No. 9
February 2017

The Mitchell Forum

Assured C2 for Airpower: A Proposed US Air Force Cyber Strategy

By Lt Gen Stan T. Kresge, USAF (Ret.)

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact on current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

Over the past 25 years, the US Air Force has enjoyed unchallenged command and control (C2) of its forces, with adversaries unable to target or affect its networks or systems to a degree that has impacted operations. Unfortunately, the service cannot continue to count on that advantage going unchallenged, due to the enormous importance of cyberspace capabilities and networks in today's US and coalition combat operations, and growing adversary cyber capabilities around the world.

The US and its allies are heavily dependent on cyber to sustain a functional, responsive C2 network with extensive reachback capabilities. But the Air Force is behind the curve today, states the author, who is a former vice commander of Pacific Air Forces. The Air Force continues to treat cyber as a separate subject area from standard operations. Critical C2-enabling capabilities of cyber, as a result, are often underemphasized.

This paper examines the nexus between cyber and C2 in modern combat operations, how to reduce airpower's vulnerability to cyber attacks seeking to penetrate networks, and how to use cyber to effectively preserve our C2 advantage. The Air Force needs to protect its "assured C2" advantage, the paper notes, which is based on a fuller understanding of intelligence, adversary cyber capabilities, and their potential impact on the ability to command and control aerospace power in combat. By improving key USAF capabilities, training practices, and organizations, the author argues, the service will better prepare its Airmen to utilize cyber in 21st century warfare, and protect its critical C2 advantage.

Introduction: Modern Airpower, C2, and Cyber

During the past 25 years of combat operations, the US Air Force has enjoyed unchallenged command and control (C2) of its forces. Enemy forces have not targeted our C2 and supporting cyber networks and systems, to any degree that has impacted operations. In all likelihood, we will not be as fortunate again.

Because of this, there is ample reason for concern about the state of the traditional Theater Air Control System (TACS)—down to individual weapons systems, which connect to other US military services and partner nation C2 systems, and are supported by myriad reachback organizations. In addition, the US relies heavily on a functional, responsive global transportation C2 network. All of these elements of C2 today are highly dependent on cyber, and adversaries will attempt to attack and degrade these networks in future wars.

Assured C2 rests on a foundation of intelligence, a full understanding of an enemy's cyber capabilities, and their potential to impact our ability to command and control aerospace power.

Despite this, it is troubling that the impact of determined cyber attacks on Air Force C2 remains largely unknown. As such, it is difficult to prepare for a problem set we don't really understand, and there are serious potential consequences in store for this lack of preparation. In a high-end shooting war, even limited C2 disruption would mean young Airmen would not return from their missions, and serious disruptions could lead to mission failure.

One reason the Air Force is behind the learning curve is because cyber is treated as a separate subject area in operations. Cyber conversations tend to focus on sexier aspects of the mission, such as how it can be utilized in offensive opportunities. The critical C2-enabling aspects and capabilities of cyber, as a result, are often under emphasized. This paper aims to highlight the nexus between cyber and C2. While the title refers to a "cyber strategy," the critical issue in talking about effectively using cyber in the future is its role in preserving C2. As noted above, cyber pervades our C2 apparatus. We must think about cyber differently, and this paper aims to encourage practitioners, C2 force providers, and others to prepare for the inevitable future where adversaries will seek to defeat us by attacking this critical capability. Cyber, in any conflict, will be everyone's business.

This paper will explore a proposed "cyber strategy" by examining several elements, the first being the importance of "assured C2," as it is vital to the ability to fly, fight, and win in a contested cyber environment. Assured C2 rests on a foundation of intelligence, a full understanding of an enemy's cyber capabilities, and their potential to impact our ability to command and control aerospace power. Three "pillars" support the goal of assured C2: First, cyber defenders and defenses must be improved. Second, C2 force providers and practitioners must play a part in solving the problem, and adopt more survivable systems and processes, implement better training, and build capabilities with state of the art tactics, techniques, and procedures. Finally, the Air Force should move to reduce C2 vulnerability wherever it is found, and move to introduce caution in areas where this dependency could increase as it could dramatically impact the success of our forces in future conflicts.

My Introduction to Cyber

In 2011, as the 13th Air Force commander, I participated in a major US Pacific Command exercise called Terminal Fury, which featured simulated cyber threats to our ability to effectively command forces. The experience was an eye-opening one.

During the first day of the exercise, participants learned a cyber "red team" had penetrated our Combined Air and Space Operations Center (CAOC) network and was in the process of stealing the Air Tasking Order (ATO), which did not bode well for our success in the exercise. Further, the exercise control team had to tell us about this development, because we had no other way of knowing. The blue forces could do nothing about the cyber theft of the ATO under way, other than shut down the command center. Fortunately, the exercise ended in three days, and we were thankful the event was merely an exercise. Determined to avoid humiliation in future exercises, Pacific Air Forces (PACAF) had to do its homework, and tried to come to grips with this thing called "cyber." What we discovered was troubling.

In fairness to Air Force cyber defenders, they did not have the chance to play in the exercise in question. But if they had, they possessed no capability to monitor our CAOC's internal network. Exercise participants also lacked the ability to monitor our network during the event. The Airmen tasked to maintain our C2 systems weren't trained to defend them, but they weren't alone. Command and control operators were not trained to recognize and react to cyber threats, either.

After the experience, the PACAF team knew it needed to change operations in order to be less vulnerable, but the way forward was not clear at the time. Guidance was nonexistent. Not only did we lack solutions, we didn't understand the problem well. No one seemed to know what a real adversary could do to our ability to command and control air, space, and cyber power in a high-end war.

The most important epiphany from our experience in Terminal Fury was that cyber is in fact a contested domain, and enemies using cyber are aiming at C2. Cyber defense of C2, as a result, is not just the concern of cyber professionals.

The most important epiphany from our experience in Terminal Fury was that cyber is in fact a contested domain, and enemies using cyber are aiming at C2. Cyber defense of C2, as a result, is not just the concern of cyber professionals. Commanders and C2 practitioners had to be part of the solution, as cyber was clearly now everyone's business. By the time the next Terminal Fury kicked off, 13th AF hired contractors to train our systems maintenance personnel and install network sensors, and partnered with our 24th AF Air Forces Cyber (AFCYBER) teammates. Collective awareness of the cyber threat was greatly elevated. The "red team" had a fight on its hands, and due to the added attention and capabilities, "blue forces" at least were able to detect simulated intrusions, and reduce the theft of information.

The PACAF CAOC's post-exercise celebration was tempered by the understanding that we had only taken the first steps. We knew that the cyber red team didn't fight with gloves off. We didn't know what a real adversary could do, but knew that the exercise didn't test the complete vulnerability of theater C2, just our own CAOC.

What About Logistics? And Why Cyber?

After the exercise, I was taken aback when the red team showed us a screen shot of a base-level fuel management system. They mentioned they weren't allowed to penetrate this system because it was outside the scope of the exercise. But the lesson was clear: they easily could have.

This reveals another oft overlooked vulnerability. Fuel, munitions, spare parts, personnel—the logistics infrastructure vital to aerospace power, another equally critical C2 realm, is supported by far less secure networks and systems. A senior Air Force cyber professional recently told me "a 17 year old in his basement could cripple Air Force logistics."

Because of these experiences and insights, I began to think differently about cyber, and its role in supporting air and space power. In response, I have come up with the following "cyber strategy" as a basic blueprint for improving how the US Air Force can better understand and leverage this critical capability.

Any strategy must tie ends, ways, and means together by identifying and articulating a goal (the "ends" part of the equation). The joint doctrine definition of cyberspace is "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] This describes what cyber is to the US military, writ large. Air Force doctrine lays out what we do with this capability (tasks such as cyberspace support, defense, and force application).[2]

It is estimated that some 95 percent of all the cyber-related USAF personnel, infrastructure, and money is devoted to building, maintaining, and securing Air Force networks and systems. But why have we made this enormous investment in cyber? The answer is so that we can effectively command and control our capabilities. If you consider C2 involves directing operations, and organizing, training, and equipping forces to conduct operations, then every Air Force network, server, and computer is enabling C2. This is why, when someone says "cyber," I hear "C2."

The term "C4"—or command, control, communications, and computers—has fallen out

of vogue, but there is a case for its return to our lexicon. You can't effectively command if you can't control. You can't control if you can't communicate. And operations are in great jeopardy if cyber networks and systems become vulnerable. This is not to discount the value of the Air Force's contribution to offensive cyber operations and network exploitation. But failure in those endeavors will not lead to defeat in the next war. A C2 breakdown will. Therefore, the proposed strategy outlined below focuses on the C2-enabling aspects of cyber. The strategy's purpose is "assured C2." Assured C2 is simply defined as the ability to ensure our forces can fly, fight, and win in a contested cyber environment (or CCE).

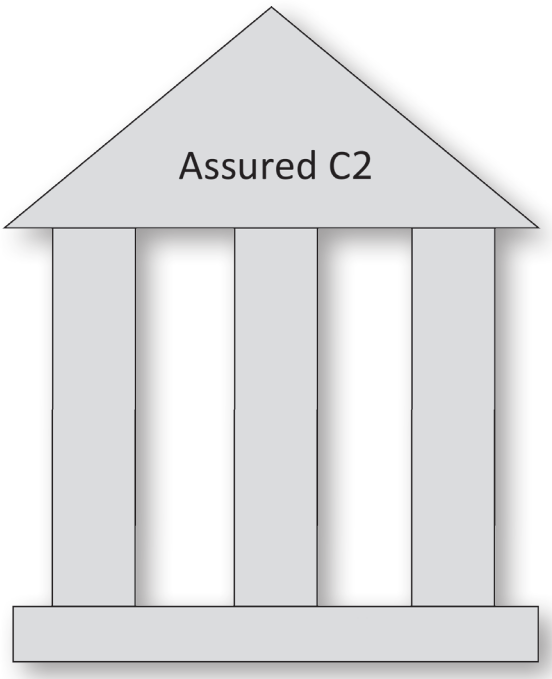

Figure 1: The strategy's goal—assured command and control

The Strategy's Base: Foundational Intelligence

In order to successfully harness cyber's potential, the Air Force must work to better understand the problem set we face. This is why "foundational intelligence" forms the base of this strategy, because this commodity informs actions needed to achieve assured C2.

Foundational intelligence answers a key question—what would be the impact of an enemy's cyber attack on our ability to command and control forces? Exercises involving cyber red teams are valuable, but red teams provide limited threat replication. They are not permitted to break systems, corrupt data, or worse, manipulate data in such a way we would be unaware our forces were acting on false information. In addition, C2 exercises typically don't test the entire theater air control and logistics system. We must move to address this training gap.

I have asked for years why exercises don't normally target these systems. Answers ranged from casual dismissals ("What are you worried about?") to uneasy alarm ("We'd all die."). In fairness, this is a hard question to answer, because the proper answer requires extensive and continuous interaction between experts in the following areas:

- The current and future cyber capability and intent of potential adversaries.
- US military cyber operations and defenses.
- C2 systems, including logistics systems, down to the equipment level.
- Experts in US Air Force and joint force C2 operations.

We need to ask where in the Air Force are experts in these disciplines working together to define this critical problem? This is a rhetorical question, and one not readily answered by quickly examining present systems and organizations. Absent foundational intelligence, our strategy for assured command and control in a CCE rests on shaky ground.

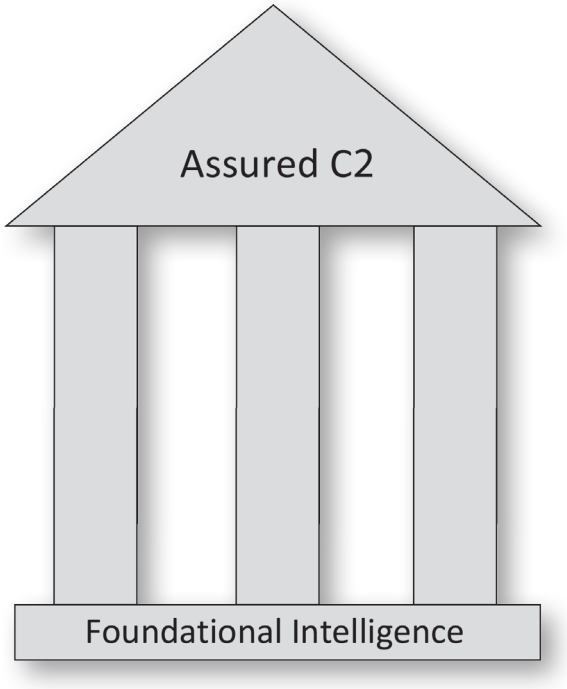

Figure 2: Foundational intelligence is a must for an effective cyber strategy

Cyber Defense

The first pillar of an effective cyber strategy includes current cyber defense efforts. The work of our AFCYBER defenders at 24th Air Force should be lauded and commended, for starters. Ongoing Air Force initiatives are encouraging, and include the USAF Cyber Task Force investigation of weapons system vulnerabilities, and Air Force Research Laboratory's (AFRL) work on proactive cyber defenses. If any action should be taken, it should be for USAF to reinforce and accelerate all work on active and passive defenses.

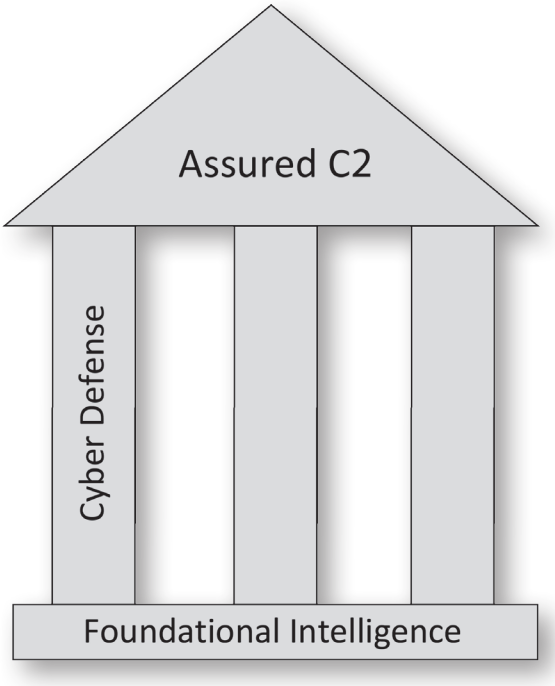

Figure 3: The first pillar—robust cyber defenses to thwart attacks on C2

However, we must not pin our hopes on cyber defenders and defenses alone. Command and control systems, processes, and personnel must be prepared for an inevitable enemy cyber attack. Effective preparation, in cyber as in all other domains, will be critical to prevailing over the enemy in actual combat.

Command and Control Enhancements

Command and control practitioners and force providers must anticipate C2 needs in a CCE. First, we must adopt a new C2 paradigm. Second, C2 processes must be designed to function in a CCE. Third, C2 practitioners must be trained to operate in a CCE. Finally, we must arm these practitioners with current and effective tactics, techniques, and procedures.

Air Force C2 doctrine offers the following warning: "Commanders should seriously consider the ability of adversaries to affect the communications required for effective centralized C2 of airpower and tailor plans accordingly."[3] This point is worth remembering. Our current C2 paradigm assumes availability of long range, secure, reliable, and high volume communications. Therefore the USAF approaches operational planning with two basic steps—first, build a plan, and second, install necessary systems for its success. Facing contested C2, we need to consider a new paradigm:

Step 1) Understand our C2 capability and limitations.
Step 2) Build a feasible plan.

The goal of assured C2 does not mean assured C2 as we know it or wish it to be. The Air Force must start by answering that key question of what foundational intelligence is, depending on the problem set or operational challenge. Then, as needed, we must make necessary doctrinal changes and changes to the associated investments in organizing, training, and equipping.

Command and control systems and processes must continue to function in a CCE, and as such cyber defense should be built into our C2 systems. During another exercise 13th AF participated in, which focused on cyber vulnerabilities, the 13th AF team was shocked to discover the number of outdated critical patches within our command center. Under a new paradigm, cyber vulnerabilities should generate as much attention as the health of our aircraft fleets.

With the threat of cyber theft growing, we should design our systems and processes to segregate the most valued and critical information from the rest—so if the enemy obtains the less valuable information, the damage will be minimized. If system destruction is threatened, we should be prepared to rebuild capability. If logistics systems cannot be adequately hardened, then we should design logistics processes to function without them. If the impact of a CCE is intermittent C2, then distributed C2 may be necessary. If the impact is low volume communication, a different approach may be required depending on the scenario.

A critical underpinning of a USAF assured C2 strategy is training C2 practitioners. Air Force doctrine Annex 3-30 offers prudent advice to prepare for challenged cyberspace, communications, or degraded and contested

environments. The question is: are our commanders, various staffs, and C2 operators trained to make these preparations? I suspect an honest assessment of our joint force air component commanders (JFACCs), CAOCs, and Air Force forces (AFFOR) formal staff training programs would tell us they are not yet.

Before we can provide training, someone must write a textbook and a lesson plan. The textbook in this case means the tested, vetted, authoritative tactics, techniques, and procedures (TTPs) for C2 in a CCE. I mean nothing less than what we provide our flying communities—detailed, written TTPs, supported by an active lessons learned program, routine field interaction, robust formal testing, a vetting process, and procedures to rapidly disseminate critical changes. This discipline and infrastructure does not yet exist for the USAF C2 community. Until it does, our strategy for assured C2 will be incomplete.

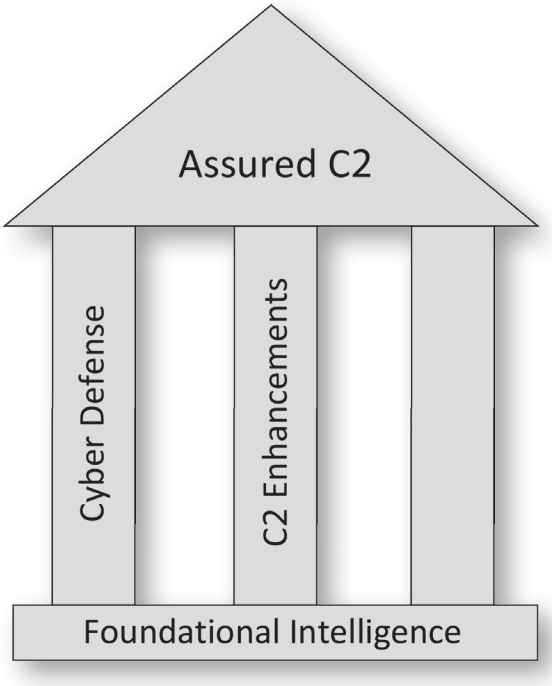

Figure 4: Second pillar—enhancing C2 to better survive in a contested cyber environment

Reduce Dependency

The third pillar in our strategy addresses dependency. It seems unwise to acknowledge that cyber is a contested domain, and then not reduce our dependency on that domain. I offer the following equation for consideration: risk equals threat multiplied by dependency.

In other words, risk to C2 is a function of both enemy cyber effectiveness and C2 dependency on cyber. To make the point, World War II C2 was invulnerable to the most aggressive modern cyber attack because the system back then was not wholly dependent on an electronic network like we are today, with its single overarching vulnerability. I'm not suggesting we turn back the clock, but rather that we reduce dependency where we can, or at least be cautious about increasing dependency. Two areas to examine come to mind—reachback and warfighting integration.

Reachback is defined as obtaining products, services, or material support from organizations not forward deployed. This is done for a variety of good reasons: efficiency, cost savings, security, and survivability. But, reachback depends on long range, secure, reliable, and high volume communications. Increased dependency means increased vulnerability. In certain scenarios, this may be an acceptable risk. In others, with elevated cyber threats and other dangers, it would clearly not be.

Warfighting integration means the artful combination of weapons systems, joint force assets, and the warfighting domains. Exquisite warfighting integration is definitely a force multiplier. But, exquisite warfighting integration depends on equally exquisite C4. Increased dependency means increased vulnerability. To the extent warfighting integration isn't possible, we should plan, train, and exercise accordingly.

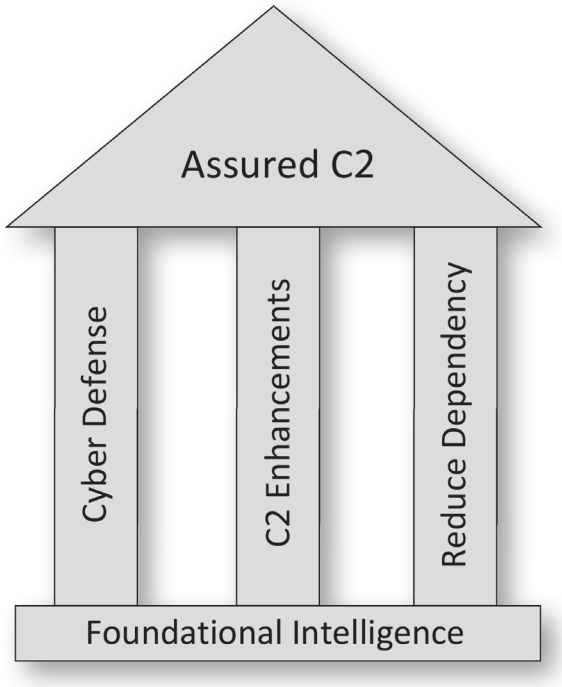

Figure 5: Unifying these elements help enable assured C2, even against potent cyber threats

Conclusion

The next conflict may very well test our ability to fight in contested environments. Cyber will be a battleground, but I have great confidence our commanders, weapons systems experts, front line operators, and logisticians can meet any challenge. I'm far less confident, however, that our current C2 apparatus will enable them to succeed.

We will give our Airmen a fighting chance if we adopt a comprehensive strategy to achieve assured C2. The strategy is founded on a clear understanding of C2 in a contested cyber environment, and supported by all our efforts in the realm of active and passive cyber defense. Equally important, we must push to adopt a new C2 paradigm, create effective C2 systems and process, train our C2 practitioners, and arm them with state of the art tactics, techniques, and procedures. Finally, we should cultivate an appreciation of cyber dependency, in our current force, for what it is—a vulnerability.

While this is easy to point to, it is far harder to execute. To foster success, I offer two suggestions. First, enable the Air Force Warfare Center to fulfill its charter. Second, enable C2 force providers to deliver effective, survivable C2.

The US Air Force Warfare Center at Nellis AFB, Nev. (USAFWC) is chartered to conduct advanced training, tactics development, and testing. It provides our flying communities with current threat information, arms our Airmen with current, relevant, tested, and vetted TTPs, and provides our Airmen advanced training and exercises. The USAFWC is one of the main reasons why the US Air Force will never be defeated—in the air.[4]

Unfortunately, the center lacks the capability to do the same for the C2 enterprise. An investment in manpower and expertise would enable the USAFWC and its partner intelligence organizations to develop skills to gather and formulate foundational intelligence. That, in turn, would inform necessary material and non-material solutions. A similar investment would enable the warfare center to provide tested, vetted, authoritative TTPs for C2 in contested environments. These investments are critical to improving training for our C2 practitioners.

My second recommendation concerns Air Force staffs responsible for delivering C2 capability. C2 and cyber experts must be literally working side by side on the necessary C2 to enable cyber defenses and C2 enhancements. That may require an investment in manpower and expertise, or possibly require a realignment of existing expertise.

The Pacific Air Forces headquarters provides an interesting case study. Several years ago, following exercise experiences with cyber vulnerabilities, PACAF merged the A3 (operations) and A6 (communications). As a result, cyber professionals from the A6 talk about C2, and operators from the A3 talk about cyber in the same directorate, and have improved coordination and collaboration as a result. This outcome is a teachable example that shows how the Air Force needs to bring together C2 and cyber professionals and operations professionals wherever possible. In the future, the collaboration and understanding between operations Airmen and C2 Airmen will be essential to building an Air Force that is well prepared for 21st century challenges. ✪

Endnotes

1 Joint Chiefs of Staff, "Joint Publication 3-12 (R) Cyberspace Operations," Feb. 5, 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed February 2017).

2 US Air Force, "Air Force Policy Directive AFPD 17-2, Cyberspace Operations," April 12, 2016, http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd17-2/afpd17-2.pdf (accessed February 2017).

3 US Air Force, LeMay Center for Doctrine Development and Education, "Annex 3-30 Command and Control," November 7, 2014, https://doctrine.af.mil/DTM/dtmcommandcontrol.htm (accessed February 2017).

4 US Air Force, "US Air Force Warfare Center – Fact Sheet," October 26, 2016, http://www.nellis.af.mil/About/FactSheets/Display/tabid/6485/Article/284150/us-air-force-warfare-center.aspx (accessed February 2017).

About The Mitchell Institute

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

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Lt Gen Stanley T. Kresge, USAF (Ret.), served as the Vice Commander, Pacific Air Forces (PACAF), Joint Base Pearl Harbor-Hickam, Hawaii, and deputy theater Joint Force Air Component Commander to the commander of US Pacific Command (PACOM) from September 2012 to July 2014. He retired from the position, and Active Duty, after 34 years of service. Prior to his last assignment, Kresge served as the commander of 13th Air Force, Joint Base Pearl Harbor-Hickam, Hawaii, from December 2010 to September 2012.

Commissioned in 1980 after graduating from the US Air Force Academy, Kresge's past commands include the F-15 division at the USAF Weapons School; 27th Fighter Squadron; First Operations Group; 33rd Fighter Wing; 379th Air Expeditionary Wing; US Air Force Warfare Center; and 13th Air Force. Kresge served in staff assignments at the Air, Land, and Sea Application Agency, Secretary of the Air Force, Office of the Legislative Liaison; Air Combat Command; and Air Force Space Command.

Kresge is a command pilot with more than 4,200 flying hours, primarily in the F-15.