longer just an enabling capability—it is a survival capability.

We need sufficient numbers of advanced munitions to prevail in the high-end anti-access, area denial fights of the future. Today we are we are running low on these kind of munitions due to their regular use in conflicts in southwest Asia. We also need to pay attention to the numbers and capabilities of the people required to accurately target these advanced weapons. In Desert Storm only about 5 percent of all the weapons employed were precision-guided, but we had over three times the number of targeteers in our intelligence force than we have today where precision weapons now make-up over 95 percent of weapons employed from our combat aircraft.

However, these needed resources are going unfunded because there is little public awareness of the problems we face relative to the reduction in resources allocated to Defense. As a result, the hollow force that the 2011 budget control act and sequestration it imposed will not be readily apparent until those forces are required. What is so devastating about the 2011 budget control act—and not obvious in a 20 second sound byte—is that it is now affecting U.S. capability to provide rapid response sufficient to meet the demands of our national security strategy. Said another way, we have a growing strategy-resource mismatch. The dichotomy

---

[4] Over 80 percent of the active duty U.S. military has joined since 9/11/2001, so their experience is primarily in the counterinsurgency and counterterrorism environments of Iraq and Afghanistan.

[5] *Three Cups of Tea: One Man's Mission to Promote Peace - One School at a Time*, and *Learning to Eat Soup with a Knife: Counterinsurgency Lesson from Malaya and Vietnam* were popular books reinforcing the primacy of counterinsurgency warfare that affected the first decade of the 21st century.

[6] *The Department of Defense Electronic Warfare Strategy*, 2017, p1.

between what we say we want to accomplish, and what we can actually accomplish is growing. Without action to eliminate sequestration, that mismatch will get worse. I believe it is vitally important to remember that the first responsibility of the United States government is the security of the American people. As the preamble of our Constitution states, the federal government was established to first, "*provide* for the common defense" and subsequently to, "*promote* the general welfare." Recent decisions have confused this prioritization, with sequestration taxing defense spending at a rate greater than twice its percentage of the total federal budget. It is time to return to the first principles of our Constitution and get our priorities straight.

The most important element in the U.S. military's ability to fight and win in any conflict in the future—much less against one in an anti-access, area denial environment—is restoring the readiness that has been robbed from it by the irresponsible budget control act of 2011. No amount of innovation, reorganization, or restructuring will allow the U.S. military to succeed in meeting its national security objectives without proper equipment, tools, people, and training essential to execute its assigned missions. Air Force Chief of Staff, Gen David Goldfein succinctly described the criticality of the role of the Congress in this regard when he stated, "There is no enemy on the planet than can do more damage to the United States Air Force than us not getting a budget."[7]

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. Accordingly, 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 Fusion Warfare based on building a Combat Cloud—moving beyond combined arms and into an approach of *combined effects power*.[8] The kind of combined effects resident in a unified ISR, strike, maneuver, and sustainment complex integrated across the electromagnetic spectrum.

The Combat Cloud inverts the paradigm of combined arms warfare—making information the focal point, not the domains in which the military operates. 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.

Capabilities from any domain can contribute to precision effects in and across all five domains. In order to maximize operational agility against advanced adversaries, actions must be designed to include integrated operations and effects in more than one domain. Desired effects must be well timed, synchronized, immediately assessable, and scalable. Soldiers, Sailors, Airmen, and Marines must collaborate with joint and coalition counterparts and with networked experts worldwide to synthesize combinations of kinetic/non-kinetic, lethal/non-lethal, direct/indirect, and permanent/reversible effects, striking targets in hours, minutes—or seconds.

To succeed against an adversary in an anti-access, area denial environment you must encourage the Department of Defense to develop and embrace concepts that have as their basis, the linking of information-age aerospace systems with cyber, sea, and land-based capabilities in

[7] Gen David Goldfein, remarks to the Center for Strategic and International Studies in Washington, D.C., Feb 23, 2017 as reported in the Air Force Association Daily Report, Feb 24, 2017.

[8] For greater insight into this concept for thinking about warfare in the 21st century see; Rokke, Drohan, Pierce, *Combined Effects Power,* Joint Forces Quarterly 73, 2nd Quarter 2014.

ways that will enhance their combined effectiveness, while compensating for their individual vulnerabilities.

3. The Key Attributes of a Modern, Fully Integrated Joint Air-Ground Theater Joint Task Force Capable of Decisive Offensive Campaigns

By definition, anti-access, area denial environments will complicate, if not hinder, our ability to conduct offensive operations. As potential adversaries expand their anti-access, area denial capabilities, our ability to conduct offensive operations is reduced, especially if we fail to keep pace by inadequately investing both qualitatively and quantitatively in advanced technology. I have the fullest confidence that our armed forces can currently achieve any military objective they are given. However, the sacrifices in casualties our service members will have to make to achieve those objectives are increasing. As our forces get older, our capabilities relative to modern threats are declining, while investment to reverse these negative trends is still not adequate.

Standoff ranges imposed by area denial capabilities degrade the effectiveness of long-range sensors in a highly contested environment. To overcome these limitations, the Air Force must build an integrated network of air, space, and cyberspace-based capabilities and leverage other service contributions from all domains to achieve a robust, reliable, redundant, sustainable means of sensing, commanding and controlling, and employing effects to meet mission objectives. Underlying this set of capabilities is the Combat Cloud operating paradigm where every platform is capitalized upon as both a sensor as well as an "effector." This vision will enable more rapid and effective decisions at the tactical, operational, and strategic levels of war and will provide us an operating advantage that will be difficult for any adversary to overcome. Key capability development areas in the Air Force to achieve this kind of operating paradigm include:

a. Data-to-Decision: The objective is to fuse data from cloud-based sensor-effector networks into decision quality information for use at the tactical as well as operational levels of war. Machine-to-machine automation will be integral to allow for the rapid turning of data into information and knowledge to inform decision-making. Big data analytics; incorporation of all-source information; and sensor-to-sensor cueing must become the norm, not the exception in creating a combat cloud.

b. ISR Collect and Persistent ISR: These are capabilities that focus on multi-domain alternatives for placing the right sensor in the right place at the right time.

c. Penetrating Counter-air (PCA): PCA maximizes tradeoffs between range, payload, survivability, lethality, affordability, and supportability to achieve penetrating counter-air effects in anti-access, area denial environments. Establish PCA as a network nodal element to relay data from penetrating sensors enabling the employment of standoff or stand-in weapons.

d. Agile Communications: This is increase in the resiliency and adaptability of integrated networks. Focus on responsive, adaptable network architectures with functionality across all platforms, weapons, apertures, and waveforms operating in a highly contested environment.

Each of the services are working to create architectures to rapidly sense, collect, process, and analyze data; turn it into knowledge; and then disseminate it among their component forces to create desired effects. The DOD vision must be to integrate each of the service architectures

to create a joint Combat Cloud where information and knowledge is shared in a ubiquitous and seamless fashion.

A fully integrated joint air-ground theater joint task force capable of decisive offensive campaigns must be capable of disrupting key adversary systems, especially air defenses. A prerequisite to effective joint operations—a sine qua non—is the need to gain and maintain air superiority. In all recent operations, we have gained air superiority rapidly and have not faced threats denying us freedom of action. In a contested environment, air superiority will be continuously important and will pace all other operations.

The recently released Air Force Air Superiority Flight Plan states, "The Air Force's projected force structure in 2030 is not capable of fighting and winning against the array of potential adversary capabilities." This is an official statement from the United States Air Force, and that statement should concern you, because without air superiority there can be no successful land (or sea surface) operations.

Developing and delivering air superiority for the highly contested environment in 2030 requires a multi-domain focus on capabilities and capacity. Importantly, the rapidly changing operational environment means the military can no longer afford to develop weapon systems on the linear acquisition and development timelines using traditional approaches.

Air superiority—as well as other military capability development—requires adaptable, affordable and agile processes with increasing collaboration between science and technology, acquisition, requirements and industry professionals. Failure to adopt agile acquisition approaches is not an option. The traditional approach guarantees adversary cycles will outpace U.S. development, resulting in "late-to-need" delivery of critical warfighting capabilities and technologically superior adversary forces.

In the future we must possess an agile operational framework that enables the integrated employment of joint and 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 capability 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.

The reconnaissance-strike group (RSG) organizational construct posited by Doug Macgregor is a step in the right direction in this regard. This concept would provide the Army an organizational entity that at its core is interdependent with the other service components—particularly the Air Force—for its success. Conversely, it provides the impetus to the other services to develop and provide capabilities to dramatically enhance the effectiveness of the RSG as a means to better secure joint task force objectives.

Beyond the RSG, all the services, and combatant commands need to be focusing on moving to a future operating paradigm of the Combat Cloud. The Combat Cloud is not simply a network, but an operating concept that integrates every warfighting platform as a node in the ISR, strike, maneuver, and sustainment complex. Because of its nature as a distributed sensor-

shooter-effector composite, it will require command and control standards and sets of operating procedures different from that which the services employ today. It must possess a command and control structure capable of operating within multiple domains and across multiple echelons while allowing operational units to operate interdependently with shared knowledge in a contested area. U.S. forces can continue to operate, to move the fight, by understanding commander's intent and guidance through mission directives or orders. The command and control structure must be adaptive and responsive enough to support decentralized execution with authorities delegated to the lowest echelon practical.

In the future, increases in threat warfighting capability that can hinder or deny traditional U.S. warfighting advantages will grow. In an era of constrained resources, the best bet for defeating modern threats is implementing the Combat Cloud concept. This approach will not only change the way we define new requirements, but 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—it is the entire enterprise of sensors; shooters; effectors; and connectors, all part of a cohesive, coherent whole and it must extend across all operating domains.

4. The Challenges Of Deploying And Sustaining Expeditionary Forces Across The Globe

The major challenges of deploying and sustaining expeditionary forces across the globe are two-fold. First there is the difference in the nature of air and land forces. Air forces can be rapidly deployed and employed anywhere in the world in a matter of hours even from thousands of miles away. Land forces, unless predeployed to the specific area of concern, take weeks or months to deploy depending on the size of the force elements required.

Second, the explosive growth in the ease and speed at which ideas and technologies are created and spread around the world has yielded a new, more unpredictable threat environments. Rapid advancements in the capabilities of our potential adversaries, notably in electronic warfare, cyber, drones, and long-range precision attack, all present unique challenges and expose vulnerabilities. Our ability to deploy and sustain forces to areas needed for deterring or countering malicious actors or adversaries is becoming ever-more contested and subject to reach by surface-to-surface and surface-to-air weapons.

The spread of advanced technologies, enhanced by rapid advances in computing power, places increasingly sophisticated ballistic and cruise missiles, integrated air defense systems, submarines, anti-ship missiles, guided rockets, fourth and fifth-generation aircraft, as well as advanced space and cyber capabilities in the hands of potential adversaries. The range and scale of possible effects with these new capabilities present a new military problem set that threatens the U.S. and allied expeditionary warfare model of power projection, freedom of action, and maneuver.

The necessity of deploying and sustaining expeditionary forces across the globe is absolutely fundamental to the U.S. national security strategy. There are two enduring tenets of our national security strategies over the years regardless of Administration party affiliation. One, that we will maintain sufficient forces and capabilities to engage around the world to encourage peace and stability to prevent conflict. Two, that in the event that conflict is unavoidable, we will maintain the ability to fight and win in more than one conflict at a time and do so away from U.S. territory.

In order to be able to accomplish both of these fundamental tenets, each of the services requires a set of robust, capable, and ready forces to establish a rotational base sufficient to

sustain operations. To do that the Air Force uses its "Air and Space Expeditionary Force" (AEF) structure to maintain sufficient numbers of rotational base forces to engage in regions around the world to shape and maintain peace and stability. AEFs provide joint force commanders with ready and complete air and space forces to execute their plans.

In the most demanding anti-access/area denial scenarios, the U.S. will be challenged to do what it has become accustomed to doing: building up combat power in an area, sustaining that force, performing detailed rehearsals and integration activities, and then conducting operations when and where desired. AEFs provide a construct for the potential of better teaming with the Army on a regular and recurring basis to organize, prepare, and train together so when it does come time to fight, our air and land forces present seamless capability.

During the 2000/2001 Quadrennial Defense Review (QDR) where I was the lead of the Air Force QDR team, I suggested to my Army counterpart that we consider assigning and teaming Army warfighting units with Air Force AEFs specifically for this purpose. I was told by him that the Army was a garrison-based force and didn't need to train for or practice for expeditionary deployments. That was before 9/11 and much has transpired since then.

With the potential of the interdependent RSG, and its ISR and strike components that parallel Air Force capabilities, it may be time to move toward greater air land interdependency by aligning RSGs with AEFs at some point in the future. The characteristics of the RSG as lighter; more agile; more mobile; and more interoperable than current Army warfighting organizational structures, opens the possibility of much greater synergy with the air, space, and cyber capabilities of the Air Force. RSGs matched with AEFs provide the basis for a step increase in the partnership between air and land force organizations in the future.

Ten AEFs provide the *framework* to achieve sufficient expeditionary aerospace forces to sustain rotational base requirements and personnel tempos to meet the dual requirements of our security strategy. The *key* to Air Force expeditionary force structure is to ensure that those ten AEFs are structured, equipped, and *equivalent in capability and capacity* for each of the Air Force's mission areas: gaining control of air, space, and cyberspace; holding targets at risk around the world; providing responsive global integrated ISR; rapidly transporting people and equipment across the globe; and underpinning each of these unique contributions with robust, reliable, and redundant global command and control. Aerospace capability does not stop with expeditionary assets. Space, ISR, cyber, national missile defense architecture, inter-theater airlift, and others, provide the foundation upon which the AEF structure stands. To meet the Nation's security challenges of the future, the Air Force will require sufficient force structure to maintain both an adequate rotational base of expeditionary capabilities, as well as its foundation—that level of force structure does not exist today. Currently, the Air Force does not have ten equally capable AEF's—it "borrows" those forces in training to make those preparing to deploy whole.

In the face of the expanding set of threats around the globe, the United States government has elected to fund fewer resources to meet them.[9] At the same time, our aerospace capabilities have reached an inflection point. Last year we celebrated the 25th anniversary of Operation Desert Storm—the first Gulf War. Your Air Force has been at war not just since 9/11/2001, but since 1/16/1991. After over 25 years of continuous combat operations coupled with budget

[9] In 2009 the U.S. spent 4.6 percent of its gross domestic product (GDP) on defense. In 2017 the U.S. spent 3.2 percent of its gross domestic product (GDP) on defense.

instability and lower-than-planned budget top lines have made the Air Force *the smallest, the oldest, and the least ready force in its entire history*.

Yet, our nation faces an ever growing and evolving list of challenges. While each of them drive an increase in the demand for aerospace power, the Air Force has to deal with unpredictable and eroding budgets that have shrunk force structure, as well as the defense industrial base upon which it heavily relies.

Today we have 59 percent fewer fighter squadrons than during Operation Desert Storm in 1991 (134 in 1991, 55 today). We have 30 percent fewer people, and 37 percent fewer total aircraft. At the height of the hollow military of the 1970's, and when President Reagan took office pledging to rebuild it, our Air Force aircraft averaged 12 years of age. Today the *average age* of Air Force aircraft is over 200 percent older...28 years.

The Air Force is operating a *geriatric* force that is becoming more so every day. Bombers and tankers over 50 years of age, trainers over 40, fighters and helicopters over 30—for comparison purposes the average age of the U.S. airline fleet is about 10 years…and they don't pull 6 to 9 "Gs" on a daily basis as do our fighters. Pilots are qualifying on the same bombers and tankers that their *grandfathers* qualified on.

In the 70's, nearly half our military planes could not fly because there were no spare parts and proper maintenance. It is just as bad today. Between 2009 and 2018, the US military will sustain budget cuts totaling over $1.5 trillion dollars. Many of these cuts have been arbitrary and not reflected in strategy or analysis. Yet, the demand for airpower keeps growing while the Air Force is seriously underfunded. This is perhaps the greatest challenge to deploying and sustaining expeditionary forces across the globe.

Conclusion

The challenge before us is to transform *today* to dominate an operational environment that *is rapidly evolving*, and to counter adversaries who *are rapidly advancing in capability*. The 9/11 commission report's now famous summary that the cause of that disaster was a "failure of imagination" cannot be allowed to be repeated across our security establishment.

I finish with a plea for new thinking. In the face of disruptive innovation and cultural change, the military can maintain the status quo, or it can embrace and exploit change. I suggest that the latter is preferred. Our services need to learn better how to rapidly adapt new technology to the innovative concepts of operation that technology enables. Our intelligence community, military, and other security institutions will suffer if their internal organizations fail to adapt to new, disruptive innovations and concepts of operation.

Just as combat tomorrow will look different than it did yesterday, so too should the military with which we prosecute it. We should take maximum advantage of the asymmetric capabilities America possesses with her air, space, and cyber forces operating in conjunction with her land and maritime forces in innovative ways. A concerted focus on further developing and expanding these forces would serve the United States well, as they are uniquely positioned to underpin the kind of defense strategy and force structure appropriate to America's future.

One of our most significant challenges is the structural and cultural barriers that stifle new ideas that challenge the status quo. That is the challenge for not just our military, but for all the other pillars of our national security architecture. We must challenge our institutions to have an appetite for

innovation—and a culture that rewards innovative solutions. I encourage you to embolden our military to seek out, experiment, and test new concepts of organization and operation.