Winter 2016

Forging Tomorrow's Air, Space, and Cyber War Fighters: Recommendations for Integration and Development

Mark Reith
Air Force Institute of Technology

Forging Tomorrow's Air, Space, and Cyber War Fighters

Recommendations for Integration and Development

Lt Col Mark Reith, USAF*

Courtesy Carrie Solberg

Today's Airmen operate in contested environments, and years of technical-data spillage, coupled with policies emphasizing commercial-off-the-shelf acquisition, ensure that the immediate future will remain contested as our adversaries seek to exploit level playing fields. Long gone are the days of Operation

*Special thanks to several leaders who generously offered their time, feedback, and encouragement: Col Pamela Woolley, Col Chad Raduege, Col Eric DeLange, Col David Snoddy, Col Heather Blackwell, Col Greg Gagnon, Col Michelle Hayworth, Col Chad LeMaire, Col Brad Pyburn, Mr. Richard White, Lt Col Eric Trias, and Lt Col Joy Kaczor.

Desert Storm and Enduring Freedom when air superiority dominated and the supporting elements of space, communications, and computers were largely out of reach for many nation-states. Since then, technology has become ubiquitously intertwined in weapon systems and today largely turns the gears of warfare, allowing a range of actors to erode national instruments of power. Today's Airmen are in the fight, whether in air, space, or cyberspace, and must be prepared with the right war-fighter mind-set to fight through modern conflict across the landscape of at least these three domains.[1]

Space and Cyberspace: Employing Critical Capabilities within and through Contested Domains

Space is not a permissive and benign environment anymore. We need to admit it's a contested domain and move on from there.

—Lt Gen David Buck, Commander
Fourteenth Air Force (2015–present)

Cyberspace is a contested domain, and it is imperative that we shift our mindset to instill an operations culture.

—Maj Gen Burke "Ed" Wilson, Commander
Twenty-Fourth Air Force (2014–16)

In today's complex war-fighting domains, Airmen find themselves operating within and through increasingly combative environments. Whether they are part of air, space, or cyber crews, the success of their mission depends on resilient space and cyber capabilities. The Airmen who provide these capabilities are not merely combat supporters but operators in their own right as they actively engage to defend these capabilities from a set of very real threats. Their daily battle to retain control of operational systems and data while assuring that the rest of the team retains maximum maneuverability and lethality requires innovation, teamwork, sound judgement, and a burning desire to win—in short, a war fighter's mind-set. The Air Force can forge the right mind-set by addressing the following issues.

Immediate and Long-Term Challenges

Our challenge as we move forward is to create linkage in all mission elements . . . the operational tapestry versus the mission threads. We don't need to command and control the mission, but we need to have full visibility of what's going on in the [cyber] space and be able to adjust it in real time to thwart adversary positioning. It makes the adversary's problem set much more difficult while preserving mission effectiveness.

—Maj Gen Suzanne Vautrinot, Commander
Twenty-Fourth Air Force (2011–13)

Lack of Fully Integrated Air, Space, and Cyberspace Operations (Long-Term Challenge)

For the purposes of this article, a fully integrated air, space, and cyberspace operation is defined as synchronized activities across multiple domains to achieve one or more effects despite adversary activity. Each operation should consider offensive and defensive perspectives in all three domains. Today, the Air Force uses separate air tasking orders, space tasking orders, and cyber tasking orders to employ forces in each domain, often independently of each other. Efforts to synchronize orders are inhibited by several factors. One part of the issue involves the lack of realistic exercises that force all three communities to work together. Although significant progress has been made in the most recent Red Flag and Cyber Flag exercises, both concentrating on air and cyber relationships, the Air Force has yet to exercise significantly across all three domains simultaneously. Investment in a robust live-virtual training construct is the right approach, but more research is needed to show how operators may dynamically share real-time problems as a means of offering timely multidomain solutions. Airmen should not view glitches as an "air problem," a "space problem," or a "cyber problem"; instead, they should offset a deficiency within one domain with the strength from another. As space and cyber communities develop their space mission forces and cyber mission forces, respectively, they should partner with the research and innovation community to help figure out such problems.[2] Vectoring operators to research and teaching positions is one approach, but investing in some multidomain mission-qualification training and experience for a few innovators might prove more effective because they bring a fresh perspective. Either approach involves a modest cost but will allow the larger Air Force team to tackle some difficult matters, such as unifying command and control across domains while taking some of the burden off the operators' shoulders.

Limited Operational Opportunities (Immediate Challenge)

The second most significant barrier to developing the war-fighter mind-set is the lack of opportunities to practice and hone one's operational art. Herein, "operational art" specifically refers to serving as an operational planner or a crew member who employs an Air Force weapon system.[3] Space and cyber Airmen need to experience at least one operational tour at the beginning of their careers so that it beneficially shapes their view of the Air Force mission and the way they fit into it. Such a tour provides a frame of reference for comparing and relating future support assignments. For example, an Airman serving as part of a crew on the Air Force cyber defense weapon system will understand the operational rigor and discipline necessary to employ it. Future assignments as an instructor, an acquisition subject-matter expert, a headquarters staff member, or even a unit commander will leverage this valuable foundational experience. Mission-qualification training, coupled with hands-on experience, lays the cornerstones of a war-fighter mind-set. Furthermore, association with a weapon system supplies confidence and credibility among fellow operators, reinforcing that mind-set. Today, a significant portion of new-accession cyber Airmen will receive fundamental training for their career field but will fill corporate Air Force positions and influence decision making without ever experiencing

the pressure, intensity, and pitfalls of operations. Instead, these individuals are forced to rely upon commercial standards and abstract concepts to shape what military capabilities should look like.[4] The net result is an attitude that favors the reliability of systems over the resiliency of capabilities. Training and education will always be necessary, but they cannot completely replace the experiential component that forges the war-fighting attitude. Training helps explain what we do and how we perform our jobs, but it doesn't sufficiently describe why they are important or how they relate to operations. The solution involves giving Airmen more operational opportunities—a subject addressed by this article below with a career-development chart and description.

Parochial Career Development (Long-Term Challenge)

The third major barrier in today's Air Force is recognizing and countering tribalism within career fields. Unlike previous generations that could develop their communities for the most part independently of others, today's service depends on capabilities across all three domains, forcing Airmen to collaborate much more across communities. Current senior leaders need multidomain experience from a combat perspective to shape decisions about organizing, training, and equipping the force. Presently, this experience is acquired very late in an Airman's career, if at all. The Air Force would realize a much greater return on investment by vectoring Airmen to positions in which they can gain this experience earlier in their careers and develop cross-community and teaming relationships. These personnel should be vectored and recognized for their cross-community expertise.[5]

One possible solution entails committing Airmen to partner with different communities. After they have learned the fundamentals of operations during their initial tour, agnostic of any particular weapon system, these Airmen then integrate across domains by specializing in terrain and/or type of operation for their first decade of service. For the space community, this process might involve specializing in satellite command and control and partnering with the flying community to ensure accessibility for air operations. Similar partnerships are feasible with the cyber community to ensure resilient communications, perhaps involving full-spectrum operations per geographical area or cyber defense of a specific Air Force mission system, such as a tanker airlift control center. Efforts to build cyber mission defense teams could be a notable example of partnering as long as the entire team of operators is held accountable for both mission success and failure. An Airman first learns operational rigor and command relationships from within Twenty-Fourth Air Force and then specializes in defending key cyber terrain, specifically supporting fighter aircraft, space control systems, and so on. The commitment to partnership is the key element here. Air and space operators need to know and trust their cyber counterparts, understanding that everyone involved has the operational discipline, background, and credibility to lead successfully. For cyber operators, they have the time to learn their specific terrain, become adept at defending it, and understand the community they have joined. Future tours as mission planners supporting air/space/cyber operations become credible because of their experience in the multidomain environment.

Cultural Legacy of Combat Support (Immediate Challenge)

> *We must resist the biases and misperceptions often induced by the abstract and invisible nature of the cyberspace domain—these service members are no less warriors than their established brethren. Cyber warriors deliver decisive battlespace effects for the commander.*
>
> —Maj Gen Chris "Wedge" Weggeman, Commander
> Twenty-Fourth Air Force (2016–present)

The final significant barrier to developing the war-fighter mind-set involves the cultural heritage associated with combat-support activities. Historically, the Air Force has viewed the space and communications communities as providers and maintainers of a utility, not unlike commercial water and electricity. Airmen were rewarded not only for providing reliable utilities but also for taking on a corporate support role of retooling and modernizing the force in an effort to provide new commercial-off-the-shelf capabilities and reduce overall cost. Space and communications culture was thus shaped by the two major activities of integration and maintenance, and such activities relied on project management, quality assurance, and technical skills.[6] This scenario will continue to inhibit efforts to operationalize space and cyber unless the culture is redefined.

Today, these "utilities" are no longer benign, having become contested domains. Conflicts can be waged in and through them, and the Air Force demands not just *reliability* but *resiliency* against the efforts of adversaries. Skills that made support Airmen successful are no longer sufficient; however, they remain complementary. For example, integrating new systems that link into space and cybersecurity sensors and tactics, techniques, and procedures will continue to be important. Nevertheless, the service needs to offer Department of Defense information network (DODIN) operators the right operational experience so they can understand why it is important. Furthermore, nonkinetic attacks may masquerade as maintenance issues, thus requiring knowledge of both cyber operations and maintenance to tease out the distinction. Successful defense calls for both perspectives. Thus, the operational rigor and discipline of the war-fighter mind-set need to be embraced and reconciled with historic support attitudes. The remainder of this article explores the key attitudes and values that must change if the Air Force is to realize a fully integrated war-fighting force; it also proposes a means to assist in this endeavor.

Crafting the "Fully Integrated" Culture across the Air Force

> *The real war-winning magic happens when our newest cyber warriors wield their power in full integration and synchronization with all kinetic and nonkinetic actions and effects of classic war fighting.*
>
> —Maj Gen Chris "Wedge" Weggeman, Commander
> Twenty-Fourth Air Force (2016–present)

According to a standard English dictionary, culture is the set of shared attitudes, values, goals, and practices that characterizes an institution or organization. It guides our decision making and influences how we perceive the world. Below are some of the key attitudes and values that need cultivating if the Air Force wishes to realize a fully integrated war-fighting culture. Please note that this list is not intended to be exhaustive and that these characteristics are not unique to space or cyber communities; instead, they highlight opportunities for all Airmen to improve.

The Will to Fight

> *Any capability that cannot survive when facing the threats of today and the future is worthless in conflict—no matter how impressive its peacetime capability. Our job is to prepare for conflict.*
>
> —Gen John E. Hyten, Commander
> Air Force Space Command (2014–16)

One might imagine that the "will to fight" is a phrase associated with physical combat. However, as our adversaries begin to look for asymmetrical techniques for reducing US power, the Air Force must expand this term to recognize that future conflict will be engaged within and through friendly space and cyberspace terrain. Contested domains are the new norm, so we should develop Airmen who can fight and win on what was previously considered unreachable home-front territory. The advent of long-range missiles and standoff weapons created a cultural perception that we don't necessarily have to expose forces in order to engage. We must temper this perception with the idea that all Airmen should expect to be part of the fight, whether as operators or consumers of the Department of Defense's global information grid. Airmen should expect to take a couple of punches and should train to counter. These blows could manifest themselves in a range of ways, including physical harm (e.g., our weapons turned against us) or attacks on our virtual personas (e.g., exploiting personally identifiable information). Recognizing and preparing for potentially dangerous repercussions will clarify purpose and harden an Airman's resolve to get it right.

Many terms exist for this concept, such as "grit" or "resiliency," but the key element is to carry out the mission despite the efforts either of our adversaries or of the fog/friction created by the complexities of these domains. Historically, the cyber community has embraced a culture of compliance but must now develop a culture of readiness.[7] The Air Force can empower its space and cyber war fighters to develop this attitude through a combination of tailored training programs and operational experience, but it won't happen if the legacy culture of combat/corporate support persists in its present form. The reality of the threat, as well as the importance of our operations, doesn't truly sink into our consciousness until we stand on that front line. Airmen need firsthand experience in why their efforts are critically important.

Vision and Innovation

> *CYBERCOM depends on three factors for success: the quality of its people, the effectiveness of their capabilities and the proficiency its people bring to bear in employing capabilities.*
>
> —Lt Gen James "Kevin" McLaughlin, Deputy Commander US Cyber Command (2014–present)

Vision and innovation continue to be cornerstones of leadership, but the goal needs to change. Historically, the goal of innovation was to modernize the force's technical maturity within some degree of the commercial world so as to minimize maintenance and training costs. Unfortunately, this objective anchors the Air Force within the technical reach of our adversaries, both state and nonstate actors. Instead, the goal of innovation should be to maximize the effectiveness—and secondarily the efficiency—of our space and cyber weapon systems. Operational units spend money in defense of the nation, and although finding ways to provide comparable military capabilities with fewer resources in peacetime is good stewardship, the concept of peacetime is a gray area for space and cyber. Air Force innovation should focus on ensuring freedom of maneuver and readiness within these domains instead of looking for ways to extend the life cycle of information technology one more year. These contested domains should no longer be viewed as support equipment but as battlegrounds. Our vision and innovation must reflect that concept.

Teamwork and Common Lexicon

> *Cyber's no different. We're understanding the domain in new and different ways. One of them is a tasking order, a defensive cyberspace operations tasking order. This is the kind of reset we need . . . [using] terms that are understandable to everybody else in the Air Force.*
>
> —Gen Mark A. Welsh III, Chief of Staff United States Air Force (2012–16)

The concept of teamwork has always been a core theme across the US military, but the composition of the team has changed. Historically, a team consisted of members from the same community, often working towards similar goals but doing so independently of other communities. Solutions to today's problems require much more coordination across domains. Barriers often include multiple assignments within a single major command, technical jargon and concepts, and myopic assumptions and cultural values specific to that community. To manage military capabilities and resources effectively, the Air Force should build Airmen who understand the broad picture, articulate issues in terms that all operators can understand, and advise leadership on how to best synchronize air, space, and cyber operations. This process begins with a common framework that all operators can understand and relate to. Given this framework, air, space, and cyber operators should put aside their technical geek speak and find common ground to socialize and collaborate.

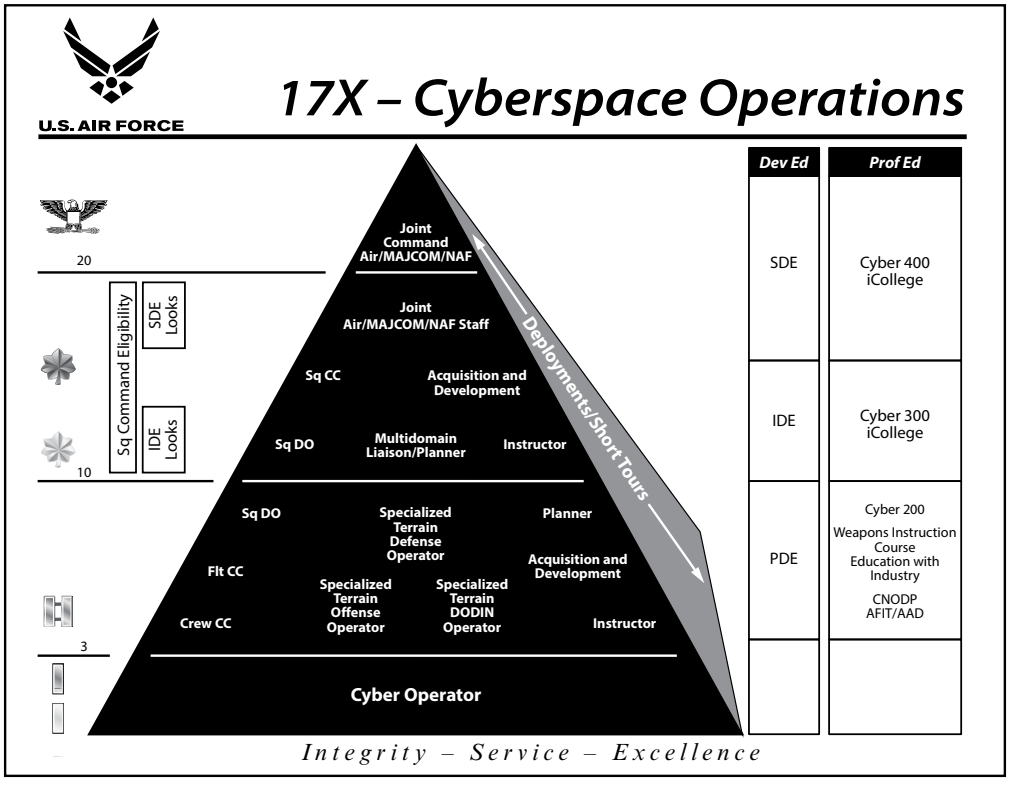
Risk Management

> *One cannot adequately defend a network without knowing the mission that network supports as well as the threat that holds it at risk.*
>
> —Col Timothy Franz, Commander
> 318th Cyberspace Operations Group (2015–present)

Finally, today's Airmen need to know how to characterize, quantify, and articulate operational risk. Specifically, they must understand relationships between military capabilities and technology, between technology and vulnerabilities, and between vulnerabilities and threats. Furthermore, Airmen should leverage the knowledge of these relationships to reconcile intelligence about threats against existing defenses and pending missions to provide commanders with decision-quality risk assessments. This analysis is complex but is the first step in assuring missions and having an objective discussion on where to spend resources. Assessing risk in this context is difficult without operational experience.

Recommendations

In light of the need to deal with contested domains and build the right warfighter culture, the following recommendations are presented. First, the Air Force should vector new-accession space/cyber operators to an operational tour within their community as early as possible, preferably their initial assignment. Second, it should encourage air/space/cyber operators to team with their counterparts beyond their community in subsequent assignments. Third, the air and space communities should develop their own career-progression pyramids that include liaison and planner opportunities within Twenty-Fourth Air Force units and in concert with mission defense teams. Figure 1 illustrates a hypothetical career pyramid for the cyber community. It is designed with specific goals in mind. First, experience in cyber operations is foundational for all 17X Airmen, regardless of their future career paths. Second, the Air Force greatly benefits from sending some of our best cyber operators as subject-matter experts to partner with the schoolhouse, laboratory, and acquisition team. Third, this approach develops planners within and across air, space, and cyber communities, preparing Airmen to represent the Air Force to the combatant commanders. Fourth, this approach gives all 17X Airmen opportunities to leverage the complementary nature of cyber operations. For instance, personnel who initially learn cyber defense do not have to remain on that path for their subsequent assignment. In fact, the service benefits greatly when that experience is coupled with cyber offense or DODIN operations because the skills are complementary, regardless of combination. Finally, this approach may encourage recruitment and retention into the space and cyber career fields because it brands Airmen as operators, allowing them to participate directly in defending the nation.



Sq - squadron
SDE - senior developmental education
IDE - intermediate developmental education
MAJCOM - major command
NAF - numbered air force
CC - commander
DO - director of operations
Flt - flight
DODIN - Department of Defense information network
Dev Ed - developmental education
Prof Ed - professional education
PDE - primary developmental education
CNODP - Computer Network Operations Development Program
AFIT/AAD - Air Force Institute of Technology / Advanced Academic Degree

Figure 1. Proposed 17X career pyramid. Key features include an early focus on operator development within Twenty-Fourth Air Force and a follow-on specialization (or partnering) based on cyber terrain such as aircraft, spacecraft, industrial control systems, and so on. The goal is to develop all 17X Airmen with the warfighter mind-set both within and across domains. Note that the largest cadre of operators will most likely support defensive roles.

Several concerns could be raised about this strategy, the most significant involving increased spending on training.[8] Some investment would be necessary, but the Air Force could accelerate the development of cyber capability and seed immediate and future growth in a sustainable manner. Training efforts could benefit from an economy of scale to justify better facilities and training-range environments. Furthermore, the expense might be offset by previous investments in programs such as Cyber Patriot and Hackfest (fig. 2), which are producing accessions who already have basic cyber skills.

Courtesy Carrie Solberg

Figure 2. Honing cyber skills at Hackfest. *Left*: Cadet Donte Dimanche (Wilmington University) practices cyber block-and-tackle techniques at the Air Force–sponsored Hackfest. *Right*: Cadet Jonathan Chua (Embry-Riddle Aeronautical University) guides Cadet Brooke Robinson (University of Colorado–Boulder) through a complicated exploit technique. Hackfest is an annual event organized by the Air Force Cyber Technical Center of Excellence at the Air Force Institute of Technology.

Conclusion

Because the Airmen of today operate in contested environments, the Air Force should make select investments and changes as outlined in this article to prepare for this new norm. The conflict of today and tomorrow will include a larger slice of Airmen than did previous struggles, so these individuals need to be ready with the right war-fighter mind-set to defend the nation and its ability to project military power. An Airman—forged in the crucible of operations, confident and emboldened by operator credentials, and experienced in working with fellow operators across other domains—is the type of formidable, disciplined war fighter the Air Force needs to best serve the country. ✪

Notes

1. Other war-fighting domains such as land and sea are equally as important in relation to cyber, and joint operations and exercises across all domains are ultimately the goal. Although this article emphasizes the war-fighting mind-set supporting the Air Force's core missions, the reader can easily extend the concepts to the joint world.

2. For example, this scenario may include industry and academia under the umbrella of the Defense Innovation Unit Experimental championed by Secretary of Defense Ashton Carter. It may also involve service schools under Air University such as the Air Force Institute of Technology and the United States Air Force Academy. Doing so ensures that Air Force space and cyber forces benefit from people educated in complex systems thinking and are not constrained by legacy paradigms.

3. Understandably, the space community might have issues with the term "space weapon system"; however, at a minimum, one merely has to recognize space systems as components of larger Air Force weapon systems, and clearly the paradigm fits. The cyber community already recognizes cyber weapon systems, both as a component of larger Air Force weapon systems and as an explicit weapon in itself.

4. For example, many personnel in the former communications career field would say that the Information Technology Infrastructure Library is the standard for governing information technology, along with a list of certifications a mile long. Instead of building Airmen with a war-fighter mind-set, we are left with a workforce that better resembles commercial contractors. A similar argument might be made within the space community, where the workforce's associations are more like those of engineers than of space war-fighting operators.

5. Presumably the strongest reason why Airmen are vectored within their own tribal units involves a desire to protect one's own community from the stratification of another. This view is myopic since our career-development goals should not be to produce the strongest pilot or space/cyber operator but to develop strong leaders throughout the Air Force who well understand the strengths, challenges, and relationships among the three domains.

6. Furthermore, serving a large population with finite resources often meant imposing a standard—largely static—technical solution in order to minimize downtime and sustainment costs, frequently leading to more cultural disconnect from war fighters. The lack of operational experience, both within and across domains, created a negligible distinction between support Airmen and contractors.

7. "Culture of compliance" refers to compliance with information security and technical checklists. The prevailing attitude is based on the assumption that if the checklist is complete, then the Air Force should have sufficient cyber defenses. This supposition ignores the dynamic, asymmetric nature of cyber warfare and the repeated examples of zero-day exploits that are often unconstrained by static defenses.

8. Key criticisms may include the following. First, Twenty-Fourth Air Force doesn't have enough positions to place additional manpower. Aside from the logistics of multibilleting accessions, the Twenty-Fourth certainly has enough cyber terrain to defend, and every available Airman will be fully employed executing these missions. Second, base communications squadrons will initially lose opportunities to gain new accessions; however, this situation is temporary while the pipeline is primed. Current manpower could remain in place until Twenty-Fourth Air Force starts vectoring experienced cyber operators, and the quality will be worth the wait. Finally, any perception that this strategy would hold up the "Comm Squadron Next" or "Mission Defense Team" effort is false since incumbent base personnel can continue this effort and leadership can immediately vector Airmen already within the Twenty-Fourth to augment as necessary.

Lt Col Mark Reith, USAF

Lieutenant Colonel Reith (PhD, University of Texas–San Antonio) previously served as deputy commander of the 26th Cyberspace Operations Group and 690th Network Support Squadron, providing enterprise cyber defense and Department of Defense information network forces, respectively. He currently serves as assistant professor of computer science at the Air Force Institute of Technology and the Center for Cyberspace Research.

Let us know what you think! Leave a comment!

http://www.airpower.au.af.mil