WINTER 2016
VOLUME 30, NO. 4
AFRP 10-1

Features

Mission Assurance through Integrated Cyber Defense | **5**
Col William D. Bryant, USAF

Operational Assessment | **18**
So How *Are* We Doing?
Lt Col James S. Welshans, EdD, USAF, Retired
Lt Col Charles Owen, PhD, USAF, Retired
Dr. Alice M. Mulvehill
Col Calvin W. Hickey, USAF, Retired
Robert J. Farrell Jr., DAF, DR-III

Suborbital Strike! | **32**
The Use of Commercial Suborbital Spacecraft for Strike Missions
Capt Daniel J. House, USAF
Dr. John Tiller
Dr. John Rushing

Selecting Qualified Airmen for the Cyber Mission Force | **47**
The Pitfalls of Hiring Operational "Analysts"
Maj David J. Ortiz, USAFR

Departments

60 | Views

The Trilateral Strategic Initiative | **60**
A Primer for Developing Future Airpower Cooperation
Col Peter Goldfein, USAF
Wing Cdr André Adamson, PhD, RAF

C4ISR via Dark Webs | **69**
An Alternative Concept for Protecting Critical Information in Contested Cyberspace Environments
Capt Kyle L. Bingman, USAF

78 | Commentary

The Fifth-Generation Fighter Pilot Force | 78
Col John D. Jogerst, USAF, Retired

81 | Schriever Essay Award Winners

Forging Tomorrow's Air, Space, and Cyber War Fighters | 82
Recommendations for Integration and Development
Lt Col Mark Reith, USAF

The Changing Face of the War Fighter | 94
Capt Justin Ryan Thornton, USAF

103 | Book Reviews

Inside China's Grand Strategy: The Perspective from the People's Republic 103
Ye Zicheng
Edited and translated by Steven I. Levine and Guoli Liu
Reviewer: Capt Stefan G. DePaul, USAF

An Untaken Road: Strategy, Technology, and the Hidden History of America's Mobile ICBMs 104
Steven A. Pomeroy
Reviewer: Daniel Schwabe

Emblems of Exploration: Logos of the NACA and NASA 105
Joseph R. Chambers and Mark A. Chambers
Reviewer: Maj Andrew L. Brown, USAF

No One Avoided Danger: NAS Kaneohe Bay and the Japanese Attack of 7 December 1941 107
J. Michael Wenger, Robert J. Cressman, and John F. Di Virgilio
Reviewer: Dr. Katherine Strus, Lieutenant Colonel, USAF, Retired

Go, Flight! The Unsung Heroes of Mission Control, 1965–1992 108
Rick Houston and Milt Heflin
Reviewer: Capt James Maday, USAF

Developing National Power in Space: A Theoretical Model 109
Brent Ziarnick
Reviewer: 1st Lt Keegan S. McCoy, USAF

The Cadet 111
Doug Beason
Reviewer: Capt Richard P. Loesch III, USAF

Mission Assurance through Integrated Cyber Defense

Col William D. Bryant, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

Adversaries increasingly contest the ability of the United States Air Force to accomplish its missions in and through the cyberspace domain. Although different communities within the service focus on various approaches for a cyber defense framework, the best way to assure the Air Force's core missions is through a combination of defense in depth, resiliency, and active defense. Each approach is necessary, none is sufficient, and the service should combine them into a coherent whole for maximum effectiveness.

The core missions of the Air Force are heavily dependent upon freedom of action within the cyberspace domain. Unfortunately, we designed most of the weapons and missions systems in use today for a pre-Internet world. The implicit assumption was that our systems would operate in a fundamentally permissive cyberspace environment and that the greatest threat would be enemy signals intelligence.[1] The

Air Force designed many of its systems decades ago, so it is certainly not surprising that no one could predict the explosive growth and importance of the cyberspace domain. When system architects considered some form of information security for weapons systems, engineers normally assumed that border network defenses would keep out adversaries so that the environment seen by the weapons system would remain permissive and protected within network defenses.

These implicit assumptions have proven dramatically false. The pace of cyber attacks increases daily across the military, government, and civilian sectors. Cyber physical systems, those that include both physical and cyber components, are no longer safe—witness the successful attacks on industrial control systems and vehicles.[2] These trends are well understood and obvious. Making the situation dangerous is the fact that our adversaries also clearly understand our vulnerability to these types of attacks and emphasize them in their official published doctrine.[3] Just as our adversaries have come to think differently about warfare in cyberspace, so must we adjust our perspective.

The presence of a maneuvering enemy within the cyberspace domain requires a fundamentally different approach that goes beyond static defenses based on information technology (IT). Viewing cyberspace as a domain of warfare helps us understand why this is so. Carl von Clausewitz, the famous theorist of war, viewed warfare as two wrestlers, each trying to throw the other while constantly adjusting and reacting to the subtlest of movements by his adversary.[4] Static approaches that do not address what the enemy is doing will fail because he will react to whatever we have done to nullify their effect.[5] Mission assurance in and through cyberspace is not fundamentally an IT problem but a mission problem that requires a mission focus and approaches that go beyond what we have come to think of as traditional cybersecurity. Part of this perspective is to grasp that cyberspace reaches much further than traditional IT and into cyber physical systems upon which we rely.

Cyber Physical Systems

All modern systems exist simultaneously in both the physical and cyberspace domains. Opening panels on a modern fighter aircraft, for example, will reveal a large number of electronic boxes connected by wires. Those boxes generally do not use the standard transmission control protocol (TCP) / Internet protocol (IP) network protocol; rather, they pass information across data busses to other electronic boxes, clearly fitting the definition of cyberspace noted in Joint Publication 3-12 (R), *Cyberspace Operations*.[6] As noted in more detail later, any defender who takes comfort in the fact that those electronic boxes are not directly connected to the Internet but are "air gapped" should think again. He or she must realize that in almost all cases, those systems are actually connected to everything via several degrees of separation that attackers have demonstrated the ability to jump across via numerous methods.[7]

Since weapons systems such as ships and aircraft rely so heavily on cyberspace, actions within the cyberspace domain directly affect war-fighting systems in the physical domains. Adversaries can attack these systems in cyberspace through numerous access points. Essentially, any physical connection that passes data or any antenna with a processor behind it is a potential pathway for an attacker. Obvious examples include maintenance and logistics systems, software-defined radios and data links, and other cyber physical systems that operators can connect to platforms, such as pods or weapons. To make things even more complex, these vulnerabilities are not static but change constantly.

Every software update, every new capability, and every novel piece of equipment can introduce new vulnerabilities. Defenders cannot simply "fix" a system and walk away, expecting the system or capability to stay "fixed." Furthermore, the weapons system platform itself may be completely secure, but maintenance, support, and logistics systems may prove just as critical to mission accomplishment. Squadrons of the most modern fighter aircraft with no fuel are nothing more than very expensive targets. Increasing complexity further is the fact that many critical mission dependencies lie outside Air Force boundaries in commercial systems such as power and transportation over which the service has very limited or no control. In some operational contexts, allied nations operate those systems with their own rules and priorities, making it even more difficult to influence how those countries protect the systems on which the Air Force relies. Since the range of vulnerabilities is so overwhelming, we must start by determining what is most important.

Key Cyber Terrain

To determine our key cyber terrain, we have to consider both the types of cyberspace assets we are examining as well as the level of analysis.[8] The three types of assets are traditional IT, operational technology, and platforms. Traditional IT systems include networks such as Nonsecure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) as well as IT-based weapons systems, including the air operations center and numerous other personnel and logistics systems. Operational technology refers to computer-controlled physical processes such as industrial control systems or other types of control systems such as building automation or heating, ventilating, and air-conditioning.[9] The latter category is a relatively new one in military circles but has attained wide acceptance in the civilian world. The final category, platforms, includes both an F-16 fighter and an Aegis cruiser. Cybersecurity experts tend to be very comfortable and familiar with traditional IT, are just starting to concentrate on operational technology, but have not yet really begun to figure out how to secure platforms.

Simply categorizing the type of asset is not enough. When determining key cyberspace terrain, an analyst should also look at three different levels of analysis and consider the component, the system, and mission levels. If our priority is mission assurance, then we will also have to move our analysis above the component level, through the system level, and finally up to the mission level. Even a relatively simple mission such as defensive counterair is enormously complex at the mission level when one analyzes the nodes and interdependencies. A fighter aircraft must be on station but must also have weapons. Where did those weapons come from? What systems were necessary to transport and load them? Are those transportation systems protected from cyber attack? Each question leads to more questions; mission owners and analysts will have to work together to determine the most critical assets that will ensure mission success. Once analysts have completed their mission analysis, senior leaders will have to determine which missions are most important so they can decide how to allocate resources among them. What is more important—air and space superiority or rapid global mobility? Is global strike more important than intelligence, surveillance, and reconnaissance? Since the number of vulnerabilities is so vast, we will have to use our limited resources carefully for maximum effect.

Different Perspectives

Even after we direct our efforts toward the most significant vulnerabilities, a substantial problem remains. Various communities see cyberspace through very different lenses, based on their organizational culture and experience. It is a bit like the old fable about multiple blind men examining an elephant and coming to assorted conclusions about what it is like. Each blind man is correct about his particular area of the animal, but none of them understands the complete picture. Terminology confusion certainly does not help because "cyber" means different things to different people.

All of these factors lead diverse communities to put forward dissimilar approaches as "the" answer to mission assurance in and through cyberspace. Traditional IT communities favor utilizing defense in depth and providing multiple layers of static IT-based defenses. These communities tend to rely on compliance and security; some go so far as to equate compliance with security, believing that if evaluators check everything off the right checklist, then the system in question is secure. Acquisition communities tend to take a very different view, preferring to build resilience into systems instead of trying to retrofit security later. They create adaptable, resilient systems, and their greatest difficulty often lies in finding the right contract language that forces vendors to truly build in resilience—something notoriously hard to define. Cyberspace operations communities take a third and quite different view of how to provide mission assurance, turning to active defense through continuous monitoring and response to attacks. This emphasis on cyberspace maneuver, which relies on high-end operators and tools, can be extremely arduous to implement outside traditional TCP/IP-based networks.

All three approaches have great value; they are not exclusive but complementary, and any robust defense must include all three—integrated to support each other. Such integration offers a sustained competitive advantage that our adversaries will find difficult to replicate because of differences in culture. The Air Force has decades of experience in operating jointly and in teams with members from many services and backgrounds while most of our potential opponents are still used to operating within traditional service stovepipes. Each type of defense asks fundamentally disparate questions; requires completely different approaches, tools, and skill sets; and provides critical capabilities not found in the other approaches.

Defense in Depth

Without solid, basic IT-based defense in depth, too many attackers will get through, bring down even resilient systems, and overwhelm defenders. Regular firewalls and IT-based defenses may not stop high-level attackers, but they do eliminate the bulk of lower-level strikes and allow defenders to concentrate on the few high-level attackers who get through. This attrition of the majority of strikes is also critical for resiliency since it reduces the amount of damage sustained that the resiliency approach must overcome to allow the mission to continue. The fundamental question asked of defense in depth is, how can this approach make it hard to attack my systems successfully?

It does so by adding layers of defense, much like a castle with multiple walls. To borrow a term from cryptology, the work factor (i.e., the effort expended to penetrate defenses) is perhaps the most appropriate way to measure defense in depth.[10] Lining up 10 of the same firewalls with the same vulnerability is not nearly as useful as utilizing 2 different firewalls that require diverse techniques and tools to exploit. Most defenses in this area are technology based, including firewalls, intrusion-detection and prevention systems, blacklisting, whitelisting, and many other technologies and approaches.

A good defense in depth consists of several components. Border defenses make up its outer shell, keeping out low-level or "script kiddie" attacks, so named because unskilled hackers using prepackaged tools or scripts usually execute them. It is not sufficient just to have one or even several layers outside a network or system. Once an attacker gets in, the defender should still block him with multiple internal barriers. Defenders should configure these barriers to prevent lateral movement, privilege escalation, and the exfiltration of sensitive data. Vulnerability management across enterprises is also part of good defense in depth. To eliminate large sections of attack surface, administrators and architects should not only close vulnerabilities but also shut down unnecessary processes and applications. Of course, talking about reducing attack surface is easy, but doing it is very demanding because it often involves removing functionality and ease of use. Normally, all of these components are most effective if system architects build them in from the beginning or have them "baked in" instead of "bolted on" afterwards. To do so calls for good, secure systems engineering that considers security throughout the design process and looks both inside the system and outside at the environment in which that system is likely to operate. Starting in the design phase is actually too late; instead, systems engineering should begin in the requirements phase. Unfortunately, no matter how many layers defenders add, defense in depth has not always been successful against determined attackers.

Although necessary for any successful defense, static defenses are not sufficient; dynamic, determined attackers always seem to find a way into targeted systems. Modern systems are exceptional at making connections and thus creating attack surface. The potential area of vulnerability of even relatively simple IT systems is vast. For critical systems, an extreme version of defense in depth is an air-gapped system, in which architects not only have protected various possible attack vectors into it but also have tried to eliminate them by physically isolating the system with no direct connections to less trusted systems. It seems that this approach would be foolproof, but in practice it is extremely challenging to implement.

In most cases, such systems are not truly air gapped because maintaining them requires connecting other maintenance systems to update or change them. Only rarely would developers update and write software that always stays within the single proprietary system. System administrators might think that their systems are truly air gapped, but an analysis of them by trained computer forensics personnel would normally demonstrate otherwise. Even if administrators were careful enough to actually air-gap a system with no leaks, in most cases that action would dramatically limit functionality. After all, the entire point of most systems is to share and process data. A computer may be "safe" if it is unplugged, buried 100 feet underground, and wrapped in 6 layers of duct tape—but it is also useless.

Finally, it is worth mentioning that a cyber physical system needs its own defenses under defense in depth. Such a system should have some defenses that do not rely on a particular host network; in aircraft, for example, the system is highly mobile, and operators and maintainers may plug it into different networks. Even if that is not the case, assuming that 100 percent security will be provided by any particular defense is not prudent. Security architects not only must plan ways to keep adversaries out but also should design the system to function even with the enemy inside.

Resiliency

Given that no defense will be perfect, systems must be able to function and carry out their missions with an enemy disrupting and attacking with some level of success. At this point, mission resiliency steps forward and makes it difficult for an enemy to realize his objectives. The Department of Homeland Security's Risk Steering Committee defines resiliency as the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[11] Resiliency allows for a less-than-perfect defense that still accomplishes the mission, even under attack in a cyber-contested environment.

Network and system engineers should plan for enemy success and expect it. They should avoid single points of failure and easy targets that enable an adversary to easily disrupt mission success for an organization. A mission system should be flexible and able to deform under pressure yet still perform its mission—much like a flexible bamboo stalk rather than a rigid oak tree.[12] It is of key importance that the mission, not the system, remain the objective of resiliency; resilience in cyberspace may lie completely outside cyberspace. Tactics, techniques, and procedures may fill in for technical defenses. For example, if an adversary disrupts a logistics system but logisticians on the ground use pencils and clipboards to figure out a way to get supplies to the right place, then a backup procedure has provided resiliency that had nothing to do with IT-based defenses. Another example: if an enemy attacks all of a squadron's smart weapons and renders them inoperable through cyberspace but the squadron switches to unguided munitions and destroys the target anyway, then the squadron has assured the mission despite the failure of some systems.

Mission resilience is designed to accomplish the mission under attack—much like a battleship continues to fight after taking numerous hits. Of course, there are many ways to implement technical and procedural resiliency. Designers build battleships with thick armor and watertight compartments to reduce the possibility of catastrophic damage when enemy shells strike. Designers can include comparable features in resilient IT and cyber physical systems.

Creating resilient systems involves a number of approaches that analysts can group broadly as multiple mission pathways, segmentation, and diversity. Multiple mission pathways make it difficult for an enemy to prevent mission accomplishment. For example, if an enemy disrupts critical system A, is there a system B that can replace its functions? Multiple mission pathways do not refer only to redundancy; system B can be a completely different type of system or no system at all if a procedure B replaces the function via some non-system-based method such as manual tracking. To create multiple mission pathways requires a significant change of mind-set away from efficiency. A completely efficient system has no redundancy or "wasteful" duplicative capabilities; a resilient system or process must have those things to prevent single points of failure. In a battleship, multiple mission pathways are the different ways that operators can maneuver the ship. The rudder is the primary mechanism, but if it fails or an enemy destroys it, the ship can be roughly maneuvered by using differential thrust on different propellers. Multiple mission pathways are a good start but offer only robust resiliency if designers segment them from each other.

With segmentation, failures should be contained and not affect an entire system. In a battleship, one obvious method of segmentation occurs through separate watertight compartments. Four discrete engines do not provide robust resiliency if a single hit can flood and disable all of them. In the cyberspace domain, architects create segmentation through separate physical infrastructure and hardware as well as IT-based defenses to prevent lateral movement between various friendly network segments. One danger in current IT trends is virtualization. A mission owner may have 10 separate servers but not realize that all of them are actually on the same physical hardware. Virtualization has considerable advantages for resiliency, but architects should apply it in a manner that avoids single points of failure. Separating systems via segmentation is an important step; the final one is ensuring that these systems do not share the same vulnerabilities.

Utilizing a single operating system, type of hardware, or application produces a single point of failure that can extend across an enterprise and present an attacker with a major opportunity. Military strategist Edward Luttwak notes that with a thinking enemy, "homogeneity can easily become a potential vulnerability."[13] For our hypothetical battleship, multiple mission pathways and segmentation are generally sufficient because an attacker has no realistic way to take down an entire category of redundant systems at the same time. An enemy must destroy each main turret separately; he cannot easily destroy them all with one shot. In the cyberspace domain, it is possible to take out any number of the same systems using the same vulnerability that an enemy rapidly propagates across systems. If an organization relies completely on a single build of a single browser to run its logistics systems, then a vulnerability in that browser could shut down access to all of those logistics systems. It would be better if designers allowed for two or three different browsers that can be used to access and manipulate the data. Of course, having too many different types of applications and operating systems is more commonly the problem in organizations. Such overabundance introduces a much greater number of vulnerabilities into the overall system. Architects must strike the right balance with a small number of well-defended systems instead of either single points of failure or large numbers of unsecured systems.

These approaches to resiliency will be expensive, so acquisition programs will not implement them until senior leaders make resiliency a priority and build it into the acquisition process. One difficulty in building resilience has not been in engineering or design challenges but in finding the right contract language that drives vendors to build truly resilient systems. Program offices measure the success of their program by cost, schedule, and performance. As long as those are the only components of a program's report card, mission assurance will continue to end up "below the cut line" and unfunded. It is possible that programs could capture mission assurance and resiliency under the performance metric, but previous acquisition programs have not prioritized these factors under performance. To force this prioritization, senior leaders must be willing to make some hard decisions and refuse to allow programs to move forward through milestones unless they have incorporated mission assurance and resiliency. Doing so will prove extremely problematic to implement because of the pressures of the acquisition process, but there are indications that some senior leaders are starting to take this approach. Those individuals illustrate that in cyberspace resiliency and mission assurance, people matter.

The most critical component of cyberspace resiliency and mission assurance most often lies outside cyberspace—with the human war fighter. People are what makes this work. This fact applies across the board, from engineers designing systems to operators figuring out procedural work-arounds in the field. Empowering those people to improve resiliency involves recognition by senior leaders of the importance of mission assurance and cultural changes that empower our Airmen to make a difference. It is absolutely critical that the Air Force leverage the human war fighter and routinely conduct training in a cyber-contested environment utilizing aggressive red teams that simulate a maneuvering enemy. Many of these exercises will not go well, and collateral damage in nonexercise systems is a known risk. The Air Force must also learn to find and celebrate not those Airmen who score 100 percent on a standardized compliance-based test but those who discover and implement creative approaches that keep the mission going during demanding exercises and inspections. The service has no realistic chance of creating robust mission assurance without routinely and accurately exercising in a cyber-contested environment. Although resiliency is critical to operating successfully within that environment, another component of a strong defense is a force that actively finds and reacts to a maneuvering enemy.

Active Defense

The final component—active defense—contributes a way to discover and respond to advanced persistent threats. Defenders must know their mission space and patrol constantly, looking for small clues that can lead to a hidden enemy. Active defense, one that seeks to find and defeat a sophisticated maneuvering adversary, causes problems for an enemy who tries to stay in systems for a long period of time.

Active defense is an emotionally loaded term that sometimes refers to offensive operations outside a defender's systems. However, the subject of this discussion aligns with defensive cyberspace operations internal defensive measures, defined in Joint Publication 3-12 (R), and remains within the defender's system boundaries.[14] Defensive cyberspace operations response actions, or defensive actions taken outside the defender's system, are important but not part of this discussion.[15] It is also important to note that active defense does not always imply real-time monitoring and maneuver; it may rely on periodic checks for some types of systems for which real-time monitoring is neither practical nor desirable. Active defense is not a new concept, and operators already have implemented it in several key sectors.

More forward-leaning organizations, such as major banks, understand active defense and have switched to a network security monitoring construct that involves active defenders inside the network.[16] The Air Force also currently executes robust active defense on its own traditional IT systems, like NIPR and SIPR. Determining how to extend active defense into cyber physical systems is much more daunting. In the near term, defenders will likely need to protect the traditional IT-based equipment that surrounds and touches a cyber physical system such as Windows-based mission planning or maintenance systems for an aircraft rather than implementing monitoring on the platform itself. In the future, as engineers design and build new cyber physical systems, it will be possible to incorporate some elements of active defense where appropriate. It will not be appropriate in all cases.

To monitor and respond within a Windows- or Linux-based device is relatively simple compared to attempting to execute active defense in a cyber physical system that runs proprietary, unique software (e.g., the avionics suite of an aircraft). One of the greatest obstacles is building a workforce capable of understanding both traditional IT hacking and the proprietary protocols that run avionics or industrial control systems. Engineers must also consider performance effects on current systems. Some cyber physical devices cannot be upgraded easily; neither can they take on the increased processing and data-transmission demands necessary to execute active defense. Another consideration is the added attack surface introduced by monitoring systems. Some very powerful network tools are now available for monitoring and response. The thought of an enemy accessing those tools on a friendly network should send chills down the spine of network defenders and motivate them to defend them vigorously. Once architects mitigate these risks, active defense will include several components.

To implement active defense, architects must create three components: maneuver forces, sensors, and tools. The greatest challenge lies in developing maneuver forces that are trained, equipped, and able to execute active defense successfully. Deep technical skills coupled with creativity and flexibility are in high demand everywhere, but they are exactly what the Air Force needs to build maneuver forces in the cyberspace domain. The service must also develop "hybrids" who not only speak the TCP/IP protocol stack of traditional IT but also have a deep understanding of avionics, industrial control systems, or other control system protocols. Moreover, the Air Force struggles with integrating creativity and flexibility within a strictly hierarchical structure and culture that values compliance and conformity. The service's culture is changing, but it must do so more quickly if we wish to avoid alienating some Airmen who can be our most potent maneuver forces in cyberspace. Finding, developing, and keeping the ones we need is a start, but we must also give them the sensors they need to find a hidden enemy.

A capable sensor suite is the second component of active defense. Cyberspace maneuver forces must be able to find a hidden enemy by following the clues and evidence across networks. Standard intrusion detection systems, part of any competent defense in depth, are a starting point, but the sensors needed by maneuver forces must go further and have more capability. The latter brings greater training requirements for personnel who use sensors because the risk of a negative outcome increases if they do not understand their tools and the effects they can generate on the network. A single overaggressive scan can bring an enterprise network to its knees. It is also worth mentioning that signature-based systems generally will not see advanced, persistent threats. Advanced actors in cyberspace have long been able to write malicious code that current scanners will not find—threats that active defenders should focus on.

The final component is that after cyberspace maneuver forces have located an adversary hiding in their systems, they must have the tools or weapons that allow them to defeat him (i.e., prevent him from fulfilling his objectives). Disruption, denial, and deception are all potential approaches for defenders once they identify an enemy.[17] After such a discovery, creative defenders have an entire universe of ways to exploit him. Furthermore, they do not have to limit themselves to "micro" approaches to whatever code the enemy implanted. The use of software-defined networking permits "macro" approaches that involve changing the entire environment in ways that make it hostile to enemy malware. It is also conceivable for defenders to react on the system level and prioritize what they protect, much like the human body will sacrifice limbs to frostbite to keep the core alive. All of these approaches demand different tool sets that defenders should have developed and ready to utilize immediately.

Moving beyond Theory

Even if the theoretical construct suggested here is correct, it means little unless the Air Force can actually implement it in meaningful ways across the enterprise. The first step is for various communities to comprehend that although their preferred approach to mission assurance is correct, so are the other ones and that all three approaches must work together for maximum effect. An important step was the creation of Task Force Cyber Secure by the Air Force chief of staff with a mandate to look at assurance of the service's five core missions in and through cyberspace across the entire enterprise. Since the task force was a temporary construct, the challenge now lies in building that enterprise-level view into a new set of structures or an enduring framework. The latter will include elements from the IT, acquisition, and cyberspace operations communities tied together through a governance process and organization. Certainly, these changes at the headquarters level are important, but sweeping cultural change across the Air Force is both more difficult and important.

A self-sustaining, evolving Air Force cyberspace culture of empowered individuals who value cyberspace and know its mission-enabling benefits is the desired end state of our Airmen with regard to the cyberspace domain. As part of the task force, Team Cyber Assure examined issues that affect the cyberspace culture of all Airmen—leaders, service providers, cyber warriors, and users. Some of their recommendations concern growing and developing a cyber-aware workforce, providing strategic communications on cyberspace to the workforce, developing and implementing better cyberspace-oriented strategy and innovation, and recruiting and retaining experts in cyberspace.[18] Moving a culture is not easy and will take time. On a shorter timeline, we can make some changes in how we utilize our cyberspace specialists.

Building up the capability to successfully execute active defense across the core missions will involve shifting some resources. We can reasonably assume that the Air Force will not receive a substantial number of new cyber specialists in the current budgetary environment. If 100 cyberspace Airmen are at a base, how is the base leadership going to utilize them? Right now almost all of them are doing IT work by building and maintaining networks; commanders will need to shift some of them to active defense of those networks. Since the workload in building and maintaining networks will not diminish, leaders must contract out more of that workload, thus shifting money from other priorities. These resource decisions will prove very difficult for the future. Presently, the Air Force is aggressively laying the groundwork for that future by executing multiple pathfinders to experiment and determine the best way for cyberspace professionals to function at the wing level. Leaders should reconsider mission priorities in order to resource appropriately. One of the first things they need to do is identify and grasp the mission impact of their key cyberspace terrain.

To more effectively assure its missions in cyberspace, the Air Force must have a better understanding of the enemy and his missions. Gathering intelligence on an adversary's cyberspace capabilities and intentions is extremely difficult, but intelligence professionals are bringing additional focus and effort to this important area. On the mission side, pathfinders at the wing level are starting their programs by examining and developing their key cyber terrain after appropriate training. The acquisition community is also pursuing multiple mission threads to develop the key cyberspace terrain at the Air Force's core-competency level. All of these initial steps call for further work and development that will help clear a path to a better integrated defense of the service's core missions in and through cyberspace.

Conclusions

The best way to effectively defend both IT-based and cyber physical systems is through a combined approach that includes IT-based defense in depth, resiliency, and active defense of those systems. Cyberspace-reliant systems are essential to mission success for the Air Force in the modern world, and a single approach will not provide the most robust defense possible.

Defense in depth, which represents the initial defense, blocks most attacks—particularly the less sophisticated ones. Without solid, basic IT defenses, too many strikes will get through for resilient systems to handle. Without good defense in depth, active defense will also fail because defenders will be overwhelmed and unable to separate and find sophisticated attackers in the mass of noise.

Resiliency offers assurance by keeping missions functioning despite some enemy success. It prevents adversaries from fulfilling their objectives in attacking friendly systems. No defense will ever be completely effective, so without resiliency, defense in depth is required to meet an impossible standard of catching and stopping every attack at the boundary. Resiliency also makes it much easier for active defenders to find a hidden enemy since the latter must tackle numerous nodes and systems to have an effect; thus, the adversary becomes "noisier" and simpler to locate than if he were able to quietly disrupt a single obscure system that creates complete mission failure.

Active defense finds and responds to sophisticated enemy forces such as advanced, persistent threats. It involves monitoring and responding to adversaries within friendly networks but does not extend beyond them into neutral or enemy networks. Without active defense, the high-level adversaries who slip through our IT-based defense in depth will have unlimited time to examine our systems, discover our resiliency measures, and determine ways to bring down even well-constructed resilient systems. Active defense also provides opportunities to mislead or disrupt an enemy through creatively responding to his attacks and potentially falsifying the effects he produces.

Only if we combine all three approaches can we attain robust mission assurance of the Air Force's core missions in and through cyberspace. Each community has a critical role to play, and each depends on successful implementation of the other categories of cyberspace defense. This combined approach plays to our cultural strengths and experience in joint warfare and can achieve a lasting competitive advantage in and through cyberspace for the United States Air Force. ✪

Notes

[1] Engineers designed many systems during the Cold War to prevent an enemy from listening in on communications; cryptography was very common for war-fighting systems. What was unexpected was that an enemy could use communications to alter the functioning of platforms such as tanks, ships, or aircraft.

[2] For automobiles see Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces" (paper presented at USENIX Security Conference, San Francisco, 10–12 August 2011), 3–5, http://www.autosec.org/pubs/cars-usenixsec2011.pdf; or Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, 21 July 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Stuxnet provides a famous example of a weapon

targeting industrial control systems. For an in-depth analysis, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, [2014]).

3. Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press and Potomac Books, 2009), 465–88.

4. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

5. For a book-length discussion of how response and interaction by adversaries create the paradoxical logic of strategy, see Edward N. Luttwak, *Strategy: The Logic of War and Peace*, rev. and enlarged ed. (Cambridge, MA: Belknap Press of Harvard University Press, 2003).

6. The United States Joint Staff has defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, 5 February 2013, GL-4, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

7. Stuxnet is the best known example of an attack crossing into a well-defended air gap. There are plenty of other examples as well. See P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, [2014]), 63; and Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 323–24.

8. Dr. William Young at Air University developed the key cyberspace terrain-analysis methodology in this paragraph. I use it here with his permission.

9. "Operational Technology (OT)," Gartner, accessed 8 September 2016, http://www.gartner.com/it-glossary/operational-technology-ot.

10. Shon Harris, *CISSP All-in-One Exam Guide*, 6th ed. (New York: McGraw Hill, 2013), 768.

11. Department of Homeland Security, Risk Steering Committee, *DHS Risk Lexicon*, 2010 ed. (Washington, DC: Department of Homeland Security, Risk Steering Committee, September 2010), 26, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

12. For a completer discussion of this concept, see Col William D. Bryant, USAF, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 87–107.

13. Luttwak, *Strategy*, 40.

14. JP 3-12 (R), *Cyberspace Operations*, II-2–II-3.

15. Ibid., II-3.

16. Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (San Francisco: No Starch Press, 2013), Kindle location 263, chap. 1.

17. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 79–84.

18. Department of the Air Force, "Task Force Cyber Secure (TFCS) Team Cyber Assure Out Brief / Way Ahead," presentation (Washington, DC: Department of the Air Force, 1 June 2016); and Department of Defense, *Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)* (Washington, DC: Department of Defense, September 2015), http://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf.

Col William D. Bryant, USAF

Colonel Bryant (USAFA; MA, American Military University; MA, George Washington University; MSS [Master of Space Systems], Air Force Institute of Technology; MAAS [Master of Airpower Art and Science], School of Advanced Air and Space Studies; MSS [Master of Strategic Studies], Air War College; PhD in Military Strategy, School of Advanced Air and Space Studies) is the deputy director, Task Force Cyber Secure, for the Information Dominance and Chief Information Officer, Office of the Secretary of the Air Force, the Pentagon, Washington, DC. The author of *International Conflict and Cyberspace Superiority: Theory and Practice* (Routledge, 2015), Colonel Bryant is a career fighter pilot, strategist, and planner who has served in numerous operational and staff assignments.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

Operational Assessment

So How *Are* We Doing?

Lt Col James S. Welshans, EdD, USAF, Retired
Lt Col Charles Owen, PhD, USAF, Retired
Dr. Alice M. Mulvehill
Col Calvin W. Hickey, USAF, Retired
Robert J. Farrell Jr., DAF, DR-III

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

> *We couldn't afford distorted assessments: too much optimism could prompt us to launch the ground war too soon, at the cost of many lives; too much pessimism could cause us to sit wringing our hands and moaning that the enemy was still too strong.*
>
> —Gen H. Norman Schwarzkopf

Introduction

Throughout history, operational commanders have asked the question, how are we doing? In the 1972 epic *Patton*, actor George C. Scott overlooks a great tank battle in North Africa through his binoculars. The famous commander takes in this expansive view of tanks and close air support on the battlefield, making his personal assessment of the situation.

Modern commanders can no longer conduct effective assessments without advanced sensor capabilities that demand information-management technologies. This situation became apparent during Operation Desert Storm and persists in current global irregular-warfare conflicts. As the appetite for assessment data intensified at an exponential pace over the past 25 years, today's commanders drown in increasingly complex volumes of data.[1] Starting with national and strategic objectives and deriving operational objectives and tactical tasks, commanders must stay attuned to myriad layers of requirements and inputs that frame an overall operational picture of the situation. Today's commanders rely on staff officers and noncommissioned officers (who rely on a variety of distributed and collaborative processes, work flows, and information technologies) to identify relevant data and provide synthesized assessments. The commander must then generate a holistic understanding of the operating environment and fuse it with interpretations and operational assessments (i.e., individualized, cognitive, and low-tech sense making) to render effective and timely decisions.

Modern operational assessment (OA) presents a combined data-management and analytical challenge. The greatest concern for the US military within the context of this dual-faceted challenge is the need for an agile OA framework that can support a human operator who is generally regarded as the critical element (grey matter) and the potential single point of failure in assessment. Although human intellect is the keystone of assessment, it does not preclude or diminish the need for existing and future technologies to support the process. Technologies designed to collect, screen, correlate, represent, visualize, and predictively model the battlespace can significantly expand and enrich the reach and complexity of human analytical thinking. Today's assessment teams must compile, synthesize, and analyze information, ultimately evaluating and estimating operational progress. The rapid advances of information and intelligence, surveillance, and reconnaissance (ISR) technologies have enabled assessors and commanders to better understand and make decisions involving nearly every facet of an operation. However, the complexity and overwhelming volume of incoming data have greatly complicated this critical task.

This article reviews foundational aspects of today's assessment paradigm, focusing on frameworks, research designs, and measurement types. An exploration of ambiguity and uncertainty culminates with a discussion of epistemological nuances. The article advocates a new foundation for assessment anchored in emerging technological innovations, revised OA epistemology, and adaptable representation systems.

US Doctrine and Operational Assessment

One of the greatest challenges facing airmen remains that of assessment: how do we know if we are achieving our objectives? The problem has haunted airmen for decades, but seems little closer to solution than it was in World War II.

—Col Phillip S. Meilinger, USAF

Simply stated, assessment measures the progress of the joint force toward mission accomplishment. Assessment continually compares forecast outcomes with empirically observed action-events to determine overall mission effectiveness with respect to attaining the desired end state, achieving objectives, or performing tasks. The focus is on measuring progress and delivering relevant, reliable feedback into the planning process to adjust operations during execution.

Although the official definition relates assessment to the *military end state*, all commanders and analysts understand that much more than the purely military consequences of an operation are monitored, evaluated, and understood in the assessment process. Carl von Clausewitz emphasized that military operations do not occur in a vacuum but are an outgrowth of a political process that operates according to larger objectives—through its set of actions—and before, during, and after the comparatively brief span of operations.[2] More importantly, military capability is only one of several elements of national power employed to achieve and protect vital national interests and is often not even the most important or the most effective means of exercising a nation's might. When viewed from this perspective, military operations are often shown to be less effective and thus less supportive of a nation's interests than the political, economic, social, and informational *soft power* elements.

Ideally, military force should be applied to operate synergistically with the other soft power elements, but because military action almost always involves either the implicit or explicit application of violence, it is the *bluntest instrument* of national power. Unfortunately, history provides unending examples of nations overreaching in their reliance on military force, often to disastrous ends. As a result, effective and judicious use of military engagement demands a means to ensure it is being applied at times and places and in ways that are most efficacious while minimizing downside risks. OA is the feedback that permits the commander to adjust to changing conditions in an appropriate and effective way to achieve mission goals and objectives. Without assessment, a commander operates blindly and relies on good fortune rather than skill and planning to accomplish the mission.

An effective assessment process must begin at the outset of deliberate military operations analysis and planning—long before (and even if) an actual crisis arises in the particular geographic area of operational responsibility. At this point, commanders and staffs must consider "what to measure and how to measure it to determine progress toward accomplishing a task, creating an effect, or achieving an objective."[3] In addition to the aspects of military operations more traditionally associated with assessment, planners must take into account a wide array of outside factors that may affect planning and execution to assess the impact on progress toward achieving objectives. Consequently, the commander and staff often collaborate (and as necessary, fully integrate) with various nonmilitary governmental agencies and nongovernmental organizations to better detect, analyze, and measure the impact of "friendly, adversary, and neutral diplomatic, informational, and economic actions applied in the operational environment."[4]

Operational Design and Research Design

> *First, anything we study in international security—an event in history, current crisis, speculative future engagement—is almost always more complex than it seems at first glance. Understanding complex national security events requires simplification, and that simplification has become a routine part of how we assess a strategic situation.*
>
> —Andrew L. Stigler
> "Assessing Causality in a Complex Security Environment"

Today's approach to operational planning and assessment is grounded in *operational design* or the "conception and construction of the framework that underpins a campaign or major operation plan and its subsequent execution."[5] Focusing more on generating a deep understanding of operational and environmental complexities than problem solving, this foundational activity helps commanders "visualize the operational environment, understand the problem that must be solved, and develop a broad operational approach that can create the desired end state."[6]

Operational design includes several well-established mechanisms to conduct effective OA. Developed early in the design process, the collection plan offers "a systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements."[7] Further, the OA collection plan identifies all of the commander's critical information requirements, which are "linked to the assessment process by the commander's need for timely information and recommendations to make decisions. The process helps staffs by identifying key aspects of the operation that the commander is interested in closely monitoring and where the commander wants to make decisions."[8]

Evolving beyond current, established processes and products can better align OA with operational design. Taking a broader perspective, one sees that the core of OA is effectively a matter of research, discovery, and interpretive sense making, grounded in rigorous, scientific, and adaptive research designs. Normally, these designs involve hypothesis testing across an effect or outcome-based framework (i.e., if action, then effect/outcome) or an independent variable = > treatment = > dependent variable design. Jennifer Mason anchors research design into three broad questions. First, what is my research about, or what phenomenon is to be investigated? Second, what is the strategy or proposed research hypothesis that would link research questions, methods, and evidence? Finally, how will the proposed research take account of relevant ethical, political, and moral concerns?[9] Research designs, therefore, combine "theoretical claims [hypotheses] and empirical evidence [indicator data] to produce an argument that answers the research question or problem that the study examines."[10] Today's operations analysts use routine office-product software or other specialized software (e.g., maps or scheduling tools) to support their investigation. Analysts then generate evidential data to answer the questions of who, what, when, where, and how of what was executed against the why that drove the planning in order to determine what, if anything, should be done next.

If the world stayed still, this process would be rather simple. But change over time is inevitable, and military operations involve motivated adversaries intent on achieving their objective(s) while simultaneously preventing us from attaining ours. Therefore, OA research designs must be flexible and adaptive. Emergent design addresses these concerns, "allowing for and anticipating changes in [assessment] strategies; procedures; questions to be asked; ways of generating data, and so on."[11] Emergent design processes, focused on innovative discovery and continuous adaptation, almost evoke a biological model in which

> the actual analysis would be less like a pre-specified process of testing and verification and more like discovery. Analysis unfolds in an iterative fashion through the interaction of the processes of generating data, examining preliminary focusing questions, and considering theoretical assumptions. Analysis thus becomes a process of elaborating a version of, or perspective, on the phenomenon in question; revising that version or perspective as additional data are generated and new questions asked; elaborating another version; revisiting that version or perspective, and so on.[12]

Instead of organizing findings in prescriptive and static knowledge category bins, emergent design anticipates and accommodates necessary interactions between the analyst and the data to generate fresh new frameworks and perspectives. It is not the evidential data that informs here but the cognitive meanings generated by and adapted from the myriad relationships among the data elements. Essentially, emergent design delivers the foundation for learning.

Measurement

> *On a cautionary note, do not try to link Measures of Performance (MOPs) with Measures of Effectiveness (MOEs). Doing things right does not necessarily mean you are doing the right things. MOPs and MOEs look at different things. MOEs and their supporting indicators measure the operational environment without regard for the MOPs and tasks. Within the assessment process, MOEs and MOPs are only looked at together during deficiency analysis. Lessons learned indicate that trying to build a linkage between MOP and MOE is a proven waste of time for staffs.*
>
> *—Commander's Handbook for Assessment Planning and Execution*

Data (relevant indicators applicable to the phenomenon of interest) are the sources for measurement and the outcomes of measurement. The act of measurement imbues data with two qualities: *accuracy* and *precision.* Unfortunately, these two concepts are often misunderstood and are used interchangeably or, worse, in a context where being precise is to be considered better than merely being accurate.

The accuracy that pertains to data obtained through measurement is defined as the "closeness of agreement between a measured quantity value and a true quantity value of a measurand."[13] This definition expresses the first critically important quality of measurement-derived data: the *measurand* is the quantity or object intended to be measured, but because all measurement is never free of error, no matter how exactingly it is performed, there is always some variance between the resulting data and (the epistemologically unknowable) ground truth. Furthermore, the concept of measurement accuracy is not a quantity and therefore is not given a numerical quantity value. Instead, a measurement is said to be more accurate when it offers a smaller measurement error. Measurement accuracy should not be confused with measurement trueness or the closeness of agreement between the average of an infinite number of replicate measured quantity values and a reference quantity value.

Data precision refers to the "closeness of agreement between indications or measured quantity values obtained by replicate measurements on the same or similar objects under specified conditions."[14] This definition introduces the second critically important quality of measurement-derived data, the *exactness* (i.e., repeatability) of the measurement act itself and the resulting agreement (or lack thereof) between data derived from repeated measurements. The specified conditions can be repeatability conditions of measurement, intermediate precision conditions of measurement, or reproducibility conditions of measurement. As a statistically derived term, measurement precision is usually expressed numerically (i.e., standard deviation, variance, or coefficient of variation). When applied in the OA context, measurements must, therefore, address these critical aspects of accuracy and precision, not only to generate assessments regarding how closely our executed operations achieve desired outcomes but also to make reasonable estimates of our success (or lack thereof) in achieving objectives.

Representing Precision and Accuracy in Indicators

An indicator is defined as a "specific piece of information that shows the condition, state, or existence of something, and provides a reliable means to measure performance or effectiveness."[15] Furthermore, "indicators are developed by identifying the data needed to answer intelligence and information requirements. Operation assessment is an iterative process that depends on accessible data sources and professional military judgment. Judging effectiveness and the degree of progress often depends on establishing trend lines for particular indicators in context with appropriate outcomes."[16]

Precision is achieved in indicators by stating the degree of specificity required in the data derived from the resulting measurement. Accuracy can be enhanced by obtaining data through means and sources most sensitive or closely attuned to those changes in enemy behaviors that an analyst is expecting to observe—especially if the analyst employs multiple means and sources rather than relies on a single or a few favorites.

Careful representation of data will incorporate a combination of numeric and textual qualifiers that reveal the information's precision and estimates of its accuracy; however, the exact form of conveying the precision and accuracy of the data will depend on the exact nature of the data being represented. For example, the intended and actual impact points of a weapon may be conveyed through a three-dimensional geographic coordinate in which the precision is expressed as the significant digits employed in the horizontal and vertical measurement. The accuracy is expressed as an estimate of the circular (horizontal plane) and linear (vertical plane) error. In the case of nonquantitative assessment data such as a poststrike mission report, however, precision is a direct function of the specificity of detail included in the report text. Furthermore, accuracy is dependent upon the extent to which any of those details can be corroborated by other sources, such as an onboard sensor video, the observations of other aircrews involved in the attack, and poststrike ISR reporting. Nevertheless, if data are to be used to maximum effectiveness for OA, the information must be represented in ways that properly reflect its level of precision and estimate of accuracy. Even more importantly, to make use of the data, OA team members must be thoroughly conversant with the principles underlying these qualities.

Representation of the data also involves bias—expressed as the human's natural tendency to seek consistency and orderliness in the natural world. In short, we seldom perceive the world as it is, unconsciously opting instead to see the world as we wish it to be. Thus, the implication for OA is to evaluate data populations or samples, gravitating toward measures of central tendency and normal (i.e., Gaussian) distributions as the taken-for-granted standard approach. Perhaps an objective and critical analysis of these human tendencies would reject center-of-mass outcomes, instead actively exploring outliers (i.e., Black Swan events), given their proclivity for greater significance and severity of consequences.[17]

That said, what data sources will provide the best answers about indicators and measures associated with the attainment of one or more objectives? Most assessors find that "there is a tendency to overstate the number of measures and indicators needed, thus generating huge data collection requirements . . . [even though] lessons learned indicate that more information does not necessarily translate into a better assessment."[18]

Uncertainty and Ambiguity

> *Uncertainty is fundamental in nature, rather than just a residual insufficiency of information. Truth is not buried in the data, information does not bring about knowledge, and the best answer is not normally within reach even in principle.*
>
> —Darryn J. Reid and Lt Col Ralph E. Giffin
> "A Woven Web of Guesses, Canto Three"

The measures and indicators developed during mission analysis are likely to be incomplete. Generating a list of possible measures and indicators for each desired objective serves as a starting point at which the responsibilities for measurement are assigned to available resources. Additionally, assessment is made difficult by two pitfalls that are part of the process: the asymmetry of human perception and the ambiguity that infects all data.

Asymmetry of perception arises from the fact that no two people will arrive at exactly the same conclusions regarding observed events or circumstances. We all tend to look at everyone and everything through a complex and often subtle interpretive framework. This framework is built over a lifetime of acquired experiences and learning (i.e., wisdom), and it functions as an essential device that enables us to make sense of our world. This interpretive framework is a direct consequence of the uniquely human attribute of self-awareness. Nevertheless, we also need to recognize that this framework tends to become entrenched over time as we collect experiences.

The result is a feedback effect that causes us to develop set interpretations of objects and events that seem to bear some sufficient level of similarity with these past experiences. In no small measure, this interpretive typing is attributable to the second pitfall for assessment—the inherent ambiguity that infects all data. Even the most objectively analytical people must admit to the influence of subjectivity and inherent bias. Also, the effect of asymmetric perceptions needs to be considered in light of the fact that the same pitfall afflicts our enemy when he experiences our offensive and defensive operations and when he plans, executes, and assesses operations against us.

Iraq's Air Force in Desert Storm

Before Operation Desert Storm, judged on quantitative and qualitative measures, Iraq possessed one of the most advanced and formidable air forces in the region. However, once combat commenced, the Iraqi air force was rarely employed and never posed a meaningful threat to coalition air or ground operations.

The asymmetry that drove the ineffective use of Iraq's air force had nothing to do with qualitative or quantitative assessments of capabilities; the asymmetry existed in Saddam Hussein's worldview and colored his decision making. He always kept his air force under close watch and on a short leash; he had good reason to be wary. Including some of the most advanced and foreign-educated members of the Iraqi military, the air force was a traditional source of conspirators at the center of previous coups against Iraqi leaders and was even involved in repeated attempts to depose Saddam himself. Thus, when the time finally came when Iraq's air forces could have been employed to far greater effect against the coalition, Saddam's asymmetric perspective toward his air arm dictated a course of events that seemed paradoxical to our thinking about how to best use a modern air force. Therefore, the targeting of much of his air force proved to be of little or no consequence to the actual course of the war, particularly considering that within the first weeks of the war, more than 125 aircraft and a substantial number of pilots fled to Iran.

For more information on this subject, see 1st Lt Matthew M. Hurley, USAF, "Saddam Hussein and Iraqi Air Power: Just Having an Air Force Isn't Enough," *Airpower Journal* 6, no. 4 (Winter 1992): 4–16.

Although asymmetric perceptions and ambiguity are closely linked and both conspire to complicate assessment, data ambiguity is a profoundly more intractable problem than our inability to objectively discern how things fit together. This difficulty arises because it is impossible to obtain every detail on any matter; there are always known and unknown issues associated with every element of information we receive. Given the complexity of modern warfare, the sophistication of our capabilities, and the expectations of our political leaders, this reality is almost ironic for the assessment process.

Moreover, the increasingly lopsided emphasis on technical intelligence and ISR in recent decades, as well as the stunning detail often revealed by these capabilities, often leads to unwarranted expectations for their truthfulness. For example, a sensor can see only what is in its field of regard and whatever is in the slice of the spectrum in which it is designed to observe and collect, but it is incapable of making a value judgment as to the veracity or meaning of what it is observing. In the case of the cited example of the a priori assessment of the Iraqi Air Force, the fact that Saddam possessed this relatively modern and rather sizeable military capability extended to an unwarranted presumption that he would employ it in the same manner as our own.

Try as we might, the attainment of explicit knowledge is a complex and elusive endeavor. As a result, assessment is itself a representation problem because of the constant struggle to get around our human inability to see things for what they truly are (perception) and to mitigate to the maximum practical extent our inevitably incomplete knowledge of the facts (cognition). This struggle requires analytical methodologies, processes, and technologies that demonstrate the potential to reduce or minimize the impact of perceptual asymmetry and ambiguity while at the same time recognize that their influence can never be completely eliminated.

Epistemology and the Operational Assessment Process

Leaving causal assumptions unstated raises the risk of taking action in the strategic realm that is founded on inaccurate expectations of causal relationships. Exploring potential vulnerabilities in our causal reasoning is by no means a guaranteed bulwark against error, but the complexity of today's strategic environment demands it.

—Andrew L. Stigler
"Assessing Causality in a Complex Security Environment"

Many rich theories describe alternative approaches to epistemology or the study of knowledge and justification. Although not exclusive to folks from Missouri, empiricists would anchor our understanding of the world in authentic, primary sense experience. For example, viewing fresh poststrike imagery of a severely damaged building would suffice as credible evidence of positive mission outcomes. Rationalists build on this empirical framework, adding reason as a logical extension to our sensory perceptions. Here, a simple cause-and-effect logical premise (i.e., *strike mission activity* = > *damaged building*) would then complete the knowledge model. When these foundationalist perspectives "seek permanent, indisputable criteria for knowledge . . . and a preoccupation with establishing correspondence between idea and object, concept and observation," they represent today's dominant approach to OA.[19] Dr. James S. Welshans points out that

> despite our best efforts at objectivity, human observation and analysis are fundamentally a subjective enterprise. Each objective measurement is only as precise as the subjectively established (i.e., culturally dominant and accepted) threshold. The researcher does not simply find data which already exists in a collectable state but instead must create viable frameworks for how to best generate and represent data from the chosen sources. Therefore, the data generation and representation processes involve activities that are intellectual, analytical, and interpretive.[20]

In addition to being the foundation of what we already know, knowledge is the framework for evaluating and incorporating new experiences and information. Our existing knowledge is used to create new knowledge. New events, experiences, and information interact with a priori observations, interpretive patterns, implicit assumptions, and beliefs. The expertise, insight, experience, and judgment of the experienced assessor cannot be easily codified, nor can it be easily shared as information. Consequently, the linchpin to making such knowledge more productive is to create or provide a sound methodology for thinking and to place enhanced emphasis on the relationships and networks between war fighters to enable knowledge to proliferate, be tested, and used most effectively. We propose a broader and more intellectually inclusive epistemology for OA that will shift our focus from exclusive notions of causality to accommodate notions of meaning. This approach should blend philosophical elements of critical social science and standpoint theory to offer a more intellectual, analytical, and interpretive environment for effective OA.

Critical social science seeks to integrate theory and practice to develop awareness of "contradictions and distortions in belief systems and social practices . . . [that] do not measure up to their own standards and are internally inconsistent, hypocritical, incoherent, and hence comprise a false consciousness."[21] We need to redefine our OA approaches with a healthy skepticism and understanding of the limits of empirical evidence and rational judgment. Today's OA analyst never truly interacts with primary evidence, but secondary (and nth order) artifacts—whether imagery, mission reports, or intelligence summaries. Whether taken individually or collectively, our text-based data elements are at best representative models of reality, as evidenced by alternative approaches offered from a research culture perspective (e.g., database structures or semantic ontologies). Mediated by the imperfections of human language, our information objects absolutely deserve a critical eye. Yet, this same symbols-based language framework adds the nuanced richness of tacit knowledge and authentic human experiences that enables sense making, learning, and shared understanding.

Standpoint epistemologies also criticize universal and objective interpretations of knowledge as unauthentic, ineffective, and incomplete. Knowing must begin with broad exposure to the experiences, interests, and values of diverse stakeholder groups and continually adapt by challenging the taken-for-granted and deconstructing the dominant perspective in active learning. *Views from everywhere* replace the outsider-observer view from nowhere to frame the analytical space, and, as such, it is "impossible to imagine uniting them into a single complete or collective view of what knowledge is."[22] The best we can hope for is the mosaic picture, the dot-matrix printout, and the highly qualified analytical text. Knowledge is ever incomplete; humans live with uncertainty and contradictions while generating informed assumptions.

Conclusion

Once in a while you get shown the light

In the strangest of places if you look at it right.

—Robert Hunter and Jerry Garcia
"Scarlet Begonias"

The best assessment practices tell us that "predicting outcomes in complex environments is problematic at best. Conditions change, adversaries adapt, missions shift, and objectives evolve. . . . As environmental conditions, political considerations, and operational realities collectively influence the successful accomplishment of developed objectives, the commander and staff must review the underlying assumptions and conditions that provided the foundation for their assessment."[23]

The commander who is unable to accurately and rapidly assess ongoing operations and relevant nonoperational events is a commander who is failing and unable to accurately make the necessary resource-allocation and operational-adaptation decisions. While crude mechanisms exist to work this analysis, they are inadequate to the challenge and overly reliant on the input of a very small number of humans. Furthermore, they currently lack a credible data foundation to ensure reasonable accuracy in both analysis and projection while accounting for innate and systemic biases and ambiguities.

Assessment is clearly more art than science. The artfulness of reasoning is the only thing that enables humans to intuit their way through the ambiguity and asymmetric perceptions that are the inextricable consequences of living life, but modern science also has a big part to play. Experienced analysts generally find that effective assessment requires significant measurements and that often the most important data are missing. Additionally, a high likelihood exists that the most likely times and places where data are missing coincide with the times and places where data are most critical. Although operational planning and execution are not deterministic, a good analyst or planner can generally estimate—with a high degree of confidence—how causes, effects, and consequences will unfold.

Clearly, what is needed is a way to both accumulate and organize the massive amounts of information required to support effective OA, enabled by means that allow operational analysts to visualize and represent those data in an intuitive and easily managed format to assist the commander in making decisions based on that information without overwhelming him or her with unnecessary or not immediately relevant detail. Note that some progress is already being made to support the data volume, velocity, variety, and veracity issues faced by the OA analyst with programs supported by agencies like the Defense Advanced Research Projects Agency.

That agency is heavily focused on programs to analyze and manage big data, with investments directed at advancing such areas as algorithms, analytics, and data fusion—and growing from just under $97 million in fiscal year 2014 to more than $164 million in fiscal year 2016.[24] If representational languages and automated reasoning technology can lift some of this fog shrouding OA analysts from key insights as they sift through voluminous data, that capability would be of enormous value. The Air Force Research Laboratory is leveraging this work in its pursuit of improving synchronized planning and execution across and within the air, space, and cyber mission elements to achieve decisive unities of effort within heavily contested environments. Effective, efficient OA grounded in an agile framework is paramount to doing so. ✪

Notes

[1] Lt Gen David A. Deptula, USAF, Retired, "A New Era for Command and Control of Aerospace Operations," *Air and Space Power Journal* 28, no. 4 (July–August 2014): 5–16.

[2] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75–99.

3. Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations*, 24 February 2014, III-14.

4. JP 5-0, *Joint Operation Planning*, 11 August 2011, Appendix D, "Assessment," D-2.

5. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 February 2016), 175.

6. Joint Chiefs of Staff, J-7 Joint and Coalition Warfighting Division, *Planner's Handbook for Operational Design*, version 1.0 (Suffolk, VA: Joint Chiefs of Staff, J-7 Joint and Coalition Warfighting Division, 7 October 2011), I-2.

7. JP 1-02, *Department of Defense Dictionary*, 36.

8. JP 3-31, *Joint Land Operations*, III-14.

9. Jennifer Mason, *Qualitative Researching*, 2nd ed. (London: Sage Publications, 2002), 27.

10. Thomas A. Schwandt, *Dictionary of Qualitative Inquiry*, 2nd ed. (Thousand Oaks, CA: Sage Publications, 2001), 229.

11. Ibid., 63.

12. Ibid., 64–65.

13. *International Vocabulary of Metrology—Basic and General Concepts and Associated Terms* (*VIM*), 3rd ed. (Paris: Joint Committee for Guides in Metrology, 2008), 21.

14. Ibid., 22.

15. Joint Doctrine Note (JDN) 1-15, *Operation Assessment*, 15 January 2015, GL-4.

16. Ibid., A-5.

17. "A black swan is an event or occurrence that deviates beyond what is normally expected of a situation and is extremely difficult to predict; the term was popularized by Nassim Nicholas Taleb, a finance professor, writer and former Wall Street trader. Black swan events are typically random and are unexpected." "Black Swan," *Investopedia*, accessed 20 September 2016, http://www.investopedia.com/terms/b/blackswan.asp.

18. JDN 1-15, *Operation Assessment,* I-11.

19. Schwandt, *Dictionary of Qualitative Inquiry*, 71.

20. Dr. James S. Welshans, "Truths, Torments, and Togas," *ITEA Journal* 34, no. 3 (September 2013): 220.

21. Schwandt, *Dictionary of Qualitative Inquiry*, 45.

22. Ibid., 239.

23. JDN 1-15, *Operation Assessment*, I-5.

24. Jonathan Lutton, "DARPA Is Spending Big on Big Data," *FCW: The Business of Federal Technology*, 15 April 2015, http://fcw.com/articles/2015/04/15/snapshot-data-programs.aspx.

Lt Col James S. Welshans, EdD, USAF, Retired

Dr. Welshans (USAFA; MS, Troy State University; EdD, University of West Florida) is a former active duty Air Force fighter pilot, instructor, and war planner. Currently president and chief operating officer with LectricSix Solutions, Inc., he advises the Air Force Research Laboratory on military command and control projects and technology transition. A founding member of the Air Force Operational Command Training Program, Dr. Welshans taught strategy and operational assessment to senior military officers worldwide during major command and control exercises. He has five years of experience teaching at the collegiate level and is a member of the adjunct faculty at Air University and the US Marine Corps University.

Lt Col Charles Owen, PhD, USAF, Retired

Dr. Owen (MBA, Louisiana Tech University; PhD, Louisiana State University) is a senior training and intelligence consultant with PatchPlus Consulting, Inc. He provides training, intelligence, and policy subject-matter expertise to Department of Defense and intelligence community customers. His areas of expertise include training development, targeting, and intelligence analysis. Dr. Owen served for 20 years on active duty as an Air Force intelligence officer, deploying to four contingencies: Operations Desert Storm, Southern Watch, Allied Force, and Enduring Freedom. He has five years of experience teaching at the collegiate level and is a member of the adjunct faculty at Indiana Wesleyan University.

Dr. Alice M. Mulvehill

Dr. Mulvehill (BS, MS, PhD, University of Pittsburgh) is a research scientist and consultant with extensive experience in the design and development of mixed-initiative, knowledge-based decision-support systems. She participated in several Defense Advanced Research Projects Agency and US Air Force research programs focused on providing advanced computing technology to military planners in support of course-of-action development, air campaign planning and execution, logistics planning, and adaptive model development. Currently, Dr. Mulvehill is president and chief operating officer of Memory Based Research, LLC.

Col Calvin W. Hickey, USAF, Retired

Colonel Hickey (BS, University of Akron; MS, Golden Gate University) retired after a 30-year career in the Air Force's regular and reserve components. He was commissioned through AFROTC in 1970 and entered the Air Force as a mapping, charting, and geodesy officer. He spent 12 years on active duty, primarily involved in operational targeting, the geospatial sciences associated with weapons and weapon system development, and associated issues related to operational planning. In 1982 Colonel Hickey left active duty to begin a career in Civil Service. From 1987 until his retirement in 2008, he served as a Department of Defense civilian working in the targeting discipline and related geospatial intelligence sciences. Among other accomplishments during his military and civilian careers, he has taught targeting, been involved in the development of modeling and simulation for weapon-effects estimation, and advised on geospatial data dependencies of weapons and weapon systems. Colonel Hickey continues to apply his particular blend of subject-matter expertise to national security issues in semiretirement as a consultant.

Robert J. Farrell Jr., DAF, DR-III

Mr. Farrell (BS, MS, Pennsylvania State University) is a senior software program engineer, Resilient Synchronized Systems Branch, Information Systems Division, Air Force Research Laboratory, Air Force Materiel Command, Rome, New York. He leads the discovery, development, and integration of innovative computer-automated decision-support technologies that give resilient command and control capabilities to Air Force and joint decision makers. These capabilities enable synchronized planning and execution across and within the air, space, and cyber mission elements to achieve decisive unities of effort, all within heavily contested environments. Mr. Farrell has 34 years of experience keeping the US Air Force the best in the world.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

Suborbital Strike!

The Use of Commercial Suborbital Spacecraft for Strike Missions

Capt Daniel J. House, USAF
Dr. John Tiller
Dr. John Rushing

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

In combat, aircraft survivability can be distilled to five key components: altitude, airspeed, battle damage absorption, emissions control, and connectivity. Since the 1980s, the US Air Force has concentrated solely on decreasing emissions and increasing connectivity to improve aircraft survivability. At the same time, the maximum airspeed and maximum altitude of the service's aircraft have actually decreased, presenting an adversary with targets that must operate well inside the threat's engagement zone.

This article reviews a concept for the use of commercial suborbital spacecraft for military purposes, allowing the Air Force once again to enhance survivability via altitude and airspeed. By utilizing commercial technology, suborbital spacecraft will be able to reach the battlefield faster than aircraft generated by the traditional procurement process, just as the Liberty program rapidly fielded effective combat aircraft.[1] Higher altitude and airspeeds will give legacy ordnance greater capabilities and permit the use of kinetic-only weapons such as hypervelocity rod bundles.[2] Finally, suborbital spacecraft will reset the clock for antiaircraft defense by flying and striking from outside the weapon engagement zone (WEZ) of current systems, thus negating most antiaccess, area-denial (A2AD) strategies. This action will force potential adversaries to spread out their limited research and procurement dollars into new weapon systems, either reducing the number of current systems they can support or leaving glaring, fatal holes in their defense posture.

Aircraft Survivability

Every aircraft, whether manned or remotely piloted, is launched on its mission with the assumption that it will survive at least to the point where it can successfully attack the enemy and, kamikazes notwithstanding, with the assumption that it will return to base for use on later missions. Traditionally, aircraft survivability has included four capabilities. The first capability is altitude—the ability to overfly adversaries' defenses—first demonstrated with high-altitude bombing by German zeppelins over London in World War I. The zeppelins flew too high for both antiaircraft artillery (AAA) and British fighter aircraft to reach.[3] From that time until the mid-1960s, aircraft attained higher altitudes to avoid the enemy's WEZ. The top two American platforms for altitude were the U-2, having a maximum altitude of above 70,000 feet, and the SR-71, above 85,000 feet. With the exception of the XB-70, which had a planned altitude of 77,000 feet, every Air Force aircraft since then has been designed for a maximum altitude of 50,000 to 60,000 feet.[4] Compare the SA-2, the oldest Russian surface-to-air missile (SAM) still operationally used, which had a maximum altitude of 72,000 feet and a range of 16 nautical miles (nm) with its original missile iteration, and the SA-20, which has a maximum altitude of 82,000 feet and range of more than 100 nm. Evidently, SAM designers have been concentrating on extending range over increasing altitude.[5]

The second capability is airspeed—the ability either to outrun the adversary's interceptors or to fly by too fast for his defenses to respond and engage. Once again, the SR-71 boasted the maximum developed airspeed with its Mach 3+ capability, and the XB-70 was designed for Mach 3.1. The Russians tried to defend against these threats by developing both high-speed interceptors (the MiG-25 and MiG-31) and a more capable air-to-air missile (the AA-9 Amos) although they never successfully shot down the fast-moving SR-71.[6]

The third capability is battle damage absorption—how well the platform can take a hit and keep flying. Both the A-10 Warthog and Su-25 Frogfoot were designed for close air support, operating in areas of heavy AAA. Multiple times they have returned safely to base despite being hit by missiles and AAA.[7] Although these aircraft are specially designed to withstand battle damage, the newest ones entering the fleet are not as robust.

The fourth capability, emissions control, involves control of both internally generated emissions (e.g., onboard radars, radios, data links, heat, and sound) and either the absorption or controlled deflection of off-board-generated emissions, such as enemy radars. Since the successful deployment of the F-117 in Operation Desert Storm, the Air Force has concentrated on emissions control as its primary means of improving aircraft survivability, specifically in relation to enemy radar emissions. The issue with this course of action is the fact that people are forgetting their basic physics. It is impossible to create an aircraft that has no emissions. Eventually the enemy will create a sensor sensitive enough to pick up said emissions, separate them from the environmental noise, and target the friendly aircraft. Second, even if one manages to decrease emissions in one part of the spectrum, one is either unable to lower them in another part or in some cases make them even worse. A good example is the controversial F-35. Even though it has low-observable capability in the S-band radar frequency range, it is less capable in the VHF and L-band, which provide a potential window for targeting.[8] Another issue concerns an aircraft's infrared emissions. Aircraft invariably heat up when they travel at high speeds through the air. One could easily imagine an opponent enhancing or replacing his integrated air defense system (IADS) radars with infrared search and track sensors on every SAM system.[9] The point here is that the easiest way to upgrade an antiaircraft missile, radar, or interceptor is to upgrade and replace the sensors. Sensor technology is constantly improving, and with globalization, possible enemies are quickly catching up in this field. After the development of a sensor technology that can counter stealth by focusing on other emissions, it will spread to our adversaries nearly overnight, significantly minimizing the benefits of stealth.

The fifth point of aircraft survivability—connectivity—has become of key importance only in the past 25 years. Connectivity has to do with the aircraft's ability to relay data in the form of location, orders, or target information. Connectivity began with light guns and flares to pass simple commands such as take off and land before it progressed to radios for relaying orders and increasing situational awareness and to "identification, friend or foe" for fast, accurate identity checks. At these junctures, it was still possible for the aircraft to fight effectively, even when connections failed because of jamming or equipment problems. In recent years, however, it has led to data links passing situational awareness first and now targeting data—and even to the successful development of remotely piloted vehicles. Manned combat aircraft can still recover to their home base, and most remotely piloted vehicles have lost-link procedures to return to base as well, but both are rendered combat ineffective as soon as their links are severed, putting them at much greater risk of destruction. The reliance on links has come to the point that in comparisons of the F-35 and Su-30, the F-35 can be effectively employed only if it has garnered off-board sensor situational awareness. That is, for the F-35 to win, it needs the presence of an Airborne Warning and Control System (AWACS) aircraft. If the AWACS is jammed or shot down, then the F-35 would not be able to compete against the more capable fighter.[10] In 1992 during an air show in Moscow, Russia announced that its Kh-31 (AS-17) antiradiation missile had been modified specifically to target AWACS with a range of nearly 100 miles.[11] One can compensate for this vulnerability by pulling back the AWACS and other high-value airborne assets but with a subsequent cost in sensor range and capability.

Such loss would decrease the effectiveness of every allied platform because of the networked connectivity inherent in today's airpower, making friendly aircraft quite susceptible to attack. Figure 1 compares the survivability of the F-22, F-35, SR-71, and U-2.

Connectivity	
Line-of-sight radio	1
High-frequency radio	2
Tactical digital information link (Tadil) J	3
Advanced data Links	4
Satellite communications	5

Stealth (radar cross section, square meters)	
100+	1
10–100	2
1–10	3
0.1–1	4
<0.1	5

Altitude (feet)	
0–20K	1
20–40k	2
40–60k	3
60–80k	4
80k+	5

Airspeed (Mach)	
0–1	1
1–1.5	2
1.5–2.0	3
2.0–3.0	4
3.0+	5

Battle Damage Absorption	
1 engine	1
Radar warning receiver	2
Chaff / flare	3
2 engines	4
Armor	5

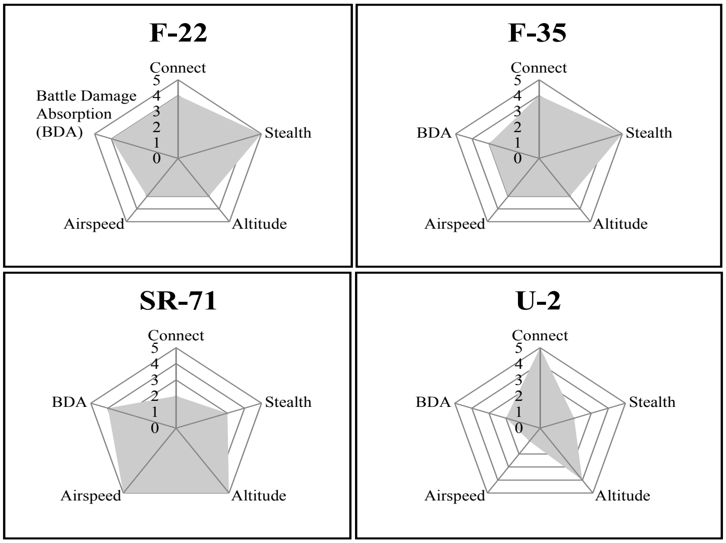


Figure 1. Survivability comparison of the F-22, F-35, SR-71, and U-2. (For the radar cross-section numbers, see Wing Cdr Chris Mills, "Air Combat: Russia's PAK-FA versus the F-22 and F-35," Air Power Australia, 30 March 2009, http://www.ausairpower.net/APA-NOTAM-300309-1.html.)

Enter the Suborbital Spacecraft

As we previously saw, the use of stealth and connectivity as the only means of increasing aircraft survivability has been outmaneuvered by recent Russian and Chinese IADS technological development. Since these systems are sold around the world, any adversary could have the advanced antiaircraft systems necessary to make any conflict very costly for the Air Force. Given both the advanced capabilities and current timeline required to bring a new airframe to the fleet, the authors of this article recognized the need to return to higher altitudes and airspeeds and to increase the speed of procuring new aircraft.

In 2012 Captain House, one of the authors, wrote his thesis on using a commercial suborbital spacecraft in a strike capacity.[12] To be considered suborbital, a vehicle must pass the Karman Line, which is set at 100 kilometers (km), requiring a vertical velocity of 1 km/second without sufficient forward velocity to enter orbit (7 km/second). Inside this zone, the vehicle will enter a ballistic trajectory that will take it into space but not keep it in orbit.[13] The authors reviewed four commercial vehicles, selecting Virgin Galactic's SpaceShip Two for analysis because it had the greatest payload capacity and was furthest along in development. Modifying the spacecraft, hereafter referred to as the Militarized SpaceShip 2 (MSS2), for a strike role allowed it to carry 2,000 pounds of ordnance—the equivalent bomb load of an F-22 in air-to-ground loadout—and a range of 700 nm.[14]

Using the desktop computer simulation "Modern Air Power" software by John Tiller, the authors analyzed the MSS2 against both a legacy IADS employed in Iraq and Libya and a modern IADS with newer systems, such as the SA-12 and SA-20. These same scenarios were run for a standard strike package, a cruise missile strike, and a stealth bomber strike for comparison against two target sets—one in a shallow strike (i.e., 50 miles of the forward edge of the battle area [FEBA]) and a deep strike (i.e., 200 miles inside the FEBA). The analysis showed that although the four MSS2s could not match the payload weight of a B-2, they were just as capable of penetrating a modern IADS. The standard strike package and the cruise missile strikes were both decimated in these environments.

The authors further refined these analyses and tested the modern IADS scenario on a Linux cluster computer. Dr. Tiller and Dr. Rushing, coauthors of this article, ran each of the four strike scenarios 10,000 times and aggregated the results. The air interdiction combat air patrol was modified to be more aggressive against friendly aircraft, and the cruise missiles were rippled fire—rapidly fired to overwhelm the enemy IADS instead of single shots to minimize exposure to individual cruise missiles. These actions increased the score of the cruise missiles compared to that of the B-2, but the scores of the standard strike package, B-2 strike, and cruise missiles were still well below the MSS2's. Figure 2 shows the aggregate results of the simulations, the horizontal line representing the scenario outcome score and the vertical line, the number of results for that outcome. Results to the right are better for the friendly side and worse for the enemy. The aggregate score is based on damage to target and Red and Blue losses that were recorded for each run.

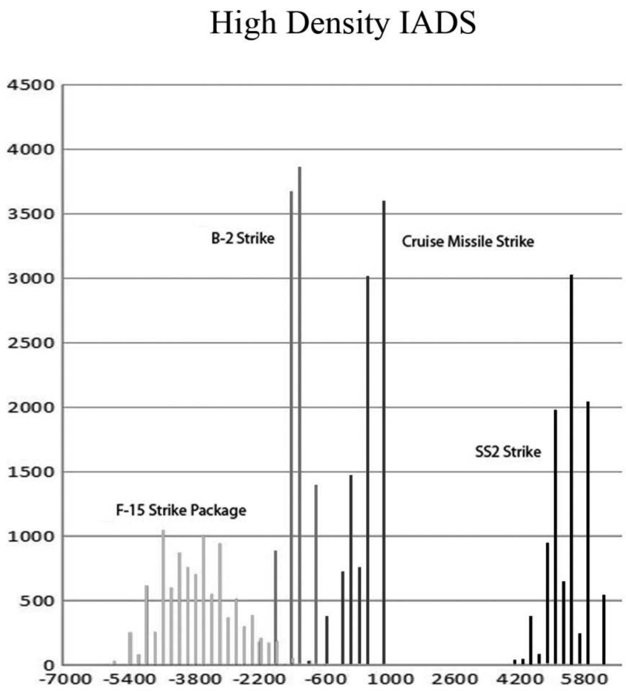


Figure 2. Comparison of four strike capabilities

In the summer of 2013, the suborbital concept was evaluated in the Air Force Research Laboratory's Advanced Concepts Exercise (ACE) 13, which used the MSS3, based on press releases' hints about the capabilities of the future SpaceShip Three (SS3). At that time, SS3 was still believed to be a long-range suborbital spacecraft for point-to-point service although it is possible that it will prove capable of orbit if unveiled. For the ACE 13 test, MSS3 had a payload of 2,500 pounds and a range of 5,500 nm. The results are classified, but the test did show that MSS3 could carry out deep strikes beyond current capabilities and proved immune to present and upcoming IADS systems.

Why So Effective?

The MSS2 concept is effective not simply because it flies outside the range of an enemy IADS. Rather, the spacecraft breaks the kill chain in multiple locations. The kill chain—the steps in dynamic targeting more commonly known as find, fix, track, target, engage, and assess—is the engagement cycle necessary to go from initially acquiring a target to successfully neutralizing it.[15] Earlier, the article noted that stealth is now the primary means of enhancing aircraft survivability. Stealth works by breaking the kill chain at the first step, making it very difficult to find the aircraft. If a B-2 is flying over an enemy nation in broad daylight and an enemy aircraft spots it, the pilot will be more than capable of fixing, tracking, targeting, and engaging the bomber. The pilot may be limited to either heat seekers or guns, but he or she will still be able to employ the kill chain successfully and take out the B-2.

All that a potential adversary must do to repair this break in the kill chain is invest in and develop sensors capable of detecting stealth aircraft, either by improving the sensor sufficiently to pick up the minuscule returns or using other sensing methods such as sounds, lasers, or heat to search the environment. Once the means of finding the aircraft is sufficiently developed, the enemy can employ either standard air defense fighters to take out our stealth aircraft or upgrade his SAMs with antistealth capability.

This development of antistealth technology is not a radical idea. More than 15 years have passed since an F-117 was shot down over Serbia, and even though some questions remain over whether recovered debris from Vega 31 made it into the labs of Russia and China, both countries have recently unveiled stealth aircraft of their own. The limited number of Russian and Chinese stealth aircraft is not too worrisome in a contingency scenario, but the fact that they exist should put fear into stealth drivers' hearts because both countries can now train their radar and SAM operators to pick out stealth platforms while exercising against real stealth aircraft. When the US Navy lost its anti-submarine-warfare experience during the force shaping following the collapse of the USSR, it rebuilt that knowledge base by training against its own submarines.[16] For the first time, enemies can do the same thing in a peacetime environment against stealth and have sufficient time to see which tactics, techniques, and procedures work and which don't, putting them that much further ahead of the learning curve on day one of the battle.

Unlike stealth platforms, suborbital spacecraft break the kill chain in two different locations. First, like stealth vehicles, they hide the aircraft. Stealth platforms do so by hiding from the radar even though they are within its effective envelope. Suborbital spacecraft operate outside the radar's field of view. Modern radars, especially the early warning types, are designed to look at very long ranges horizontally along the surface of the earth and slightly above. There has yet to be a threat to radars in the suborbital realm, so they are not designed to look upwards. For example, the FPS-117 long-range radar has a maximum range of 180 nm, but its maximum elevation is 20 degrees. That is, the maximum altitude the radar can see is 60 nm—and only at the maximum range. The radar's maximum altitude will drop 1 nm for every 3 nm closer to the radar.[17] Without targeting information, the rest of the kill chain cannot be prosecuted.

Although current IADS early warning radars can be pointed upwards, doing so will not provide sufficient warning either to employ antispacecraft weapons or to seek shelter because suborbital spacecraft will be directly overhead upon discovery. Consequently, any ordnance already would have been released and would be only moments away from impact. If a radar is to have sufficient power to see far enough and high enough to acquire a suborbital bomber with sufficient reaction time to engage it successfully, then the country will need to invest in the equivalent of the United States' Ballistic Missile Early Warning System (BMEWS). Doing so will call for radars with capabilities like those of the AN/FPS-115 PAVE PAWS and the AN/FPQ-16 PARCS, both of which are large, immobile systems with massive power requirements, making them both very expensive to build and operate and easy targets to find and destroy. Since the MSS2 is carried on a mother ship that uses Jet A fuel and theoretically could be refueled in flight, the spacecraft could be launched from any location; therefore, the entire perimeter of a country would be susceptible to a suborbital attack. To cover an entire country's airspace with a BMEWS would also demand a large expenditure of capital to build and maintain the system and would significantly drain that country's military budget, especially for nations like Russia or China that have large landmasses.

The second break in the kill chain is the lack of weapons to engage the suborbital bomber (fig. 3). The current iteration of non-US SAMs does not have sufficient altitude to engage a suborbital spacecraft. Both China and Russia have demonstrated some antisatellite capability, but their weapons are still few in number and designed to take out satellites, systems with no onboard countermeasures such as chaff, or systems unlikely to maneuver because of limited fuel on board and a lack of refueling capability. Since the suborbital spacecraft is in space for only a relatively short time, it can afford to carry decoys such as chaff, assemble a flight with some vehicles carrying jamming pods, or use onboard cold gas systems to maneuver. The only current forces that could engage and destroy a large fleet of suborbital spacecraft are the US Navy's AEGIS radars and RIM-161 Standard Missile 3 and the US Army's AN/TPY-2 radars with Terminal High Altitude Area Defense (THAAD) missiles, both designed for an anti-ballistic-missile role.

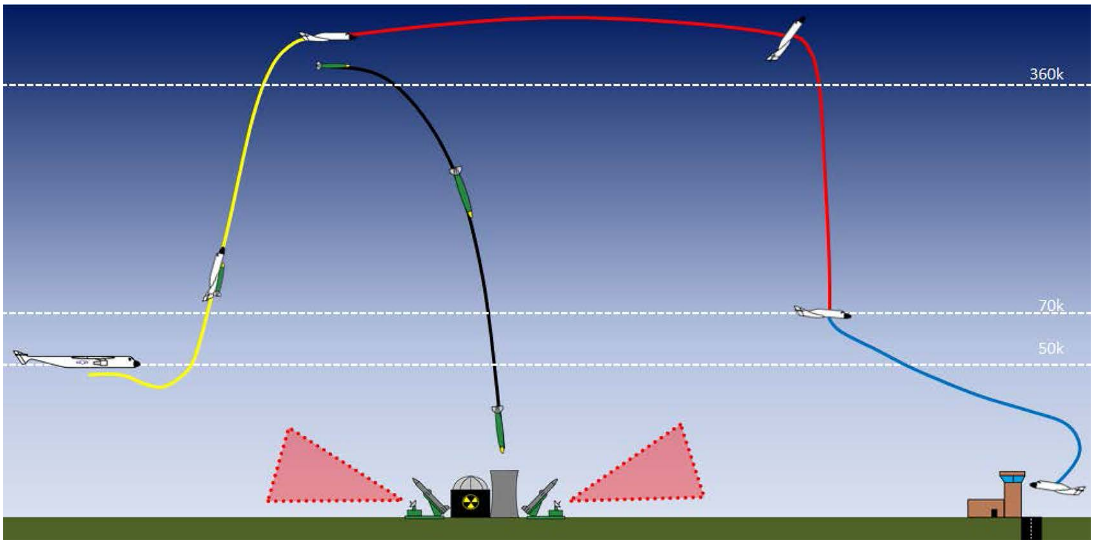


Figure 3. MSS2 overflight profile

There are three other ways to attack the suborbital spacecraft. First, a laser-based system is designed to burn through the skin of the vehicle. The US Airborne Laser was close to coming into production but would have had an issue firing directly overhead. No other major power is near fielding an airborne laser system. A ground-based system could be used but opens itself up to easier destruction. A laser-guided concrete or tungsten bomb, fitted with a sensor tuned to the laser's wavelength, could ride the beam down and destroy the mirror assembly as long as the sensor had sufficient shielding. A second countertactic involves deploying smoke, chaff, or an inflatable Mylar mirror between the laser and the spacecraft. Since there is very little atmosphere and the spacecraft would be cruising at this point, countermeasures once deployed would remain between the spacecraft and the earth. A second attack would take the form of an electromagnetic strike, such as jamming or high-power microwaves, but the long ranges make such an effort extremely difficult to execute without excessive power requirements. By keeping the spacecraft manned, almost all of these threats can be mitigated since the pilot can still operate and attack whereas a remotely piloted vehicle would lose link and refuse to fire. The final method of counterattacking, high-altitude nuclear detonation, entails exploding a nuclear warhead over one's own country, but some radical leaders might resort to such tactics.

This dual breakage in the kill chain from suborbital spacecraft is much more exploitable than the single breakage generated by stealth. Newer and better sensors are being devised every day; recently, gallium nitride semiconductors were authorized under the US arms export policy. When applied to the Patriot radar, these semiconductors allowed it to operate in 360 degrees instead of just a sector, at the same time decreasing cost and maintenance.[18] As long as an opponent uses a set protocol for communication between the sensor head and the flight-control package for a missile—either surface-, sea-, or air-launched—the sensor package can be quickly and quietly swapped out and the Air Force will not know until it loses aircraft to the upgraded weapon. For the suborbital bomber, however, physics becomes our friend.

To counter the suborbital spacecraft, an adversary would need to (1) build a BMEWS that provides total perimeter coverage and (2) completely redesign his missiles to have sufficient energy to reach space. Every joule of energy needed to attain higher altitude, though, will subtract from the energy necessary to operate in the horizontal plane, thus shrinking the weapon's engagement zone. The extreme high altitude from which ordnance would be released would give weapons a glide distance of hundreds of miles; consequently, simple, static point defense of high-value targets would no longer be effective. To counter the suborbital spacecraft threat, the enemy must invest in very large—hence expensive—missiles and a significant number of them to provide complete coverage. We can see in figure 4 that it takes nearly 14 notional SA-30s to offer the coverage against a suborbital spacecraft that a single SA-30 would provide against common airborne targets. This development and deployment of a BMEWS, as well as many interceptor missiles, would prove incredibly costly. Thus, with the development and deployment of a suborbital striker into the US Air Force inventory, an opponent would face the choice of either severely curtailing spending on a traditional IADS to funnel money into antisuborbital weapons or having an IADS that is unable to counterattack. In an A2AD scenario, the first situation results in a severely weakened traditional IADS for the standard aircraft to break through. The second situation produces a robust traditional IADS, in which case the standard aircraft would stand by until the suborbital spacecraft finishes dismantling the IADS with impunity. Either way, the A2AD IADS scenario is neutralized.

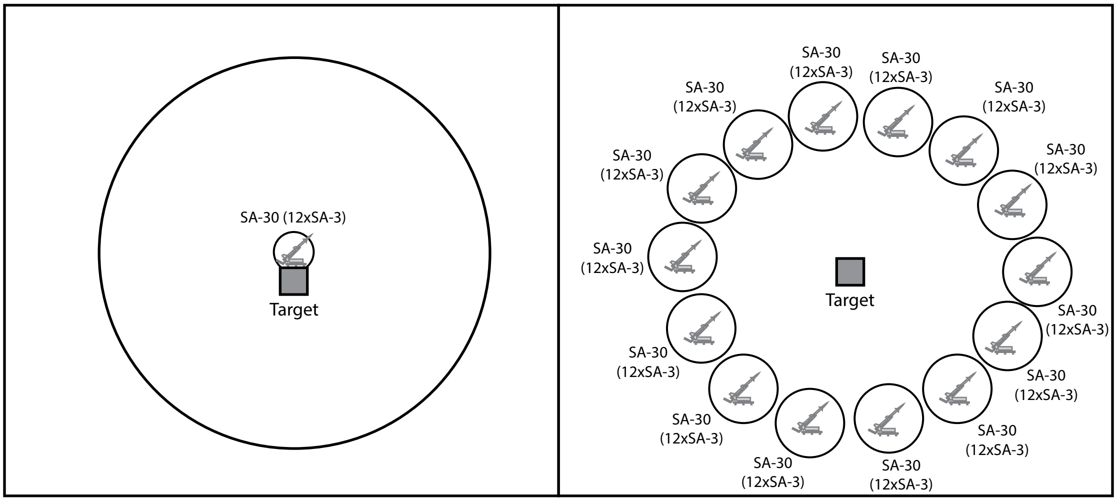


Figure 4. Limitations of airborne versus suborbital SAM requirements

Although the suborbital spacecraft concept does open up a considerable number of new possibilities and almost completely neutralizes current A2AD scenarios, it does have limitations. No single technology is a panacea that can cure all the Air Force's woes. Technology has its own strengths and weaknesses, and limitations must be recognized if it is to be properly employed. A suborbital bomber is not a "Swiss Army knife." The suborbital bomber will fly high and fast, allowing it to be quite effective for missions such as strategic bombing and deep air interdiction for which it needs to cut through the IADS; suppression and destruction of enemy air defenses; and reconnaissance missions that require battle damage assessment, especially if friendly satellites have been neutralized. The spacecraft will not be able to loiter, so it cannot be used for surveillance. Nor can it go low and slow, excluding it from effective use in either a close air support role or combat search and rescue support.

Rapid Development

We have shown that a suborbital spacecraft not only is a viable weapon platform but also is necessary in the coming age to counteract the increasing A2AD capabilities of potential adversaries. However, we have not discussed how to procure said spacecraft. Since this concept opens up a new field of airpower, it needs to be treated as a

Skunk Works–style project so that new ideas can quickly be tested, evaluated, and either implemented or killed as necessary. The program should be run much like the one for the MC-12 Liberty, using quick-reaction capabilities to modify a commercial aircraft into a viable weapon system. The MC-12W program went from establishing requirements to flying operational missions in 14 months.[19] The commercial suborbital spacecraft nearest completion that meets the necessary mission specifications is Virgin Galactic's SpaceShip Two. Even though its initial test bed, the VSS *Enterprise*, crashed on 31 October 2014, taking the life of one test pilot and injuring a second, Virgin Galactic nevertheless is moving ahead with production.[20] As of this writing, the second SpaceShip Two has been built and is finishing the ground-test phase prior to flight testing.[21] Given the present rate of production, it is possible to procure and have ready for testing an MSS2 by the end of 2018.

This early adaption would provide three additional advantages. The first is that tactics, techniques, and procedures could be developed from a clean slate. No other country would have this capability, and we could test and employ it to our maximum benefit since enemies would not know what to expect. The second is an economic boost in the US space-development sector that would keep it more firmly implanted in the United States, not only providing stable jobs but also keeping the advanced technology and corporate knowledge for its development and manufacture in this country. The third is that the launcher for MSS2, WhiteKnight Two, can also be used for launching satellites, thereby increasing the Air Force's capability of rapid space response.

In addition, to save both development costs and prevent future countermeasures, the authors recommend that MSS2 be manned. First, remotely piloted communication systems are not designed for use in suborbital spacecraft but for communicating with an air-breathing platform below them via satellite or talking to a satellite directly overhead via a ground station. A remotely piloted suborbital spacecraft will need a new communication method for its higher data rates—one that can fill the gap between aircraft and satellite. The second reason that MSS2 should be manned is that remotely piloted aircraft have an inherent risk that the link can be tampered with or cut. Any country that has sufficient technological capability to create an advanced IADS can carry out computer and network attacks over radio frequencies. Reportedly, in 2007 Israel used a computer network and an electronic operation to take down the Syrian IADS, assuming control as administrators and turning sensors off target.[22] Remotely piloted vehicles are susceptible to the same types of attacks, the simplest of which is jamming the Global Positioning System so it cannot confirm its location and refuses to release its ordnance. The more advanced attacks can take over as the operator of the remotely piloted aircraft directs it to turn, land, or even theoretically release its ordnance on friendly forces. Jamming a manned spacecraft may prevent the pilot from deciding to release weapons, but we do not have to fear inadvertently dropping bombs on friendly forces.

The final aspect of development that needs to be discussed is the weapons that MSS2 will carry. Extremely high altitude will allow a weapon to generate a substantial amount of kinetic energy without the need to resort to explosives. By channeling that energy, we can create weapons that do not need explosive charges, thus generating two benefits. The first is that they are inert at ground level. A tungsten rod travelling at zero miles per hour is able to injure somebody only if he or she trips over it. Therefore, one can use cluster munitions without the political backlash they generate from unexploded munitions left behind. In a war zone, if an ammunition ship or ammo bunker filled with these weapons is hit, there will be no subsequent detonations that lead to further damage to the ship convoy or base. Second, without the need for explosives, the weapon itself can be made smaller, allowing the vehicle to carry more of them. Utilizing the DeMarre equation for the penetration of kinetic energy weapons, the authors were able to determine that a 5 centimeter by 25 centimeter tungsten penetrator should be able to pierce the top armor of a Russian T-72 tank. The shrinking of guidance systems has led to the development of laser-guided bullets. With either infrared or television guidance, a single cluster bomb of tungsten penetrators should be able to take out an entire airfield or every ship in a harbor.

The weapon bay itself, though, will be designed to hold conventional munitions. Such bays should accommodate the weapon, not the reverse. Designing a weapon to reflect the limits of the aircraft always hurts the weapon. The Air Force recognized this fact first with the development of the AIM-4 Falcon, originally designed to fit into the weapons bay of the F-102.[23] The constraints placed on the missile by doing so rendered it almost useless. It proved ineffective in Vietnam and was eventually retired from the Air Force in favor of the AIM-9, designed by the Navy without restraints at the same time as the AIM-4 and still in use today. Like the F-117's, the weapons bay will be designed around the weapons, allowing the MSS2 to employ conventional munitions while suborbital munitions are in development, along with a much faster initial operational capability. We can compare the survivability capabilities of the MSS2 to those of the SR-71 and see their near overlap, except for the fact that the MSS2 will be capable of employing munitions (fig. 5).

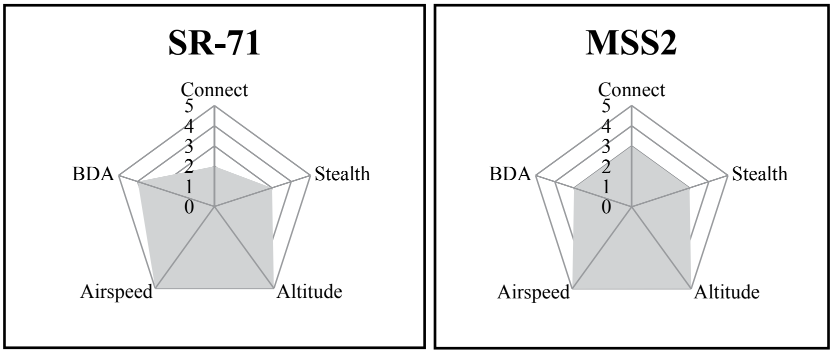


Figure 5. Survivability comparison of the SR-71 and MSS2

Conclusion

In the 1930s, the United States Army Air Corps, along with the rest of the world, was infatuated with long-range bombers. The Air Corps Tactical School pushed the doctrine of strategic bombardment. The statement "the bomber will always get through" was quickly taken up despite the warnings of fighter advocates such as Claire Chennault.[24] This stance directly affected aircraft development in peacetime, allowing creation of the B-17 but no other effective airframes. The United States entered World War II with a heavy bomber but no developed doctrine besides massed air raids or advanced aircraft for any other roles, and the Army Air Corps suffered severely for it.

We are quickly entering the 1930s mind-set again in today's Air Force, but now the rallying cry is "the stealth aircraft will always get through!" To develop weapons that provide the greatest capability and most efficient use of resources, the Air Force needs to examine aircraft survivability from its five key components and apply each one to its individual mission.

The most effective method for breaking apart an A2AD IADS environment involves procuring a vehicle that can attack from outside the scope of the enemy's IADS. The weak points here are altitude and airspeed. The current iteration of SAMs and fighters cannot touch a suborbital spacecraft. Although opening and developing a new line of air vehicles and training personnel to operate them may be expensive, the cost does not begin to compare with what adversaries would need to spend to counteract them.

A suborbital spacecraft, procured rapidly from commercial designs along the lines of the MC-12 program, will supply the necessary capabilities to keep the Air Force viable well into the 2030s to 2040s. It will regain freedom of maneuver within the A2AD environment and allow the creation of weapons that rely only on kinetic energy and that remain inert directly after use. Such a vehicle will keep technologically advanced jobs and manufacturing in the United States while forcing potential adversaries to spread their budget more thinly over multiple defensive systems. The future is forever changing. Only by thinking outside the norm and being willing to test new ideas will we have any hope of keeping up. ✪

Notes

1. "MC-12W Liberty Intelligence, Surveillance and Reconnaissance (ISR) Aircraft, United States of America," airforce-technology.com, 15 March 2015, http://www.airforce-technology.com/projects/mc-liberty/.

2. Headquarters USAF/XPXC, *The U.S. Air Force Transformation Flight Plan* (Washington, DC: Headquarters USAF/XPXC, November 2003), 66, http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf.

3. Wilbur Cross, *Zeppelins of World War I* (New York: Paragon House, 1991), 153.

4. "Lockheed SR-71A," National Museum of the Air Force, 29 May 2015, http://www.nationalmuseum.af.mil/Visit/MuseumExhibits/FactSheets/Display/tabid/509/Article/198054/lockheed-sr-71a.aspx; "U-2S/TU-2S," US Air Force, 23 September 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104560/u-2stu-2s.aspx; and "North American XB-70 Valkyrie," National Museum of the Air Force, 3 November 2015, http://www.nationalmuseum.af.mil/Visit/MuseumExhibits/FactSheets/Display/tabid/509/Article/195767/north-american-xb-70-valkyrie.aspx.

5. Dr. Carlo Kopp, “Almaz S-75 Dvina/Desna/Volkhov,” Air Power Australia, 19 February 2015, http://www.ausairpower.net/APA-S-75-Volkhov.html; and Kopp, “Almaz-Antey S-300PMU2 Favorit,” Air Power Australia, April 2012, http://www.ausairpower.net/APA-S-300PMU2-Favorit.html.

6. Dario Leone, “How the MiG-31 Repelled the SR-71 Blackbird from Soviet Skies,” Aviationist, 11 December 2013, http://theaviationist.com/2013/12/11/sr-71-vs-mig-31/.

7. Francis Crosby, *The Complete Guide to Fighters & Bombers of the World* (London: Hermes House, 2008), 447, 492.

8. Dr. Carlo Kopp, “Assessing Joint Strike Fighter Defence Penetration Capabilities,” Air Power Australia, 7 January 2009, http://www.ausairpower.net/APA-2009-01.html.

9. Wing Cdr Chris Mills, “Air Combat: Russia’s PAK-FA versus the F-22 and F-35,” Air Power Australia, 30 March 2009, http://www.ausairpower.net/APA-NOTAM-300309-1.html.

10. Dr. Carlo Kopp, “Sukhoi Flankers: The Shifting Balance of Regional Air Power,” Air Power Australia, April 2012, http://www.ausairpower.net/APA-Flanker.html.

11. Norman Friedman, *The Naval Institute Guide to World Naval Weapon Systems,* 5th ed. (Annapolis, MD: Naval Institute Press, 2006), 533–34.

12. Daniel House, “The Viability of Commercial Sub-orbital Spacecraft for Military Strike Missions” (thesis, American Public University System, Charles Town, WV, 2012).

13. Simon Adebola et al., *Great Expectations: An Assessment of the Potential for Suborbital Transportation*, Masters 2008, Final Report (Strasbourg, France: International Space University, 2008), 6–14, https://isulibrary.isunet.edu/opac/doc_num.php?explnum_id=95.

14. “F-22 Raptor,” US Air Force, fact sheet, 23 September 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104506/f-22-raptor.aspx.

15. “Dynamic Targeting and the Tasking Process,” in Curtis E. LeMay Center for Doctrine Development and Education, “Annex 3-60, Targeting,” 10 January 2014, https://doctrine.af.mil/download.jsp?filename=3-60-D17-Target-Dynamic-Task.pdf.

16. CAPT William J. Toti, USN, Retired, “The Hunt for Full-Spectrum ASW,” US Naval Institute *Proceedings Magazine* 140, no. 6 (June 2014), http://www.usni.org/magazines/proceedings/2014-06/hunt-full-spectrum-asw.

17. “AN/FPS-117 Long-Range Air Surveillance Radars,” Lockheed Martin, 2013, http://www.lockheedmartin.com/content/dam/lockheed/data/ms2/documents/FPS-117-fact-sheet.pdf.

18. Sydney J. Freedberg Jr., “The Biggest Thing since Silicon: Raytheon’s Gallium Nitride Breakthrough,” Breaking Defense, 20 February 2015, http://breakingdefense.com/2015/02/the-biggest-thing-since-silicon-raytheons-gallium-nitride-breakthrough/.

19. “MC-12W Liberty Intelligence, Surveillance and Reconnaissance (ISR) Aircraft, United States of America,” airforce-technology.com, 15 March 2015, http://www.airforce-technology.com/projects/mc-liberty/.

20. Tariq Malik, “Virgin Galactic SpaceShipTwo Crash: Full Coverage and Investigation,” Space.com, 19 December 2014, http://www.space.com/27629-virgin-galactic-spaceshiptwo-crash-full-coverage.html.

21. “FAA-AST Awards Virgin Galactic Operator License for SpaceShip Two,” Virgin Galactic, 1 August 2016, http://www.virgingalactic.com/faa-ast-awards-virgin-galactic-operator-license-for-spaceshiptwo/.

22. John Costello, “Bridging the Air Gap: The Coming ‘Third Offset,’” War on the Rocks, 17 February 2015, http://warontherocks.com/2015/02/bridging-the-air-gap-the-coming-third-offset/.

23. Ron Westrun, *Sidewinder: Creative Missile Development at China Lake* (Annapolis, MD: Naval Institute Press, 1999), 28–29.

24. Martha Byrd, *Chennault: Giving Wings to the Tiger* (Tuscaloosa: University of Alabama Press, 1987), 46–53.

Capt Daniel J. House, USAF

Captain House (BA, Texas A&M University; MA, American Military University) is the flight commander of Advanced Capabilities and Targeting Strategies, 55th Intelligence Support Squadron, 55th Wing, Offutt AFB, Nebraska. He is responsible for conducting signal development, big data and advanced analytics, full-spectrum mission integration, emerging technologies capabilities, and tactics, techniques, and procedures for all RC-135V/W, RC-135S, and RC-135U collection airframes. An RC-135V/W Rivet Joint electronic warfare officer instructor with over 1,500 hours, he has flown combat missions in Operation Enduring Freedom, Operation Unified Protector, and Operation Inherent Resolve.

Dr. John Tiller

Dr. Tiller (BA, Hendrix College; MSc, PhD, McMaster University) is president of John Tiller Software and has been a professional war-game designer and developer for over 20 years. During that time, he has published more than 100 war-game releases for Windows PC, Macintosh, Linux, iPad, Android, and Kindle. His war games have received multiple awards, including War Game of the Year on several occasions. For over 10 years, Dr. Tiller has performed in excess of 20 research and development projects for the Air Force and Navy, including organizations such as the Air Force Office of Scientific Research and Squadron Officer College. He is also a private pilot with over 1,000 hours of flight time.

Dr. John Rushing

Dr. Rushing (BS, Rensselaer Polytechnic Institute; MS, PhD, University of Alabama in Huntsville) joined Intel Corporation in 1999 as a senior computer-aided design engineer. In 2002 he returned to the University of Alabama in Huntsville where he is currently a principal research scientist. Dr. Rushing's current research includes artificial intelligence, modeling and simulation, data mining, and parallel algorithms.

Let us know what you think! Leave a comment!

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

Selecting Qualified Airmen for the Cyber Mission Force

The Pitfalls of Hiring Operational "Analysts"

Maj David J. Ortiz, USAFR

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

```
1 packets transmitted, 1 received, 0% packet loss,
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock ->
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> sp
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run ->
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
```

Setting the Stage

The Air Force, like each service, is charged with providing cyber operations and intelligence professionals for the Cyber Mission Force (CMF) being built by US Cyber Command over the last four years. The CMF build-plan calls for dozens of teams serving in offensive, defensive, and supporting roles. Inside the CMF, the combat mission teams are aligned to the combatant commands to serve the offensive cyber needs of the combatant commanders. US Cyber Command manages over a dozen national mission teams aligned to conduct a defend-the-nation mission called the Cyber National Mission Force. Both the combat mission teams and the national mission teams also have support teams assigned to help with development and analysis. Finally, a large number of Red Team–like units called cyber protection teams are under operational control of the combatant commands and the Cyber National Mission Force for defensive purposes. Most of these teams are trained inside the National Security Agency (NSA) under its rules and high standards, using its capabilities.

From the NSA's birth, military intelligence, communications, and scientific units have provided personnel to supplement offices in support of the collection of signals intelligence and the requirements of information assurance. Over the past decade, the services—in varying forms—have also established cyber-focused units to supply qualified personnel to various cyber missions within the NSA. Thus, when the CMF began in 2012, needing over 60 people apiece to serve in national mission teams or combat mission teams, many of these service members found themselves realigned to a cyber team of one stripe or another. At the time, no ready source of individuals existed to meet the substantial manning needs of the new CMF, so converting the majority of service-billeted people and service civilians already embedded in the NSA made good sense.

After the in-place turnovers, the functional managers within the services faced the difficult prospect of hiring en masse a workforce of cyber professionals. It must have been hard for them to divine exactly what the CMF needed for obscure work roles that didn't exactly translate into many mapped military career paths. There were some exceptions because some services created career-code "shred-outs" (i.e., "markers" to track skills or experience) to specifically align people to the NSA's cyber work roles.

In the past, finding a handful of qualified service members per squadron or company for the NSA who possessed unique technical skills was totally feasible with the flexibility given to local training managers and superintendents. However, the CMF has dozens of sizeable teams, so the demand for these low-density, high-demand cyber, development, and intelligence skills went through the roof over the last four years. Whereas previously a unit may have been asked to provide only a handful of qualified service members, now it eventually had to supply dozens. (Furthermore, they will be permanently changing station every two-to-three years, so a dedicated pipeline will be necessary.) When the integration numbers within the NSA were lower, units had the luxury of farming out resumes and sending Airmen, Soldiers, and Marines to interview within the agency to find the right office. The advent of the CMF limited that freedom of placement because the teams had to meet readiness requirements set down in their manning layouts, which could not be altered (i.e., each team must be built exactly the same way). This inflexibility further increased throughput to specific NSA offices and now from specific military career codes. Consequently, how does the Air Force cope with these challenges and serve the needs of the CMF mandate to produce qualified cyber professionals?

The Air Force and possibly other services may be exacerbating the difficulty of finding a greater quantity of qualified applicants for some CMF/NSA work roles by self-imposing self-limiting rules based on career codes (Air Force specialty codes [AFSC], military occupational specialties, and others). Since the need for qualified cyber Airmen is high and not likely to change anytime soon, this article recommends a few reasonable steps to better position our beloved Air Force and the other services to meet readiness requirements through more flexible applicant searches, skill tracking, and a reexamination of what it means to be "operational" in cyber.

Background: Why Should We Listen to You?

Where you stand often has much to do with where you sit. In the interests of full disclosure, most of the work week I am an NSA deputy division chief, leading an operational cyber force of awesome civilians, contractors, and military personnel. Integrated into my division are more than a dozen CMF teams with all the US Cyber Command people I could ever want. My alter ego is the Reserve assistant director of operations for a cyber operations squadron whose job it is to supply interactive operators (ION) right back to my own NSA mission space and other offices. Therefore, I believe I am in a unique position to experience both sides of the problem and can see some already viable solutions that the Air Force and other services should consider to improve exploitation analyst (EA) throughput specifically. (Note that some of the lessons learned could be applied to other work roles in the CMF as well.)

Inside my civilian mission space, we integrate two types of CMF- and NSA-recognized work roles: EAs and IONs. From an operational perspective, they are two peas in a pod, working together daily conducting cyber missions—not exactly "pilot and navigator" or "Maverick and Goose," but for the purposes of this discussion, these analogies are useful.

As a reservist, I help my squadron supply quality ION trainees to attend a long, structured NSA pipeline that lasts anywhere from 18 to 24 months. It's a demanding program that begins with passing a standardized test and a personal interview after completion of initial training. The pass rate in this complex cyber training course was slightly less than 60 percent over the last year (civilian and military), but, thankfully, our squadron has had about a 100 percent pass rate among its students.[1]

My division hires, trains, and certifies EAs to work in the same cyber mission space as our IONs. Think of EAs as cyber (sniper spotters) and mission planners for the IONs since they work hand-in-hand on the same complex operations. The training program for EAs is about six to nine months long (depending on class dates) and is similarly demanding. The work role requires many of the same skills but asks the EA to accomplish different tasks. To begin EA training, applicants go through a resume review and a technical interview. The pass rate for the interview process was not high among our Air Force applicants over the last year, running at a very dismal 12 percent.[2] Granted, even for civilians with university degrees, the pass rate is not 100 percent.[3] Therefore, it is problematic just to get EA trainees in the door, much less through the six-to-nine-month training program. The good news is that, as a whole (civilian or military), the pass rate for the EAs who enter the program is around 90 percent.[4]

An obvious question would be, "Why is the Air Force having great success staffing IONs but struggling with getting Airmen into the EA pipeline on exactly the same cyber operational team?" Imagine the problem this way: would it be acceptable for an Air Force training squadron prepping a pilot and navigator team to fly an airframe to have a 100 percent pass rate for the pilots but just a 12 percent rate of acceptance for the navigator pipeline (to say nothing of their pass rate once they enter the program)? Probably not—so is the Air Force somehow identifying the right Airmen to fill ION positions yet looking in the wrong direction for EAs? My theory is that it may have to do with the *analyst* part of the "exploitation analyst" name and the perceived skills associated with that title.

An Analyst Is an Analyst Is an Analyst . . . until He or She Is Not

In the military, the words *operator* and *analyst* evoke very real, distinct impressions. In the Air Force, the *analyst* conjures scenes of Airmen diligently typing on a keyboard and working through tough scientific or intelligence problems. Perhaps these analysts are also drafting air campaign plans or collection requirements. Regardless of the task, most people would agree that an "analyst" is not executing an "operational" mission on a daily basis—just a rough estimation. (Clearly, there are exceptions for Airmen serving on various airframes who are intel folks.)

On the other hand, the term *operator* easily brings to mind the flying or space world—Airmen on stick, loadmasters, boom operators, pararescuers, combat controllers, or Airmen serving on missile crews. Although many of us may not work in these "operational" career fields, it is easy to envision the Airmen in them flying, employing weapons systems, or serving on security details. The line between analysis and operations is easy to grasp. Unfortunately, in the cyber "operational world," that line is not so easily visible because of the way operations are conducted and the way many people are involved on a single operation. Even worse is trying to draw these lines based on AFSCs and military occupational specialties, which is counterproductive and might make it harder for the Air Force and other services to find qualified cyber professionals.

Current Alignment of Air Force Specialty Codes

To further explore the AFSC problem, we have to look at how the Air Force fills ION and EA billets across the CMF and NSA right now.

Interactive operators. In light of the fact that the term *operator* is in the ION work-role title, Twenty-Fourth Air Force fielded cyber operations squadrons (formally network warfare squadrons) to provide qualified Airmen to train at the NSA for complex cyber operational jobs. Undoubtedly, the agency and the CMF are looking for cyber-ready individuals whose A-school prepped them for this type of training pipeline. For the Air Force, that is Undergraduate Cyber Training (UCT). The AFSCs, such as 17Ds, 17Ss, and 1B4s, awarded after UCT and follow-on training denote Airmen destined for cyber operations. These professionals would largely go on to work in positions like base communications, cyber operations, or network defense, to name a few. UCT's stated focus is to prepare Airmen to establish, secure, operate, assess, and actively defend multiple types of networks, including command and control systems, Internet, telephony, satellite, and mobile telecommunications, among others.[5] An operationally minded course ensures that Airmen understand they are prepping to fight and win in another military domain. When Airmen graduate from UCT, the best of them continue to take supplemental cyber warfare officer training, with the best of this school usually selected to take the NSA's difficult ION entrance exam. Those who pass are usually slotted for a 300-series squadron such as the 315th or 390th Cyber Operations Squadron and then come to Fort Meade, Maryland, to prep for their training. In the 315th, potential IONs are interviewed and further screened when they arrive, just to make sure they are technically ready for the long training pipeline. It is no wonder that the Air Force has an admirable pass rate, producing some of the best operators serving in the CMF and the agency.

Exploitation analysts. As exploitation "analysts," these Airmen are staffed by Twenty-Fifth Air Force under an intelligence function. Units like the 16th and 41st Intelligence Squadrons receive intelligence officers and enlisted service members who have likely gone through the JCAC (Joint Cyber Analysis Course) in Pensacola, Florida, and are then slotted against EA positions on the CMF that the squadrons support. The JCAC is designed to give personnel with minimal computer skills a wide range of cyber and analytical instruction over six months.[6] The goal is to prepare them to conduct technical network analysis in support of computer network operations effects and national intelligence requirements. When potential EAs arrive at their squadrons, many of them enter the US Cyber Command / J7 pipeline—an amalgamation of NSA, industry, and military training programs designed to prepare a person for the EA role. Unfortunately, this path is not working as well for our Airmen as the one above for the IONs even though they both need to perform at the same operations station and support each other to conduct the same mission. How, then, is the Air Force succeeding extremely well with one work role yet struggling with the other?

Work-Role Requirements

From the training statistics, the Air Force seems to have cracked the code in finding Airmen to become successful IONs. Twenty-Fourth Air Force understands the requirements and has a training program that readies Airmen for the world of cyber operations. The Twenty-Fourth knows that its mission is to prep cyber Airmen for an operational war-fighting role.[7] I fear, however, that a mismatch exists somewhere for EAs when people see the word *analyst* and then collectively pivot to intelligence units and AFSCs to fill the bill. Unfortunately, for a job like EA, intelligence analysts are not what the NSA is looking for to populate its training program. The EA position is a cyber-operations job, regardless of its name, because that is what EAs do with IONs—conduct operations. EAs are at the nexus between cyber intelligence analyses, requirements, effects-based planning, cryptology, cyber operations, cyber development, and operations security. Threading that line demands a deep knowledge of the cyber world, not just a concentration on either network analysis or reporting.

What is the National Security Agency looking for in an exploitation analyst? Many of the daily work-role functions of an EA are classified, but the way the NSA hires civilian EAs or interviews military applicants is entirely unclassified. Below are the five major knowledge categories that hiring managers look for in an EA applicant.[8] The first screen is a resume review, and the second is an in-person interview to assess critical thinking, problem solving, teamwork, collaboration, professional development, and the applicant's currency in technology, the last of which is very important in cyber.

- Programming Concepts /Application Development
  - Secure code or other exploitation concepts
  - Scripting
  - Programming languages
- Operating System Fundamentals—Windows/Linux
  - Command-line concepts
  - Key file locations
  - System configuration and running state
  - Client/server concepts
- Networking Fundamentals
  - Open systems interconnection concepts
  - Routing/switching
  - Subnetting
  - Network services
- Network Security Architecture
  - Segmentation
  - Firewalls
  - Virtual private networks
  - Proxies/guards
- Computer Network Defense
  - Penetration testing
  - Vulnerability assessment
  - Intrusion detection and network forensics
  - Incident response and host forensics
  - Malware analysis

What's in a work role? This list makes it much easier to see why a technical mismatch exists at the EA desk within the intelligence squadrons. For example, the NSA's EA technical interviewers are not looking for traditional intelligence analysis skills like reporting and all-source analysis. Instead, they want to see a decent concentration in three of the five technical categories listed above, such as network administration, programming, or malware analysis. EA applicants don't have to be experts in each, but they should have some background in most of the subjects and, hopefully, thorough knowledge of a few. The division's hiring managers regularly remind the CMF and other partners that the EA work role is not a place to learn basic computer and networking skills. Rather, it's a position to enhance and apply already good cyber skills for a difficult mission. This is not just their opinion. In fact, the NSA considers the EA work role to lie within the *networking and telecommunications* skill community, not as it happens within the *intelligence analysis* skill community.[9] Naturally, the ION work role is also within the *networking and telecommunications* skill community.[10]

Unfortunately, the Air Force's manning model is asking an intelligence analyst to do a very "cyber" job. The JCAC, the class that many intelligence personnel attend for cyber analysis instruction, is not exactly paying the bill for this specific work role regularly. Intelligence professionals with AFSCs like 1N4 and 14N, as well as other AFSCs who are not cyber-focused, usually don't pass the interview or complete the training. Although the division has had successful intelligence professionals from JCAC, they have mostly come with cyber skills of their own via a personal hobby, additional schooling, college courses, or self-paced study in cyber.[11] Other factors can contribute to lower pass rates as well in this population. For example, the length of time between the JCAC and a CMF position could take six months to a year as they wait for a clearance. This makes it hard for some people to recall key technical details from the JCAC or other schools during an interview if they don't have an innate interest in cyber as a hobby. The secret for our successful career intel-trained applicants and other noncyber AFSCs is that they are already interested in networks, hacking, malware analysis, and digital forensics anyway, so they are keeping current all by themselves.[12] *We call them keepers*.

From the point of view of our civilian hiring managers, they are confounded as to why the Air Force sees the EA work role as an "intelligence analyst" job because it has always been a cyber job to them. Then again, our civilians don't have the military background to cloud their interpretation of the term *exploitation analyst* either. The division's hiring managers only care about the critical functions within the work role that need to be done. For example, EAs conduct the lead-up cyber-target development and preoperations analysis, draft operational plans, guide operations that IONs conducted on-keyboard, help keep operations safe, and conduct postoperations analysis. Airmen can roughly equate the EA to a navigator on a spice freighter, but the work has more of a mission-management focus to it as well—similar to a mission commander on an Airborne Warning and Control System crew who shares mission-execution responsibilities with the pilot. One can't effectively get the job done without the other. EAs are target-subject-matter experts, knowing all there is to know about a target. They are responsible for ensuring that the operational team secures national intelligence or prepares to support the commander's intent. Frankly, with these responsibilities comes the need for a wide variety of cyber skills not necessarily related to either intelligence analysis or reporting, which are traditional core functions of intelligence analysts.

Applicants

Successful Applicants

At this point, readers could point out that many 1N4s, 14Ns, and 1N2s have passed the EA interview and are succeeding in their positions. That is true, of course. The fact that our division employs skilled intelligence analysts as EAs supports that argument. What, though, are the common threads that have led to their success?

Experience matters. In the initial days of the Cyber National Mission Force, many EA slots were billeted from Airmen already EA-qualified or from the best cyber analysts scattered among the all-source-analysis community at the NSA. These individuals were E-5s and above with a tour or two in network analysis shops, Red Teams, or Blue Teams—or they were network administrators who were good enough after their interview to walk in the door outright. To acquire that baseline knowledge, some took on work roles in their shops that were more cyber focused than perhaps advertised, and others sought out mostly cyber shops that wouldn't usually be offered to their AFSC in the greater Air Force. That can happen in the NSA because a civilian office may not care what someone's AFSC is—only that he or she can do the job or be willing to learn the skills for the work role. Finally, some IONs also came over to the EA work role with their cyber skills and shine brightly. Intelligence folks have also succeeded as IONs.

Interest. The most successful analysts (enlisted, officer, civilian, or contractor) are at-home cyber enthusiasts.[13] Just for fun, these applicants like to create networks of their own to study at home. Some have created "honeypots," used to attract hackers and capture malware on the Internet, and stand-alone networks called "sandboxes" to analyze malware they find. They monitor their inbound and outbound connections with netstat and similar network utility tools to learn more about their craft. Others still are practicing with openly available network security testing tools like Backtrack (legally, of course) on their own closed networks. Some of these career intelligence Airmen in the division are also working on their computer science degrees, and that foundational academic knowledge helps out a great deal with the interview and EA training.[14] Whether they began as intelligence analysts or weeds-and-seeds workers, these are the Airmen we want!

Dedication. I don't have to tell these types of Airmen to keep up with current technology or get trained on something new. They do it on their own, aggressively. These Airmen will bleed a training manager dry by signing up for anything available on cyber. Doing so pays off for both the member and the office as long as they retain and then apply their skills at work. What is great about the NSA is that Airmen with experience know how to look for and take a wide variety of agency classes available to service members integrated into the agency. Many classes are exceptional and have prepared them for success within the division as cyber professionals, regardless of where they started or what AFSC badge was pinned on their shirt.

Dogged determination. Some people have failed the entrance interview and have worked for six months, taking courses and studying to close knowledge gaps with added training. I am impressed with them because of the self-discipline needed to improve their skills. Despite the option to reattempt the interview, not everyone passes the second and final time around. Just for reference, six to eight months is the estimated time it would take to prepare a cyber novice within the division so that he or she could simply begin formal training (we've done it before). It is one good reason for the screening process because the division has neither the manpower nor the time to teach basic skills on a regular basis.

Not-So-Successful Applicants

Unfortunately, this category represents a significantly higher number than we would like for the Air Force. At last count, within the previous year, Airmen were batting about one for eight on recent interviews, some of them not clearing the interview on the second try.[15] The other services are doing better, largely due to two factors: prescreening of applicants before the interviews by qualified EAs (some of the best) and sending their version of cyber professionals to the interviews. Not all of them make it, but they enjoy a higher rate of acceptance than does the Air Force at this time. Nobody wants to see this trend continue, and the squadron director of operations and other local experts are trying hard to look for viable solutions to improve the throughput. This article is one of those efforts—an appeal to senior Air Force cyber and intelligence leaders to take notice of the problem and explore some of the solutions recommended below.

Proposed Solutions

Changing the Perception of Cyber Operations

If those of us in the cyber operations field were to walk a group of pilots through the operations floor, they would likely understand many of the positions and functions we have, even if they've never plugged in a router. They could appreciate that place as our "battlefield" and the support elements on the watch keeping our troops and infrastructure safe. They would understand the senior watch officer position monitoring the assets and teams during operations. Finally, they would see kindred spirits/professionals diligently working to carry out the mission in real time. That is their professional world—real-time operations. It is the same world of our IONs and EAs as well when they complete a mission together. If nothing else, this visual could help Air Force leaders grasp that the EA position is a cyber-operational job and that any plans to classify the work role as anything else should be halted.

Recommendations for the Exploitation Analyst Pipeline

The Air Force has tried the same thing for more than three years but has not improved its results. In fact, a case can be made that it has gotten worse at staffing EAs using the current pipeline process. Therefore, I highly recommend that the Twenty-Fourth and Twenty-Fifth Air Forces seriously reconsider how they normally staff and train EAs and other cyber analytical positions.

They should consider sending 14Ns, 1N4s, and 1N2s identified for future EA positions to UCT as a secondary AFSC training requirement. This action would give intelligence professionals a firm foundation in cyber operations and the technical skills needed to succeed at a higher percentage than is the case today. Although doing so may cost more and extend the timeline for preparing an intelligence officer / enlisted Airman for the CMF, it would significantly increase the types of skills needed for this work role.

Furthermore, they should begin drawing directly from UCT the Airmen who already have an exceptional cyber background to qualify for the EA work role. The first option may lie outside the acceptable timelines for 14N, 1N4, and/or 1N2 development, but then again something has to change to improve the numbers.

Another consideration to improve the EA pipeline involves following some of the steps that the 300-series cyber squadrons use to pick IONs. The Twenty-Fourth and Twenty-Fifth could select the best of the UCT or JCAC graduates, interview them before they come to the squadron (if possible), and then screen them again when they arrive. They should provide Airmen more focused training, and then mentor them to ensure knowledge retention. *After all, if personnel do not perform these tasks regularly, then the skills atrophy fast*. Nothing is perfect, but the 315th Cyber Operations Squadron's near–100 percent ION throughput is unmatched by the other services.[16] We must keep in mind that this program is one of the most rigorous in the US government for cyber training, so the squadron has some proven processes.

Process Recommendations

The Air Force has a diverse talent pool, and it should identify applicants early. I am a firm believer that the service needs to open up positions like ION and EA to any Airman qualified to carry out the mission. These positions need to be advertised internally, and since the IONs have an entrance test for training, anyone should be able to take it if he or she is eligible. As for the EAs, a records review and prescreening interview would be a good way to gauge cyber competence. Perhaps using the ION test could also be useful, but keep in mind that it's not directly meant for the EA position. (Note that the NSA is working on a standardized entrance test for EAs as well, but it is not certified yet. In the meantime, we will have to wait for the review board to finish.)

If the Air Force is not already doing so, it should consider testing Airmen for cyber aptitude right out of basic training and in college programs during the junior and senior years to identify cyber talent early. Other services are developing or are already employing these tactics to quickly identify the individuals most interested in cyber careers.[17] The Air Force should consider doing the same with our captive audiences in ROTC and the academy before they enter active duty.

Finally, those of us who have been around the service for a while know that there are some brilliant Airmen walking around with us who may not be in the job they are best suited for. How can we identify them? The key is getting better at tracking skills and training classes that are not currently on an Air Force training report. As a case in point, let us examine the last 1N4 to pass the EA interview in my division. He is one of the eight Airmen who attempted the interview in the past nine months. When I first met him, I knew after five minutes that he was going to pass the interview and do great things with us. Later during an interview for this article, I asked him about his background and why he thought he was prepared for this job. The following are some highlights from the Airman's interview.

Employment background. He spent seven years within the NSA working in multiple intelligence analysis and data forensics shops.[18] Network- and host-based forensics positions are superb training grounds for Airmen wanting to work as IONs or EAs.

Training. Since his intelligence analysis shops required considerable understanding of networking technology, data analysis, and forensics, he had to learn about them. Initially, he took a variety of NSA classes to hone his skills and then never stopped. His NSA training records look like a rap sheet of cyber and analysis classes heading into the sunset.[19] The EA interview was a breeze for him largely because he had seen so much of it before and was already an expert in one of the technical skills that our hiring managers value. The problem for the Air Force is that it didn't really know anything about his training.[20] Word of mouth in the squadron was that he was smart, but his Air Force records were only mildly impressive. Most of his training with the SANS Institute, certifications, and NSA class work just didn't show up on the Air Force's radar.[21]

Aptitude. He is also succeeding because he still wants to learn more, not because he was in a forensics shop or because he has a technical degree. He is in awe of the people he serves with, and they are in awe of him. The best EAs and IONs are humble in expressing the extent of their knowledge and always believe they can learn something new from their counterparts. These stars are usually the brightest in the bunch. Screening for this quality is difficult, but it is part of the interview when we ask how the applicant keeps up with technology and works with others. Those who study cyber at home for fun or experiment with networks are usually terrific applicants.

Conclusion

My hope is that Air Force cyber leaders get more out of this article than replacing 1N4s with 1B4s. That is not the point. I would like the service to really appreciate the fact that in cyber, the line between operations and support analysis is often hard to draw. Airmen whose job title may suggest that they are out of the operational loop are actually on the front line. Airmen with hard-to-find skills are out there in the force, so we shouldn't make it harder for them to sign up. Devising an economical way to identify their talent and being flexible with AFSCs will allow the Air Force Personnel Center to locate Airmen who want to serve where they are most needed. That is good for the Air Force and great for the Airmen.

The venerable AFSC is a fine idea, but it has somewhat lost its luster in cyber. This article has addressed 1N4s, 1N2s, 14Ns, and the cyber-operational AFSCs, but let us not forget the engineers, scientists, mathematicians, and other career Airmen who have completed NSA tours and received the same training and certifications. Who are we to tell them they can't do the job just as well? Why would the Air Force want to do so when it is so hard to find qualified Airmen? Some of the smartest people we have in my division are our transient Airmen in special programs on nine-month or one-year tours. These individuals are usually in the scientific, engineering, and computer-maintenance career fields, but the Air Force never lets these Airmen serve very long as EAs or IONs because of their pedigree. That's a shame. The ever-dreadful unit manning document should be a helpful guide, not a means to remove the odd person out because his or her AFSC is different from the one on the spreadsheet. The adversary doesn't care what our AFSCs are—guaranteed—so we shouldn't either.

Lastly, the Air Force has to do a better job of identifying its talented people by their skills and outside training. If nothing else, we should be able to ingest the training records and certifications from another Department of Defense school like the NSA's Associate Directorate for Education and Training so that cyber functional managers can make more informed decisions. What if we needed someone in a crisis or, worse yet, had to pay contractors to come in when the Air Force already had the talent on the flight line? It's just not good resource management, so I hope this article can help us move in a better direction. ✪

Notes

1. Deputy chief of ION training, interview by the author, subject: Statistics, 2016.
2. Branch chief, interview by the author, subject: Managing EA Hiring, 2016.
3. Ibid.
4. Ibid.
5. 81st Training Wing Public Affairs, "First Cyber Class Graduates," 8 December 2010, http://www.afspc.af.mil/News/Article-Display/Article/250046/first-cyber-class-graduates.
6. Thom Seith, "Joint Cyber Analysis Course Challenges New and Veteran Sailors," US Navy, 22 January 2015, http://www.navy.mil/submit/display.asp?story_id=85292.
7. Twenty-Fourth Air Force Public Affairs Office, "24th Air Force Fact Sheet," 2014, http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663.
8. National Security Agency (NSA), "Unclassified Interview Concepts" (Fort George G. Meade, MD: National Security Agency, 2014).
9. NSA Associate Directorate for Education and Training, "Work Role Titles" (Fort George G. Meade, MD: NSA Associate Directorate for Education and Training, ca. 24 November 2014).
10. Ibid.
11. 17S, 1N2, and 1N4 Airmen, interviews by the author, subject: Backgrounds and Training, 2016.
12. Ibid.
13. Ibid.
14. Ibid.
15. Branch chief, interview.
16. Deputy chief of ION training, interview.
17. S3 operations officer, 780th Military Intelligence Battalion, interview by the author, 2016.
18. 17S, 1N2, and 1N4 Airmen, interviews.
19. Ibid.
20. Ibid.
21. Ibid.

Maj David J. Ortiz, USAFR

Mr. Ortiz (BS, MS, Norwich University, the Military College of Vermont) serves as a leader in cyber operations, planning, and analysis as a Department of Defense (DOD) civilian. He has led an eclectic civilian career after leaving active duty in the Air Force in 2002 to work full time as a scientist and developer. Mr. Ortiz traveled the world to secure some of our nation's most important facilities. In 2008 he switched careers and moved to the Joint Staff where he advised the J-6 on multiple DOD cyber and information assurance programs. He then began work in division-level leadership jobs that created, sustained, and managed cyber operations centers. Mr. Ortiz's military career is similarly diverse, spanning more than 4 years of active duty and another 14 as a reservist. He has worked in 4 distinct career fields, including air battle management, intelligence, research, and cyber operations. Currently, he serves as the individual mobilization augmentee (IMA) to the director of operations for the 315th Cyber Operations Squadron. In his spare time, he volunteers on the Norwich University Alumni Association Board of Directors, providing career and resume counseling to many alumni. Mr. Ortiz resides in Maryland with his wife and four children, who fill his leisure time with an endless supply of hilarious soliloquies and craziness.

Let us know what you think! Leave a comment!

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

The Trilateral Strategic Initiative

A Primer for Developing Future Airpower Cooperation*

Col Peter Goldfein, USAF
Wing Cdr André Adamson, PhD, RAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

Since the rudimentary deconfliction measures of the First World War, the US Air Force, Royal Air Force, and French Air Force have developed their ability to conduct coordinated air operations, a practice they have further refined since the end of the Cold War. Interoperability—the effective integration of planning and execution during coalition operations—is now a critical factor for success. Specific to air operations, the importance of interoperability has consistently been identified during North Atlantic Treaty Organization (NATO) actions in the Balkans, Afghanistan, and Libya, as well as ongoing coalition efforts in Iraq, Syria, and sub-Saharan Africa. Although each campaign has highlighted specific challenges for the three air forces, they have also demonstrated the potential of airpower integration. Thus, even though all three nations reserve their prerogative to act autonomously, a coalition effort seems a likely response to future crises.

Current doctrine and future strategy also confirm the importance of a coalition approach to air operations.[1] Broadly speaking, coalition operations offer some tangible advantages. Specifically, political resilience, strategic reach, and individual niche capabilities are better employed when air forces combine capacity. The identification of common objectives makes national efforts more closely aligned and coherent. Additionally, responding collectively at short notice is increasingly important to national leadership; consequently, success depends upon the constant monitoring of and investment in interoperability, even for the closest of allies. Operations act as a catalyst to integration (through sheer necessity), but difficulties that emerge during complex multinational operations point to the need to preempt those frictions by raising the baseline of trust and interoperability ahead of the next operation. The effort demands clearly articulated political intent, the identification of common objectives, and the necessary resources to develop a trust-based, effective partnership.

*This article is reprinted from *Air and Space Power Journal–Africa and Francophonie* 7, no. 1 (1st Quarter 2016): 5–13.

The Trilateral Strategic Initiative (TSI) provides one such framework. The initiative had its origins in the personal relationships among the three air force chiefs who articulated their initial vision via a letter of intent in 2011 and signed a TSI charter in 2013, which not only outlines both intent and objectives but also designates a steering group. Three pillars of strategic importance lie at the heart of the initiative: increasing trust, improving interoperability, and advocating for airpower. Together, they set conditions for the more effective employment of airpower. Oversight of the initiative is the responsibility of the Trilateral Strategic Steering Group (TSSG), composed of senior officers from the three nations, serving in trinational teams placed in strategic posts close to the chiefs. This arrangement maximizes their effectiveness in areas of trilateral interest.[2] The TSI is now in its third generation of trilateral chiefs who are equally supportive of the initiative, and a new version of the charter was recently signed at the Royal International Air Tattoo, United Kingdom, in July 2015.

To better understand the potential of this initiative and its steering group as a model for advancing international cooperation, one must explore the elements that make it a viable proposition for the constituent air forces. Doing so requires consideration of the initiative's defining characteristics, the means chosen by the steering group to develop it, and the challenges that the initiative faces to achieve its goals.

Natural Convergences and Characteristics of the TSI Model

The US, French, and Royal air forces have strong historic and cultural ties; moreover, each has played a predominant role in developing and employing airpower as an instrument of national security. The core values of integrity, service, and excellence permeate these countries' military cultures, which also have been shaped by a historic record demonstrating a consistent political appetite to employ airpower in support of national and international interests.

Existing and emerging crises have brought about a convergence of many national security objectives for the United States, France, and United Kingdom. Further, contextual reality, simultaneous multinational global operations, the diversity of threats to collective security, and an environment of increasing financial scrutiny continue to support a more compelling case for cooperation. At the same time, each of the three air forces has confronted the issues of maintaining readiness while remaining committed to expeditionary operations and wide-scale modernization. Such centripetal forces, therefore, have reinforced the need for "burden sharing" and have highlighted the value of effective military cooperation. All of these factors validate the chiefs' vision of shared operational efficiency.

As for the characteristics of the TSI that help define its potential to progress under this vision, two in particular stand out. First, the exchange of senior officers who make up the steering group offers a small-scale but enduring framework to build trust and improve interoperability at the strategic level of each air force. Granted, the crucible of a multinational air campaign or even a complex exercise normally results in improved trust and interoperability among international participants. However, without a permanent framework designed to capitalize on progress, any advances risk being overlooked in subsequent efforts. Although not designed as a "lessons learned" mechanism, the TSI does give each air staff a mandate to promote an agenda of improving international cooperation, and its multinational steering group includes action officers charged with that responsibility. Second, the fact that the TSSG operates without the cumbersome bureaucracy commonly associated with a formal alliance or coalition gives it the liberty to creatively pursue the chiefs' vision within the limits of its resources and to be innovative in its approach.

The convergence of values, as well as historic and current context, combined with national and organizational goals across the three air forces, helps explain the "why" behind the TSI, and the defining characteristics of its steering group help clarify the parameters of their mission. The "how"—the means employed under the initiative to realize its ambition—clearly need to be consistent with these parameters in order to sustain the tangible progress towards fulfilling the vision of the three service chiefs.

Means

The establishment in each air staff of a cadre of international officers responsible for driving trilateral cooperation at the highest level of each air force, itself a manifestation of trust, is a central pillar of delivering this vision. As with any exchange of international officers, incumbents quickly recognize the limitations of a purely national view, and their perspectives are necessarily broadened by their wider exposure. Although tactical-level exchange officers are rightly focused on developing tactics, techniques, and procedures, the individuals on this strategic exchange cross-pollinate ideas and concepts that directly influence the employment of airpower. In turn, having privileged access to the air force chiefs, they are well placed to influence the thinking of senior leaders.

The approach adopted by the steering group is a relatively simple one: it identifies impediments to airpower's interoperability and presents solutions involving trilateral cooperation. The basis of the chosen model is ongoing collaboration among the elements of the steering group in each air force, creating opportunities for an informal exchange of ideas and for the sharing and debating of concepts (flavored by the perspective of each air staff) designed to feed the thinking of senior leaders. By maintaining an understanding of ongoing bilateral initiatives among the three air forces and an awareness of their institutional and operational priorities, the steering group can identify areas most likely of interest for trilateral cooperation. The desired results are not predicated upon placing any one nation in a lead role; rather, given the open-ended nature of the initiative, the interoperability and trust it seeks to build could support any number of cooperative constructs well adapted to a variety of operational requirements. To prime this model, each air force must select officers for this type of exchange who are well suited professionally and personally for the demands of duty at the strategic level of an air staff and who possess additional traits necessary to collaborate and advance a trilateral agenda while serving abroad. To inform its own internal discussions, the TSSG has brought together subject-matter experts and has hosted a number of forums on a rotational basis, reflecting the service chiefs' specific priorities or deriving from major lessons identified during combined operations. Previous subjects have included combined crisis response, command and control, operational readiness, air advocacy, and national approaches to regional tensions. The formats have included workshops, planning exercises that address particular scenarios, academic seminars on airpower topics, and broad analyses. Generally, TSI activity also incorporates civilians, academics, and members of think tanks who make recommendations that will have the most impact not only on modifying reflexes and shaping behaviors but also on improving trust. The subsequent publication of trilateral results is intended to influence broader, higher-level national debate.

By steadily developing the network of officers and civilian airpower professionals associated with the TSI, efforts to institutionalize this collegiate approach are gaining traction. In Europe, trilateral cooperation has taken root among the three air operations centers, initiated through a series of exercises called Tonnerre-Lightning, launched in 2013 to conduct combined air command and control and to incorporate live sorties under progressively more complex scenarios.[3] With its imperative to maximize the output of trilateral exercises, the combined air staff continually identifies opportunities to integrate collective aims into the exercise calendar. This aspect of the trilateral relationship has been reinforced by quarterly video teleconferences among air operations chiefs of the three air forces and by a new operational trilateral charter that they signed in March 2015.[4]

The trilateral exercise hosted by the US Air Force's Air Combat Command at Langley AFB, Virginia, in December 2015 is another excellent example of cooperation. US F-22 Raptor, French Rafale, and UK Typhoon aircraft operated together for two weeks at Langley to develop and better integrate their niche capabilities. This type of initiative, which seeks to prepare our combat forces prior to a complex conflict, concentrated on generating a disproportionate operational advantage. Other, equally pertinent opportunities for trilateral cooperation exist. An infrastructure-protection exercise held at the Avon Park auxiliary field in Florida in 2015 highlighted how this sort of cooperation can extend beyond aircraft participation. Security forces from each air force sought to protect and defend an air base by utilizing shared resources and objectives. The exercise provided an excellent basis for future operational integration among support mechanisms for air operations.

Efforts conducted under the TSI also contribute to more effective and credible air advocacy. Each of the air chiefs recognizes the priority of preparing airmen to positively influence joint and national decision makers. The most recent trilateral workshop, conducted in Washington, DC, in March 2015, was tailored to crafting a more refined, targeted trilateral airpower narrative. Furthermore, by contributing to the development of airpower, other allies can benefit from the TSI acting as a "trailblazer" or an intellectual catalyst. Results of TSI-sponsored activities have already informed ongoing debates within NATO and in the headquarters of allied air forces. The initiative can have a continuing role as a body representing the position of the three most capable air forces in the alliance on a broad range of airpower determinants. The seventh TSI workshop, to be held in France in 2016, will address potential convergences among the three air forces' visions of future airpower employment. Moreover, it will shape recommendations for areas of emphasis in the trilateral relationship, which can complement a wider NATO study on the future of joint airpower in the alliance.

Intrinsic Challenges

Just as trilateral progress requires continuous effort, so does it demand perseverance in overcoming a variety of challenges. Fulfilling the trilateral vision of the chiefs calls for stamina, patience, and a deep cultural understanding of the three air forces so they can reach a mutually agreeable position. The steering group's independence from organizational bureaucracy, a sort of blessing from which it derives a substantial degree of freedom of action, can equally be viewed as a curse when it comes to implementing trilateral activities.[5] The streamlined nature of the model, which empowers a small group of senior officers to creatively advance their service chiefs' vision, helps minimize implementation costs to each service. It sits on the opposite end of the spectrum from treaty-based military cooperation, created to respond to higher and more complex political objectives that require significant investment across the joint military staffs of participating allies into the oversight of cooperative objectives. Although the trilateral steering group is easier to implement than a treaty-based military hierarchy, its independence from organizational oversight means that the group cannot act as an empowered executive staff entity. Rather, it relies on initiative and creativity to overcome friction, and—given the limited degree of direct leverage that the steering group can exert on senior decision and policy makers—it must make the most effective use of its time and manpower.

At the practical level, a common impediment to cooperation is simply a lack of technical interoperability. Incompatibility of communication, information, and computer systems has a significant effect on effective integration. Coupled with the commercial sensitivities associated with procurement and open competition within the defense sector, such incompatibility makes industrial collaboration an even more complex issue. Therefore, new approaches to defense procurement may need to innovate; it is even conceivable that trilateral interoperability could become a contracted requirement in the future. Equally, in the conduct of air operations, trilateral activities will be inherently more complex than either national or bilateral alternatives and, at least initially, will demand more time to plan. To be addressed effectively, matters such as information exchange, security caveats, and intelligence sharing will call for considerable effort and trust. A central aspect of this shift is the willingness to exchange sensitive information. That is, building trust and confidence will depend upon moving from the principle of a "need to know," which underpins many protocols related to information security, towards a "need to share" in the context of multinational operations. The TSI facilitates this principle by promoting among the partner nations an open exchange of concepts and doctrine that can propagate into wider, more accepted practices. A lack of language proficiency can also reinforce technical and procedural barriers. During a recent combined joint expeditionary force exercise between the United Kingdom and France, for example, translation and communication issues were identified as one of the major impediments to timely and accurate decision making in the combined headquarters.

However, the predominant strategic impediment to trilateral activity is cultural. Despite historic links and an increasingly rich operational capital to draw on, vested national interests and "national reflexes" can still offer a reassuring alternative to the inevitable friction and uncertainties associated with multinational operations. Even with shared NATO doctrine, defense policy and ambition are not identical and reflect the capacities and priorities of each nation. The US-UK "special relationship," however defined, is woven into the cultural fabric of generations of military and political classes in the United Kingdom.[6] This kinship greatly facilitates cooperation between the two countries' air forces but is insufficient in itself to ensure an equally coherent trilateral relationship. Similarly, the principle of strategic autonomy is a sine qua non to France's defense policy and continues to define many aspects of its military culture.[7] Work under the TSI, therefore, must honestly acknowledge these differences and identify and exploit opportunities in each bilateral relationship to better align behaviors at a trilateral level.[8]

Furthermore, practical realities within each air force demand that a preponderance of the effort focus on national priorities. The inevitable consequence for most airmen is an infrequent exposure to their international counterparts, which in turn reinforces cultural reflexes towards national solutions when a country faces the need to employ airpower. Activities sponsored under the trilateral initiative are designed to expose participants to the potential of multinational operations and seek to readjust their reflexes for national responses towards a more trilateral perspective. The model must also confront limitations associated with any single-service initiative, given that many issues of interest to the three air forces inevitably have joint equities. If the TSI is to address those issues, exposure to the joint level will be necessary, and—in the absence of parallel trilateral initiatives outside the air domain—solutions for particular matters must be sought on a case-by-case basis.

Finally, the dynamic and cyclic nature of national politics presents a challenge to continuity. The TSI's ambition to continuously improve integration is vulnerable to political cycles—a nation's appetite for foreign intervention can change on short notice. Moreover, the level of priority afforded to defense and security concerns in national dialogues can have a profound effect on the sustainment of military partnerships. To remain insulated from these dynamics, cooperative initiatives such as the TSI must constantly prove their value. Thus, ambition should be tempered accordingly. The TSI was never intended to become the basis for an executive body in each air staff; rather, it serves as a framework designed to inspire activities to strengthen personal relationships, develop mutual understanding, and build confidence.

Consequently, even though the initiative offers a common vision for high-level trilateral cooperation, technical challenges, cultural dynamics, and national priorities will inevitably act as a drag on the rate of progress. Faced with these issues, the three countries will find that results are often difficult to quantify and must be validated against more pragmatic criteria. In this context, incremental gains and gradual progress pursued under the TSI meet the spirit of the chiefs' vision and reflect the relatively informal nature of the steering group they established to pilot the initiative.

Conclusion

Although not a unique approach, the TSI and the steering group responsible for its implementation represent an original and potentially innovative model for exploring common ground and improving coherence in the development and employment of airpower. Each nation offers a different perspective on how to employ air and space capabilities, but the TSI seeks to refine the combined capabilities of the three air forces to respond as a team to rapidly emerging crises. By implementing a valuable forum for strategic communication and coordination, these air forces can identify and address operational impediments, establish greater cohesion, and explore the frontiers of trilateral cooperation.

As for the chosen means to implement the initiative, one finds an elegant approach in the establishment of a multinational steering group cross-pollinated at the strategic level of the three air staffs, which collaborates and sponsors trilateral activities, free from bureaucratic oversight but equally limited in its executive role. Its simplicity differs significantly from more formalized and more ambitious cooperative models such as the NATO command structure and the framework created in the French and UK military staffs to advance political objectives of the Lancaster House treaty. In this sense, the group meets the chiefs' intent to advance their vision while respecting the practical realities confronting each air staff and its capacities to confront cultural barriers and practical challenges. The success of the TSSG depends on cultivating a community of participants in its trilateral activities and widening the number of individuals exposed to the results of its debates.

As this model gains traction, some questions inevitably arise concerning the broader utility of such an agreement: what, for example, might its applicability be for land and maritime forces or within a joint construct among the United States, the United Kingdom, and France? These aspects could broaden trilateral cooperation to build trust and advance interoperability across a wider spectrum of military operations. Are there other international trilateral groupings that might benefit from a similar initiative of their own, based on its own logic, such as that of regional cooperation? Responses to these types of questions could depend on exposure and evaluation of this trilateral initiative beyond the three participating air forces.

The future success of trilateral efforts under this model hinges on several factors: sustained political intent, the highest levels of support within each air force, and continued evidence of advancement towards objectives. This progress is anticipated on multiple fronts in 2016, in collateral activities subsequent to the December 2015 trilateral exercise at Langley AFB, in the continuation of the Tonnerre-Lightning exercise series in Europe, and directly from the forthcoming TSSG workshop in France. The strategic context demands these types of efforts from close allies, and ongoing operations are sure to reinforce this requirement. The TSI model is a valuable tool in meeting that need. ✪

Notes

[1] Joint Doctrine Publication 0-30, *UK Air and Space Doctrine*, July 2013, 2-5–2-6; Joint Concept Note 3/12, *Future Air and Space Operating Concept*, September 2012, 1-12–1-13; Department of the Air Force, *USAF Strategic Master Plan* (Washington, DC: Department of the Air Force, May 2015), 28–29, 34–35; and Ministère de la Défense, *Livre Blanc: Défense et Sécurité Nationale* (Paris: Ministère de la Défense, 2013), 21.

[2] The US Air Force hosts UK and French officers in its Strategic Studies Group (HAF/SSG); the French Air Force hosts US and UK officers in its Plans Bureau, Strategic Studies Division; and the Royal Air Force hosts US and French officers in its Air Staff, International and Engagement Division.

[3] The three centers include the 603rd Air and Space Operations Center at Ramstein Air Base, Germany; the UK joint force air component commander at RAF High Wycombe, England; and the French Centre National des Opérations Aériennes at Lyon Mont-Verdun Air Base, France.

[4] An agreement between the US Air Force's Third Air Force commander, the Royal Air Force's commander of operations, and the French Air Force's commander of air defense and air operations, the document creates a framework for multiple trilateral working groups designed to improve interoperability, specifically in the planning and conduct of air operations.

[5] This independence could be contrasted with the proliferation of bilateral responsibilities assigned to officers in the military staffs of France and the United Kingdom as a result of the 2010 Lancaster House Treaty on Defense and Security Cooperation, a binding agreement designed to significantly improve defense and security cooperation between the two allies. Implementation has resulted in well-developed plans at the joint and single-service level to field a combined joint expeditionary force, providing a scalable asset up to two brigades in strength with an associated naval task group and air expeditionary wing. Of necessity, this approach demands general officer engagement at multiple staff levels and a commitment to training and regular exercises.

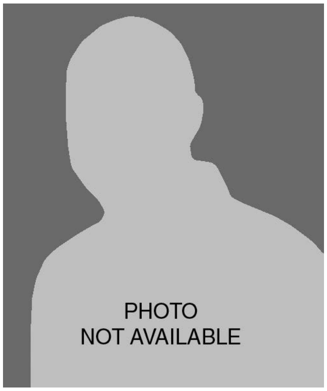
[6] The US Air Force and Royal Air Force benefit from a privileged level of information sharing that underpins a robust officer exchange program and a tradition of high-level bilateral training. Though somewhat mirrored in the post–Lancaster House Treaty growth of UK-French cooperation, this sharing still outbalances similar US Air Force programs with the French Air Force.

[7] Ministère de la Défense, *Livre Blanc*, 19–22.

[8] Bilateral relationships include those provided under the United Kingdom–France Lancaster House Treaty and those that arise from increasing US-French cooperation in Africa.

Col Peter Goldfein, USAF

Colonel Goldfein (BSE, University of Michigan; MA, Army Command and General Staff College; MA, Air War College) is a command pilot with extensive operational experience in both Air Mobility Command and Air Force Special Operations Command. He has completed NATO staff tours at the Joint Warfare Center and in the command group at Supreme Headquarters Allied Powers, Europe. Since 2013 he has been the USAF exchange officer to the French Air Staff, serving in the strategy division.



Wing Cdr André Adamson, RAF, PhD

Wing Commander Adamson (MS, PhD, King's College London) is a flight operations officer who has operational experience in Afghanistan, Bosnia, and Mali. He has also completed assignments in Germany and Canada. Since 2014 Wing Commander Adamson has been the RAF exchange officer to the French Air Staff, serving in the strategy division.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

C4ISR via Dark Webs

An Alternative Concept for Protecting Critical Information in Contested Cyberspace Environments

Capt Kyle L. Bingman, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

The world is increasingly connected, both physically and metaphorically, by the relentless spread of networks such as the Internet and the multitude of devices reaching out for the information it contains. Even further, individuals, organizations, and nation-states are becoming more reliant on this interconnected world for activities from the mundane to the critical. This trend towards greater connectivity is likely to continue on an upward spiral. According to research done by Cisco Systems, global Internet protocol traffic in the past five years has increased fivefold and will pass the zettabyte threshold (approximately 1 trillion gigabytes or 10^{24} bytes) by the end of 2016.[1] At the same time as this astounding development and its consequent benefits for society are occurring, however, cybersecurity incidents have increased. In 2015 over $75 billion (US) were spent on cybersecurity in an attempt to safeguard protected information from a range of malicious actors including criminals and those working for nation-states.[2] The United States made this outlay despite acknowledgment that the most often pursued method of cyber defense—defense in depth—has failed time and again.[3]

This complex and insecure reality affects not only the civilian world but also the military; the US Air Force is most certainly not exempt from this situation. Instead, with its dependency on integrated communications and weapons systems to carry out key missions, it is the service perhaps most reliant on this incredibly vulnerable construct of networks and devices. Over the years, the Air Force has attempted to posture itself in a manner that allows it to maintain surety and the integrity of its networks and information by using the same defense-in-depth method of cybersecurity as the commercial sector. However, as evidenced by successful attacks against many of the most critical networks, this approach is becoming a losing battle against skilled adversaries who can outpace the development of new defenses.[4] Faced with near-peer cyber actors such as China and Russia, among others, as well as highly skilled independent and transnational actors, the Air Force must find a way to ensure the accessibility and usability of its key information by a means that departs from the status quo. Otherwise, it must accept significant risk during future operations due to adversarial actions taken in cyberspace. This article details the nature of this complex, problematic reality and offers a solution for the service to regain control and the integrity of its key information.

The Situation

Capabilities designed to connect nodes quickly and share information act as a force multiplier because of gains in effectiveness. The interconnected environment allows military forces to resupply, coordinate, reposition, and share intelligence at incredible speeds. Yet, as much as these capabilities open possibilities for the Air Force, they also expose vulnerabilities. Actors around the globe—from the nation-state level to hacktivists, from China and Russia to Anonymous—recognize this fact as well. Cyberspace is now the first war-fighting domain and, perhaps more specifically, the first and primary target as the default means to initiate hostilities. Leaders in China's People's Liberation Army, for instance, have embraced the idea that successful war fighting is predicated on exerting control over the adversary's information and associated infrastructure. Assessments state that during a conflict, the army would target logistics; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and other mission-critical systems to delay US force flow into a theater and to degrade war-fighting capabilities.[5] In other instances, individual, unaffiliated hackers have expressed interest in military systems or have conducted attacks that highlighted significant vulnerabilities in military-related networks. These include hacks of satellites and associated systems, attacks that caused physical damage by means of malicious code, and distributed-denial-of-service strikes that significantly degraded globally scaled networks.[6] The examples are innumerable, but a theme runs through them all: the Air Force relies on information systems to manage and operate a high-technology force, but those same systems are at the center of many potential adversaries' targeting bull's-eyes.

Many assessments acknowledge the likelihood that cyber attacks will be successful in degrading military capability and reducing capacity. In the Defense Science Board's 2013 report on the resiliency of military systems in the face of advanced cyber threats, experts noted that "the United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities."[7] The report goes on to say that, among other effects, "weapons and weapon systems may fail to operate as intended."[8] Other assessments are similarly dire in their pronouncements. Alan Shaffer, former assistant secretary of defense for research and engineering, admitted that "the Department of Defense is being challenged for technological superiority in ways we have not seen for many years," including cyberspace.[9] He added that "systems whose capabilities can be negated by cyber-attack offer no advantage to the United States."[10] In subsequent testimony to Congress, Mr. Shaffer went on to say that "this has led to a situation where . . . US superiority in many warfare domains will be at risk."[11] That is, future conflicts are not likely to be ones of *Blue versus Red* as we typically conceptualize conflict but ones of *Blue versus the operational constraints imposed by a contested cyberspace environment as created by Red*.[12] This construct benefits any actor with the desire to create an asymmetric advantage to prevent the United States from performing to its greatest abilities. If America has to fight to present, supply, and coordinate its forces, then the likelihood of success is small as long as its forces struggle against the constraints rather than expend resources against the adversary. To overcome this situation, US forces must find a way to act *beyond* the constraints in order to conduct C4ISR effectively. Current methods, however, fail to enable this requirement.

Defense in Depth

At the moment, the method utilized to handle this situation and secure the Air Force's critical systems is the traditional defense-in-depth means of cybersecurity. Developed in the early days of the Internet when security was not a significant concern, defense in depth applied the principles of separation and distance so effective for securing assets in the physical world to the growing cyber world. It did so despite the fact that these physical laws are irrelevant in the cyber domain unless one is referring to the physical infrastructure upon which it exists. With defense in depth, networks are protected by using layers of detection and protection mechanisms such as firewalls, intrusion-detection systems, antivirus software, physical security, and an informed user base. Like an army besieging a castle, defense in depth notionally forces an attacker to expend a large number of resources attempting to find a way into a target network. However, regardless of the significant amount of money and effort put into building these protective mechanisms, they have largely proved ineffective against the most creative and skilled attackers. Instead of attackers being deterred by resource costs required to sustain a siege, the situation reversed itself so that network defenders expend massive numbers of resources in an attempt to withstand almost constant intrusions by the adversary.

Statistics of recent years reveal this unfortunate truth quite plainly. In 2014 the number of reported cybersecurity incidents around the world rose 48 percent; furthermore, another cybersecurity firm reported that as many as 71 percent of compromises go undetected.[13] Additionally, when compromises are detected, approximately 90 percent were enabled by malware targeted and specifically crafted for a particular system, thereby ensuring that it would elude detection or mitigation by commonly used defense-in-depth mechanisms.[14] With over 1 million malware threats released per day, it is no wonder that the cybersecurity firm SANS perceptibly referred to defense in depth as "unsustainable"; indeed, advanced threats are outpacing defenses.[15] Around the same time, the National Science Foundation's Special Cyber Operations Research and Engineering Committee pointedly stated that "defense-in-depth failed to provide information assurance against all but the most elementary threats, in the process putting at risk mission essential functions."[16] The group then went on to speculate whether defense in depth was actually a means to "defer harm rather than a means to security."[17] Such speculation has proved accurate; the defense-in-depth status quo will not protect key systems and information used by the Air Force to carry out operations from the most advanced attackers. Unfortunately, this truth remains largely unacknowledged because of a cultural unwillingness to shift to a new mode of conceptualizing the cyber world.

Continuing to utilize defense in depth as the sole mechanism for cybersecurity adheres to a view of the world in which kinetic conflict was the sole method of war.

This perspective still offers viable solutions for the kinetic world; however, it became less relevant when cyberspace made distance and topography no longer the defining concerns for a military's defense. Attempting to rely only on defense in depth for cybersecurity essentially amounts to trying to protect a three-dimensional world from adversaries with access to a fourth dimension—there is always a way for them to gain access when they can see from a different viewpoint. As Gen Stanley McChrystal, USA, retired, mentioned in a recent talk, defense in depth is effectively a "Maginot Line" method of cybersecurity.[18] It is successful in keeping many less capable or less innovative adversaries out of networks—an assured benefit—but it will also result in the skilled opposition finding a new and less expected way past the barrier. The standard defense-in-depth responses of increasing the layered defense around networks—and even newer initiatives such as using hunter teams as point-defense-type mechanisms—are not going to be completely effective when adversaries have had years to prepare access to networks under defenders' watchful eyes. Change is clearly needed. Any method of defense that is to be truly effective in protecting key information and systems needed for C4ISR must also embrace the characteristics of cyberspace as it truly exists rather than try to make it conform to an outdated understanding that it surpasses and encompasses.

A Solution

Although the current outlook is bleak, the situation can be improved if Air Force leadership decides to radically alter its current methods of carrying out C4ISR in a contested environment. The service must be prepared to implement an additional, radically different construct for C4ISR that belies any previous method or network and—in all likelihood—that runs markedly against the current common culture of widespread information sharing and common operating pictures. Only through this type of additional defensive option can the Air Force increase the chances of operational success, thereby mitigating the likely actions of a skilled adversary. The following steps detail the main components of a truly viable C4ISR system for contested environments.

Information Prioritization and Risk Assessment

Prior to the start of a conflict with an adversary who has sufficient capability to disrupt current C4ISR systems and networks, information must be prioritized in terms of its necessity to create effects as well as the amount of risk that can be accepted within a set of information due to deception. Information that is less necessary or for which an acceptable amount of risk can be anticipated or mitigated without notable difficulty should continue to be passed via primary methods. One should do so not only to limit the scope of the additional method of communication detailed below but also to ensure that no noticeable decrease occurs in traffic that could cue an adversary to this method.

Unassociated Infrastructure

During a conflict, the Air Force must not rely solely on any previously utilized network or system to pass key information or maintain a common operating picture. Instead, it must switch to systems that have never been used and that have been verified in origin to mitigate a potential supply chain or otherwise previously placed malware. Moreover, the service must utilize a network entirely unassociated with the current means of passing military-related traffic. The speed and covert nature with which this new construct must be set up will limit its size and require that only key participants have access to it. Only information deemed essential will be passed via this network. Information for which misinformation or degradation is an acceptable risk can and should still be passed by current methods and systems. Doing so not only will lower the required scale of the network necessary to pass key information but also will ensure that a significant decline in traffic on current networks will not act as an indicator for the adversary. Development and testing of this alternative network—as well as its other components, discussed below—must take place outside the standard acquisitions process to guarantee its unanticipated use.

Commercial Networks and Dark Webs

Traffic must pass entirely over commercial networks, ideally transiting through and primarily remaining in dark web, peer-to-peer networks such as the Invisible Internet Project or Freenet.[19] Because the Internet is a distributed network of networks constantly reestablishing connections with each other rather than a single, coordinated system, it can essentially self-heal and remain available even under attack; disruptions in routes are temporary and often quickly subverted. The global nature of the Internet also increases its resiliency since effects to one region can be mitigated by shifting to routes through another. Peer-to-peer networks have proved even stronger with this capability, as seen in their numerous, successful evasions of law enforcement's attempts to take them down.[20] This resiliency could be strengthened by augmenting the diversity of possible connection infrastructure from primarily fiber-optic lines; however, the Internet's current state is still strong. Given the amount of traffic transiting the Internet as well as the inherent anonymity of dark web network users, key data would be secured by the obscurity of hiding in plain sight rather than relying on defense-in-depth mechanisms such as firewalls and intrusion-detection systems around known military networks.

Constantly Shifting Data

Data must not be stored in the same place for a significant period of time. Using technologies such as cloud hosting and the peer-to-peer construct upon which many dark web networks are built, one must shift any large store of information from location to location frequently. Doing so will help ensure that if an adversary does detect this additional method of C4ISR, he will have a difficult time catching up to the numerous shifts and that, if the actor does locate it, he will have visibility for only a short period of time.

Multiple and Redundant Data Paths

There must be multiple ways to input data to and retrieve it from this dark-web-based information store. One must be able to abandon ties to information paths traditionally considered "secure" for the most crucial information in view of potential compromise by a skilled opponent. Instead, key data must be input into and retrieved from the dark web data store surreptitiously and in the clear by multiple methods—again utilizing the principle of hiding in plain sight. Any source or location could input data by methods including automated posts from all forms of sensors or even less traditional ones such as using chat platforms or forums. By not being dependent on a single method or source, the Air Force gains not only security through obscurity but also resiliency. Further, given the nature of peer-to-peer dark web networks, loss of one information path would not reveal the central store or result in the compromise of other data paths.

"Honeycomb" Information Sharing

Information fusion and analysis must happen in nontraditional settings not associated with traditional centers such as those throughout the distributed common ground system (DCGS). Because the latter is an existing system, one must assume that it is compromised. Rather than information flowing in a hierarchical manner to a specific group of analysts, it must move throughout weapons systems, analysts, and planners around the world in a honeycomb manner to make full use of processing capabilities as well as data points. Information sources would "push" small notifications of data points that they can provide while requirements could be "pulled" by sources as needed, thereby limiting the amount of traffic passed through the network and aiding in its hiding in plain sight. Since the DCGS construct already has placed analysts and associated requirements around the world, the personnel are in place; however, they must be moved away from known military facilities to new sites equipped with the required technologies. Any or all sites could carry out analysis, but the construct could change this situation throughout the operation, based on the viability of data paths to particular sites. To make this scenario actionable, one would have to conduct a full study of personnel needs for this "all-source DCGS."

Replaceable Hardware

These sites and others tied into this new C4ISR network must not rely either on large-scale critical infrastructure or single methods of connection to the Internet. In light of the nature of possible power outages and the chance for compromise, it is essential that any system be able to stand alone and be easily replaced. Consequently, the Air Force must rely on systems more reflective of the current cyber domain, such as laptops and tablets that can be swapped quickly and easily disposed of. Moreover, the service must utilize multiple access points to the Internet, from traditional fiber connections to more open means such as cell networks or public WiFi hot spots.

Defense via Deception

The Air Force must develop a deception capability to assist in hiding the existence of this additional communication method in the event that it is discovered. By flooding the Internet with realistic but deceptive traffic, one could force an adversary to spend a considerable amount of time working to discern which information was real and which was not.

Conclusion

In essence, these are the tactics of asymmetric actors such as insurgents. This proposed means of C4ISR clearly breaks with the Air Force's current culture of hierarchical information flow and decision making as well as its belief in defense in depth as the most effective means to secure information. Defense in depth as a means of cybersecurity does safeguard networks against lower-level threats and should not be abandoned, but it is not a viable solution for securing the most critical information during a conflict. The solution, one possible conception of which was detailed above, calls for embracing a broader understanding of security that acknowledges the true strengths of cyberspace. By utilizing dark web capabilities, taking advantage of the geographic relativity of cyberspace, and embracing a honeycomb flow of information, the Air Force can overcome the constraints upon C4ISR that an enemy will attempt to place on the service during a conflict.

Adopting such methods would be unconventional. Nevertheless, failing to do so is to ignore not only the fact that the domains in which the service fights have expanded but also that cyberspace is a drastically different realm. By utilizing only models like defense in depth to secure its information rather than accepting the new environment in a way that also takes advantage of its strengths, the Air Force is not protecting its key information in the best possible way but is making it easier for an adversary to find and access that data. Cyberspace operations have the strong potential to negate the effectiveness of the service's operations if the status quo does not change. It is time for the Air Force to accept the true nature of cyberspace and operate there using capabilities designed for success in that domain. ✪

Notes

[1] "The Zettabyte Era—Trends and Analysis," Cisco, 2 June 2016, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html.

[2] "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015," Gartner, 23 September 2015, http://www.gartner.com/newsroom/id/3135617.

[3] *Defense in depth* is a broad term and can mean, without error, many different things to different people. This article uses the term only to refer to a layered defensive construct for a network that includes technology-based elements such as firewalls and intrusion-detection and -prevention systems, administrative elements such as password policies and bans on removable media, and physical elements such as securing access to hardware components.

4. Numerous examples of critical networks could be cited here. A sampling of the most important, post-Stuxnet, include Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Dan Goodin, "Active Malware Operation Lets Attackers Sabotage US Energy Industry," *Ars Technica*, 30 June 2014, http://arstechnica.com/security/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/; Dan McWhorter, "Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators," FireEye, 19 February 2013, https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html; and Nicole Perlroth, "In Attack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

5. Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (West Falls Church, VA: Northrop Grumman Corporation, 7 March 2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf; and Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: Office of the Secretary of Defense, 7 April 2015), http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

6. Tony Capaccio and Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites," Bloomberg Technology, 26 October 2011, http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites; and Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, 8 January 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/. The example of distributed-denial-of-service attacks is not clearly related to the Air Force but shows how even a small group of technically skilled actors can produce serious effects against large networks. Often accused of "ruining Christmas" just to anger people and doing little to refute the claim, Lizard Squad is an example of the type of rogue actor that should be considered alongside more organized groups when one thinks of conflict in cyberspace. Abby Ohlheiser, "Xbox Live Is Up, PlayStation's Network Still Recovering after Christmas Day Outage," *Washington Post*, 26 December 2014, https://www.washingtonpost.com/news/national/wp/2014/12/26/playstation-and-xboxs-networks-are-still-recovering-from-a-christmas-day-outage.

7. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Department of Defense, Defense Science Board, January 2013), [ii], http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

8. Ibid., 28.

9. Senate, *Testimony before the Senate Appropriations Subcommittee on Defense, Witness Statement of HON Frank Kendall, Under Secretary of Defense for Acquisition, Technology & Logistics, Mr. Alan Shaffer, Principal Deputy Assistant Secretary of Defense for Research & Engineering, Dr. Arati Prabhakar, Director, Defense Advanced Research Projects Agency*, 114th Cong., 1st sess., 22 April 2015, 12, http://www.defenseinnovationmarketplace.mil/resources/042215DoDInnovationResearch-JointTestimony-SAC-D.pdf.

10. Ibid., 7.

11. House, *Statement Testimony of Mr. Alan R. Shaffer, Principal Deputy, Assistant Secretary of Defense for Research and Engineering, before the United States House of Representatives Committee on Armed Services, Subcommittee on Intelligence, Emerging Threats and Capabilities*, 113th Cong., 2nd sess., 26 March 2014, 9, http://www.acq.osd.mil/chieftechnologist/publications/docs/FY2015_TestimonyASD(RE)_ShafferA_20140326.pdf.

12. In military settings, "Blue" typically refers to friendly forces while "Red" refers to aggressor forces.

13. "The Global State of Information Security Survey 2015— Managing Cyber Risks in an Interconnected World," PWC, http://www.pwccn.com/home/eng/rcs_info_security_2015.html.

14. Rajendra Dodhiawala, "Why Protection Alone Won't Work Today," CounterTack, 14 December 2015, http://www.countertack.com/blog/why-protection-alone-wont-work-today.

15. Virginia Harrison and Jose Pagliery "Nearly 1 Million New Malware Threats Released Every Day," *CNN,* 14 April 2015, http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security; and Prescott E. Small, *Defense in Depth: An Impractical Strategy for a Cyber World* (Bethesda MD: SANS Institute, 14 November 2011), http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896.

16. "Assumption Buster Workshop: Defense-in-Depth Is a Smart Investment for Cyber Security" *Federal Register* 76, no. 8 (12 January 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-01-12/html/2011-522.htm.

17. Ibid.

18. "Stanley McChrystal," video, 4:15, Big Think, 2016, http://bigthink.com/videos/s-mcchrystal-cybersecurity.

19. The Internet is not the only means to share data among computers; rather, it is simply the most common as well as the most easily accessed because it is publicly indexed. Therefore, it is referred to as the "visible" or "surface" web. Other networks exist that serve a similar purpose but are neither indexed nor accessible without special software. These networks are often referred to as part of the "dark web" due to their security and anonymity. Many of them utilize a decentralized peer-to-peer framework that, along with encryption, makes it difficult to perform traffic analysis on shared data. Although it would be clear to an "observer" that someone was using a service like the Invisible Internet Project, it would be very difficult to determine what was being done or shared.

20. George Dvorsky, "Could Someone Really Destroy the Whole Internet?," *io9* (blog), 19 September 2012, http://io9.gizmodo.com/5944558/could-someone-really-destroy-the-whole-internet.

Capt Kyle L. Bingman, USAF

Captain Bingman (MA, American Military University) leads intelligence and war gaming for the Center of Strategy and Technology's Blue Horizons program. She is responsible for directing intelligence efforts supporting the USAF chief of staff's most forward-looking strategic study, evaluating the impact of emerging and disruptive technology as well as geostrategic trends on defense capabilities. As an intelligence officer with a unique background in cyberspace, Captain Bingman began her career as a part of Detachment 2, 318th Cyberspace Operations Group, where she worked to integrate offensive and defensive cyberspace operations into exercises such as Red Flag and USAF Weapons School events. She then was the senior analyst for the 57th Information Aggressor Squadron, where she led research efforts to ensure that the squadron's Red Team cyber operations replicated realistic, threat-based tactics. Prior to her current assignment, Captain Bingman was a senior instructor at Squadron Officer College.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

The Fifth-Generation Fighter Pilot Force

Col John D. Jogerst, USAF, Retired

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

The latest generation of combat aircraft provides us with amazing capabilities and an intractable problem. The cost of leading-edge technology is making these systems unaffordable in large numbers. Somehow we must get the needed combat capability—determined by the threat—from a constrained fleet.

Fifth-generation fighters like the F-22 and F-35 bring unparalleled capabilities to the fight. However, these platforms come at a cost. The original USAF proposal for 750 F-22 Raptors was reduced to 339 for operational reasons through the *Report on the Bottom-Up Review* and *Report of the Quadrennial Defense Review* after the breakup of the Soviet Union in 1991.[1] The F-22 program spent all the money originally budgeted for 399 aircraft yet bought only 188.[2] Not counting test, training, and Reserve aircraft, the Air Force should end up with about 126 combat-coded planes.[3] The 1998 budget limited the engineering and manufacturing development plus production costs for the F-22 program to $62 billion. By 2010 the Department of Defense had estimated the total spent to be $67 billion. Anyone can easily pick at those numbers. Development problems, changing requirements, inflation adjustments, and so forth, are all factors. However, they do not change the result for the public who pays the bills and the members of Congress who represent them. They gave us the money, and we spent it all.

The history and current status of the F-35 program seem to be following a similar path. What we learn from this admittedly small historical sample is that we are likely to see lower numbers than we would like, making it imperative that we get the most out of every airframe.

Of course, simple numbers of aircraft are not capability. For the air component commander, capability includes what aircraft bring to the fight as well as how many are in the fight at the time. The key is how often we can put those relatively few aircraft into the fight and keep them there—captured in the aircraft utilization rate (how many hours per month an aircraft flies). More hours in the air for each aircraft equal more hours/sorties in the fight. That is the real metric to measure combat capability.

More time in the fight means less time on the ground. While we know how to hot-turn aircraft to rearm and refuel them quickly, just making a rapid turnaround will not solve the problem. The aircraft may be happy with a quick fill-up and reload, but the same cannot be said of the aircrew. There are fundamental limits to human endurance, and a combat sortie is not the place for anything less than peak performance.

Although crew ratios (CR) vary, the traditional USAF fighter squadron has 30 pilots for 24 aircraft or a 1.25:1 CR. With a few pilots detailed as planners or higher headquarters liaisons—or on the sick list—the deployed squadron can be quickly reduced to an effective 1:1 CR with one pilot per aircraft. For comparison, World War II single-engine fighter groups were also manned at one pilot per aircraft.[4]

Consequently, the combat capability available is limited by the human part of the system. People have a limited amount of endurance and a minimum amount of recovery time before reengaging. Crew duty-day constraints and crew-rest requirements can be waived, but it seems that doing so while conducting multiple, high-stress combat sorties is counterproductive. To overcome this limitation, we need to expand our hot turn to include refueling, rearming, and recrewing the aircraft.

This concept is not new for the USAF. It is built into the way we operate the airlift fleet. We maintain several crews (active duty and Reserve) for each aircraft in the inventory and position those crews to keep the aircraft moving.

We can do the same thing with a fifth-generation crew force for the fifth-generation fighter force. As each crew reaches its fatigue limit, the aircraft is quickly relaunched with fresh personnel and returns to the fight. Exactly how many crews are needed per aircraft will depend on theater requirements. For a quick example, let's assume a 2:1 CR.

Two crews per aircraft allow almost continuous utilization of each airframe. Instead of one sortie per aircraft daily, we get two. Each crew does a normal 12-hour duty day (planning, flying the mission, and debriefing) followed by 12 hours of recovery in crew rest.

With one simple change, we can turn 126 combat-coded airframes into 252 capable aircraft. Unfortunately, the situation is not quite that simple. Airplanes, like aircrews, need care and feeding. Logisticians know there's no such thing as a free lunch. Where do we get the people, spares, and consumables to double the aircraft utilization rate? How long will the airframes last?

The solution is to look at the original fighter program. An F-22 program with 339 aircraft is more than engineering and manufacturing development and acquisition funding. It includes enough aircrews, support personnel, spares, and so forth, in the out years to operate and maintain those planes. Congress only refused to provide increased funding to buy more airframes. If the Air Force simply maintained the remaining funding lines in the program, then we get the people and parts we need.

These costs are not trivial. Doubling the CR doubles the personnel and training expenses. We must pay not only for twice the number of aircrews per airframe but also for twice as many maintainers on the flight line and in the back shops. Those maintainers will also need roughly twice as many spare parts to keep the aircraft flying.

Airframe life is another constraint. If we fly more hours per aircraft, the basic structure of the airplane will wear out sooner. Although we can mitigate this situation with service-life extension programs, remanufacturing major components, and so forth, these costs are additional. Reducing peacetime training hours may be possible with increased use of simulators although doing so also involves cost increases as the fidelity and capability of the simulators improve. Ultimately, we should expect to have to replace the aircraft sooner.

The need to squeeze the most combat capability from a limited inventory has not gone entirely unnoticed. Brig Gen Peter Pauling, former commander of the Hawaii Air National Guard's 154th Wing, stated a preference for at least a 1.5 CR for the F-22.[5] Faced with a very limited number of F-35s, the Royal Netherlands Air Force is planning to man those aircraft at a 2.0 CR.[6]

Intentionally or not, the Air Force and Congress have decided that the additional combat capability is not worth the cost. The result is an Air Force operating the fifth-generation fighter force just as we did the first. ✪

Notes

[1] Les Aspin, *Report on the Bottom-Up Review* (Washington, DC: Department of Defense, October 1993), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA359953; and William S. Cohen, *Report of the Quadrennial Defense Review* (Washington, DC: Department of Defense, May 1997), http://www.dod.mil/pubs/qdr/.

[2] Jeremiah Gertler, *Air Force F-22 Fighter Program*, CRS Report RL31673 (Washington, DC: Congressional Research Service, 11 July 2013), 9–10.

[3] Larry Lawson, executive vice president and F-22 Program general manager, Lockheed Martin, quoted in David Fulghum, "Raptor's Edge," *Aviation Week and Space Technology* 170, no. 6 (9 February 2009): 25.

[4] Wesley Frank Craven and James Lea Cate, eds., *The Army Air Forces in World War II*, vol. 6, *Men and Planes* (1955; new imprint, Washington, DC: Office of Air Force History, 1983), 59.

[5] Quoted in David A. Fulghum, "Raptors Remain on Course for Hawaii," *Aviation Week and Space Technology* 171, no. 5 (3 August 2009): 49.

[6] Tony Osborne, "Fast and Furious: F-35 Buy Will Quicken Evolution of Netherlands Air Force, Says Commander," *Aviation Week and Space Technology* 177, no. 24 (7–20 December 2015): 35.

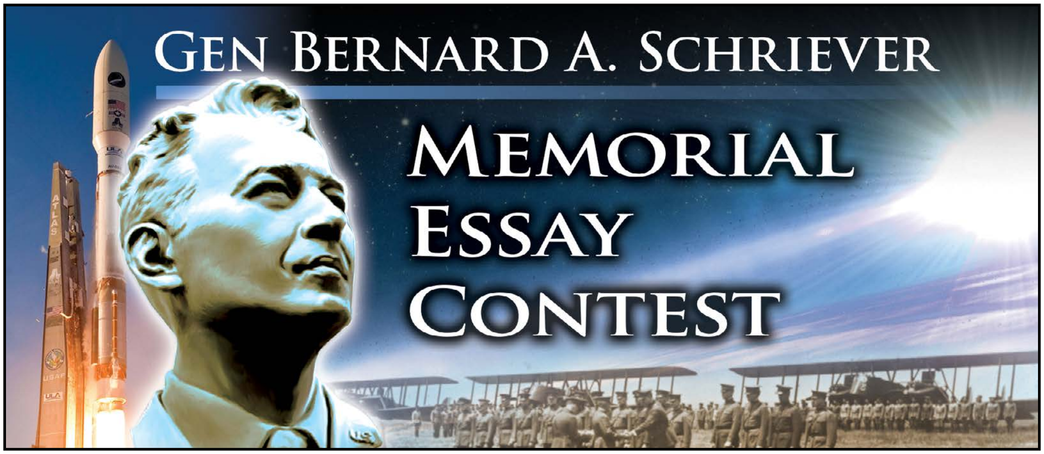
Col John D. Jogerst, USAF, Retired

Colonel Jogerst (USAFA; MS, University of Arkansas) is a C-130/MC-130 master navigator and was a rated personnel analyst at the Air Force Personnel Center. He served as a squadron commander, commandant of the US Air Force Special Operations School, and faculty member at the Air War College as Special Operations Forces Chair to Air University. The colonel commanded deployed theater aviation components for special operations during Operations Provide Comfort, Enduring Freedom, and Iraqi Freedom. Colonel Jogerst is a graduate of Squadron Officer School, Air Command and Staff College, and Air War College.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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



In the name and memory of a great Air Force pioneer, the Lance P. Sijan Chapter of the Air Force Association in partnership with the *Air and Space Power Journal* is pleased to announce the winners of the Gen Bernard A. Schriever Memorial Essay Contest. The purpose of the contest is to stimulate thought, discussion, and debate on matters relating to how the Air Force and Air Force Space Command provide space and cyberspace capabilities for the joint force and the nation.

First Place

Lt Col Mark Reith, USAF

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

Runner-Up

Capt Justin Ryan Thornton, USAF

"The Changing Face of the War Fighter"

Honorable Mention

Col Troy Endicott, USAF

"A Warrior's Mind-Set: Key to Winning in Space"

Maj Brandon Erwin, USAF, and Maj Allen Varghese, USAF

"Next-Generation Warfare Requires a Next-Generation Approach:
Implementing Evolved Operations and Adaptive Acquisitions for a Contested Space Environment"

Capt Joseph Robinson, USAF

"Creating the Space War Fighter: A Rapid Satellite Development Unit Proposal"

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

Recommendations for Integration and Development

Lt Col Mark Reith, USAF*

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

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.

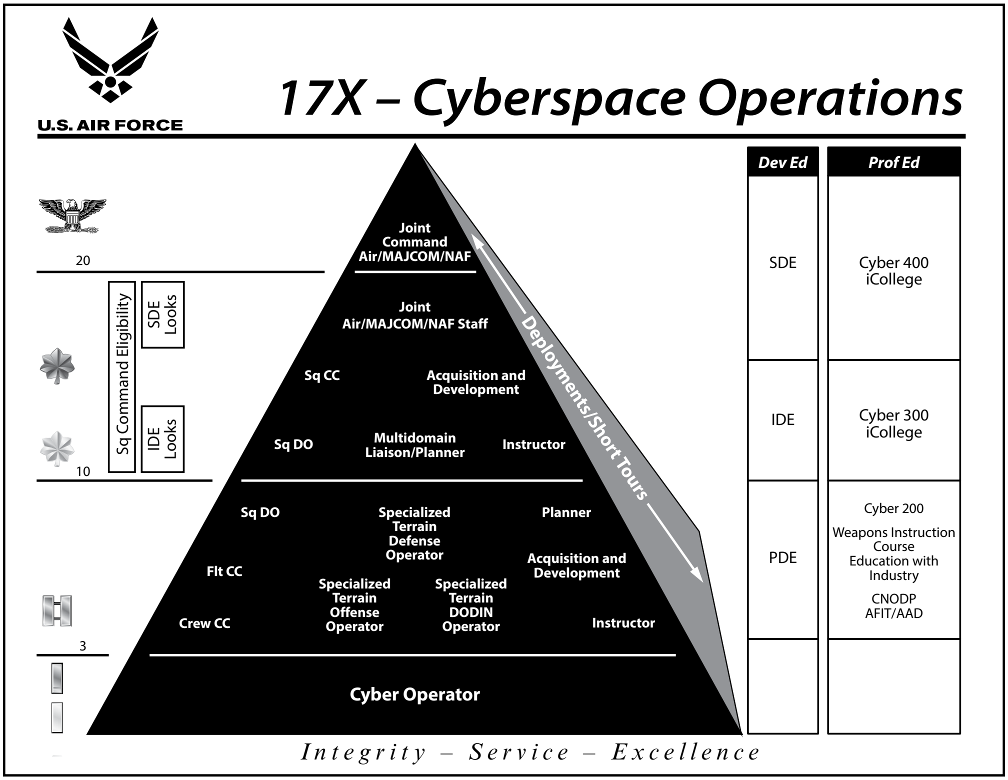
Risk Management

> *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.



U.S. AIR FORCE

17X – Cyberspace Operations

20
10
3
Sq Command Eligibility
SDE Looks
IDE Looks
Joint Command Air/MAJCOM/NAF
Joint Air/MAJCOM/NAF Staff
Sq CC
Acquisition and Development
Sq DO
Multidomain Liaison/Planner
Instructor
Sq DO
Specialized Terrain Defense Operator
Planner
Flt CC
Acquisition and Development
Specialized Terrain Offense Operator
Specialized Terrain DODIN Operator
Crew CC
Instructor
Cyber Operator
Deployments/Short Tours

Dev Ed	Prof Ed
SDE	Cyber 400 iCollege
IDE	Cyber 300 iCollege
PDE	Cyber 200 Weapons Instruction Course Education with Industry CNODP AFIT/AAD

Integrity – Service – Excellence

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

The Changing Face of the War Fighter

Capt Justin Ryan Thornton, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

After the Chinese antisatellite missile test in 2007 and Russia's successful flight test of an antisatellite missile in May 2016, space no longer remains an uncontested mission area for any spacefaring nation.[1] Similarly, the attack on the Pentagon's e-mail server, which affected approximately 4,000 Department of Defense (DOD) employees, shows that cyberspace networks—like space—are also areas of conflict that require special attention.[2] These and many other instances suggest that the Air Force must now consider space and cyberspace as domains of combat and all Airmen operating in those arenas as war fighters. The challenge now lies in adapting the Air Force and its space and cyberspace Airmen to a war-fighter mind-set. By realigning our functional major commands (MAJCOM), divesting regional MAJCOMs, revamping training/deployment constructs, and updating policy and doctrine, we can ensure that the war-fighter mind-set is instilled in our Airmen.

For many years, the United States flew satellites with little concern of possible threats to our control of the mission area. Other countries simply could not afford to operate in space, let alone contend with the United States for control. Because of the decrease in launch and satellite costs, the competition has caught up, nation-states' space capabilities have increased, and US military forces are now feeling the ramifications of competing for space control. Similarly, another highly contested domain—cyberspace—poses a serious threat to Air Force missions. Tools and techniques available on the Internet allow individuals without a formal educational background to easily learn the ways of hacking. These innovations make it simpler and cheaper to stage a war.

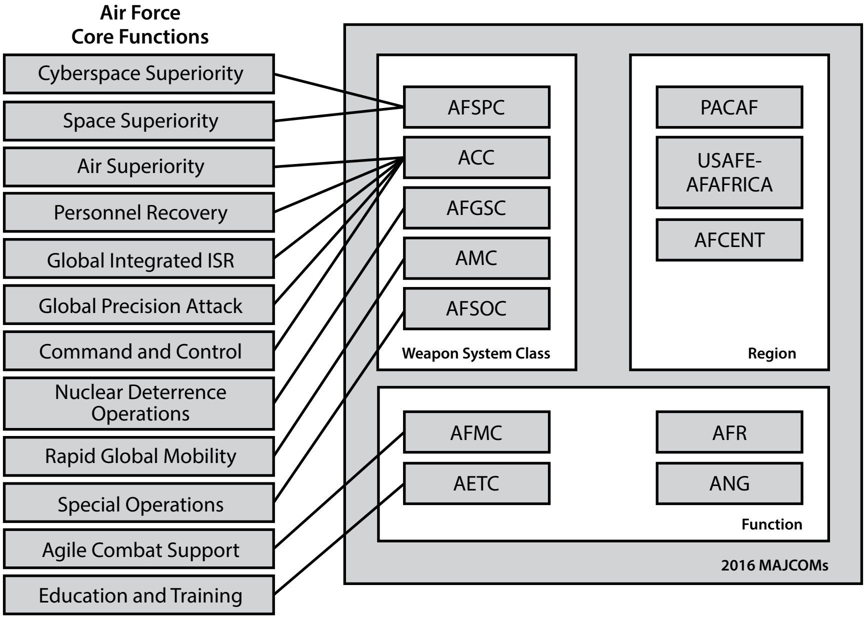
Because of the limited cost of combat in both of these new mission areas, for the foreseeable future, the United States will have to face increasingly capable adversaries bent on circumventing our space capability and exploiting our cyber vulnerabilities. To counter near-peer advances and challenges, the DOD must set out to find "third offset" capabilities to regain the US military advantage lost through the proliferation of technology (developed, stolen, and/or shared). The Air Force must also develop a strategy to meet these problems and threats and to ensure that our Airmen understand that they are competing in a real war zone. By positioning ourselves realistically to confront such issues, the Air Force will continue to sustain the war-fighter mind-set.

To stage our strategy, we look to insights from our commanders. The secretary of the Air Force and chief of staff have provided strategic direction in four documents:

America's Air Force: A Call to the Future; *Air Force Strategic Environment Assessment 2014–2034*; "Global Vigilance, Global Reach, Global Power for America"; and the *Air Force Future Operating Concept: A View of the Air Force in 2035*.[3] Each document outlines a dynamic, ever-changing national security threat environment that requires the Air Force to adapt its five core missions (air and space superiority; global integrated intelligence, surveillance, and reconnaissance [ISR]; rapid global mobility; global strike; and command and control) into a more integrated, agile, technology-driven, and multidomain service. By the year 2035, the Air Force's core missions will have evolved into adaptive domain control, global integrated ISR, rapid global mobility, global precision strike, and multidomain command and control. The change in the Air Force's core missions calls for an examination of the service's current MAJCOM structure to see if it can realistically complete the new missions as presently organized.

Historically, the Air Force MAJCOM structure evolved from conflicts in World War II and the Cold War and were based on weapon-system class, mission areas, and region (fig. 1) to meet the demands of direct military force-on-force. This organization greatly benefited US national security interests and resulted in our successes during the Gulf and Afghan wars. However, given our fielded forces' performance, our enemies will most likely confront us and our allies in more indirect ways (space, cyber, and terrorism) rather than direct military force-on-force. Similarly, unless a major conflict or a significant geopolitical change alters the world order of the last 30 years, Russia, China, North Korea, and Iran are the new threats to our nation's security, with radical Islam continuing to morph from one terrorist group to another. According to *America's Air Force: A Call to the Future*, tomorrow's operational agility demands flexible, integrated multidomain operations; superior decision speed; dynamic command and control; a balanced capability mix; and performance-optimized teams.[4] The question remains as to whether the current structure of the Air Force can attain this operational agility.

To determine whether the Air Force can achieve this vision, one must look at developments of the Space Enterprise Vision (SEV) and possible development of a Cyber Enterprise Vision (CEV); one highlights the capabilities of the Air Force structure while the other all too clearly demonstrates its faults. The SEV required the holistic review of classified and unclassified space system planning. This information was then integrated into a single SEV across platform classes (regardless of organization) to outline where the Air Force should go with space capability development. Such is not the case with the CEV, however. Because the Air Force, DOD, and world at large all interact in cyberspace, the Air Force faces an immense challenge. Any thoughts of structuring a single cyber vision quickly break down because of integration issues arising from the current weapon-system–based organizational structure of the MAJCOMs. Thus, the failure of the Air Force to develop a CEV indicates that it cannot complete the new missions proposed with the current MAJCOM structure.

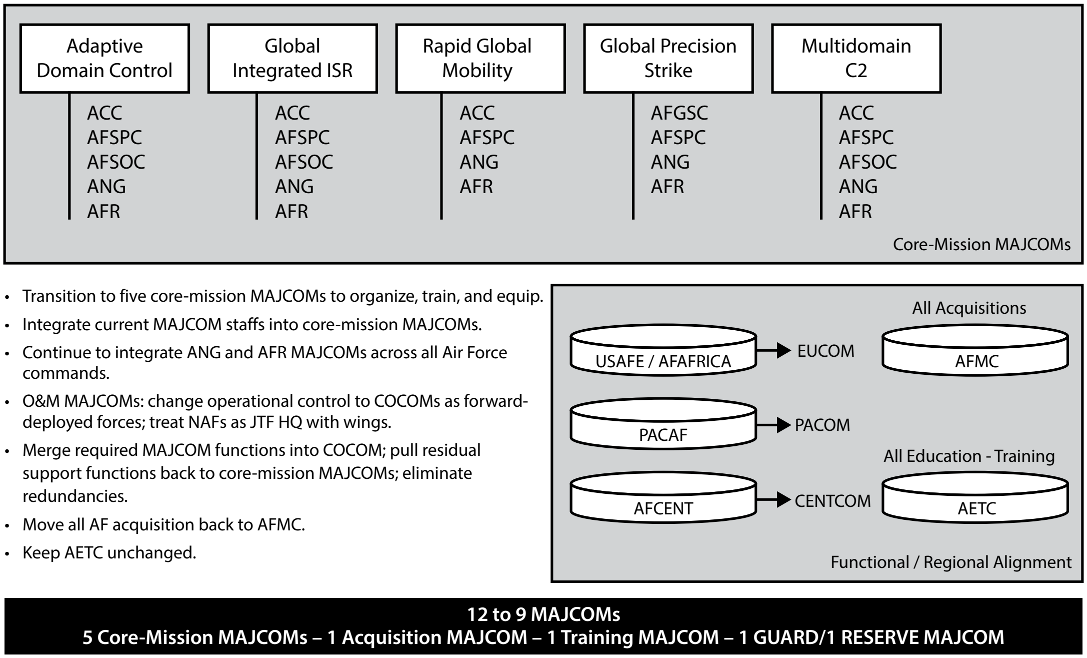


ISR - intelligence, surveillance, and reconnaissance
AFSPC - Air Force Space Command
ACC - Air Combat Command
AFGSC - Air Force Global Strike Command
AMC - Air Mobility Command
AFSOC - Air Force Special Operations Command
PACAF - Pacific Air Forces
USAFE / AFAFRICA - United States Air Forces in Europe / US Air Forces Africa
AFCENT - US Air Forces Central Command
AFMC - Air Force Materiel Command
AETC - Air Education and Training Command
AFR - Air Force Reserve
ANG - Air National Guard

Figure 1. 2016 Air Force MAJCOM organizational structure with core functions

To fulfill the missions proposed in the *Air Force Future Operating Concept*, the service must reorganize and realign the current MAJCOM structure to synchronize the five core missions across capabilities, staffs, and expertise. Doing so will make the idea of war and its application real to our Airmen. To realize a 2035 end state, the Air Force must go beyond the current MAJCOM structure by asking whether it is organized to attain its 2035 vision. Imagine an adaptive-domain-control MAJCOM that develops capability across air, space, and cyber whereby doctrine is written as an integrated solution, requirements are defined across multiple-domain platform classes, and budgets are advocated as an integrated solution across multiple-domain systems on behalf of a core mission. To meet the Air Force's 2035 vision, address the MAJCOM organizational problems, and ingrain the war-fighter spirit into our troops, this article proposes a core-mission MAJCOM realignment.

By 2035 the service will need to consolidate and realign the current MAJCOM organizational structure from 12 to 9 MAJCOMs if it wishes to fully realize the secretary and chief's vision and allow for better integration of war-fighter capabilities. This concept proposes five core-mission MAJCOMs, one acquisition MAJCOM, and retention of the Air Education and Training Command, Air National Guard, and Air Force Reserve MAJCOMs in their current forms (fig. 2).



- Transition to five core-mission MAJCOMs to organize, train, and equip.
- Integrate current MAJCOM staffs into core-mission MAJCOMs.
- Continue to integrate ANG and AFR MAJCOMs across all Air Force commands.
- O&M MAJCOMs: change operational control to COCOMs as forward-deployed forces; treat NAFs as JTF HQ with wings.
- Merge required MAJCOM functions into COCOM; pull residual support functions back to core-mission MAJCOMs; eliminate redundancies.
- Move all AF acquisition back to AFMC.
- Keep AETC unchanged.

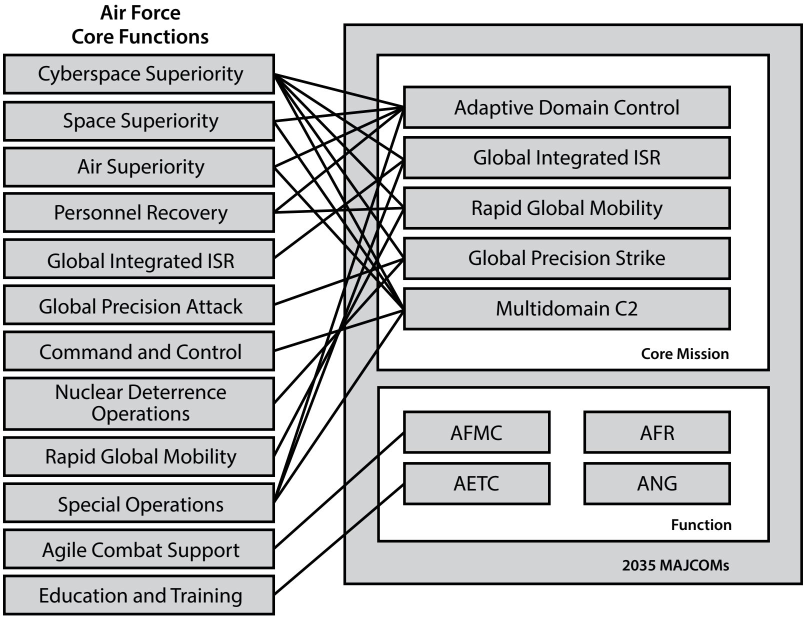
12 to 9 MAJCOMs
5 Core-Mission MAJCOMs – 1 Acquisition MAJCOM – 1 Training MAJCOM – 1 GUARD/1 RESERVE MAJCOM

ACC - Air Combat Command
AFSPC - Air Force Space Command
AFSOC - Air Force Special Operations Command
ANG - Air National Guard
AFR - Air Force Reserve

ISR - intelligence, surveillance, and reconnaissance
AFGSC - Air Force Global Strike Command
C2 - command and control
O&M - operation and maintenance
COCOM - combatant command
NAF - numbered air force
JTF - joint task force
HQ - headquarters
AFMC - Air Force Materiel Command
AETC - Air Education and Training Command
USAFE / AFAFRICA - United States Air Forces in Europe / US Air Forces Africa
PACAF - Pacific Air Forces
AFCENT - US Air Forces Central Command
EUCOM - US European Command
PACOM - US Pacific Command
CENTCOM - US Central Command

Figure 2. 2035 Air Force MAJCOM realignment concept

To transition regional/mission-area-class MAJCOMs to core-mission MAJCOMs, the Air Force should integrate the commands' staffs into appropriate core-mission MAJCOM staffs. Three of the five core-mission MAJCOMs (Adaptive Domain Control, Global Integrated ISR, and Multidomain Command and Control) would integrate staff elements of Air Combat Command, Air Force Space Command, and Air Force Special Operations Command. The Adaptive Domain Control Command would integrate across air, space, and cyberspace "to achieve varying levels of domain superiority over adversaries seeking to exploit all means to disrupt friendly operations."[5] The Global Integrated ISR Command would develop doctrine and plans to enable "leaders to make informed decisions at a *superior decision speed* to help ensure freedom of action, maintain deterrence, contain crises, and achieve operational success" (emphasis in original).[6] The Multidomain Command and Control Command would focus on organizing, training, and equipping "forces to ensure the ability to conduct effective multi-domain operations."[7] For the remaining two core-mission MAJCOMs, Air Mobility Command and Air Force Global Strike Command would become Rapid Global Mobility Command and Global Precision Strike Command, respectively, while integrating staff elements from Air Force Space Command. Rapid Global Mobility Command would employ "a *balanced capabilities mix* of manned, remotely operated, and autonomous assets to support operations in both contested and uncontested environments" (emphasis in original).[8] Space launch would consolidate under this command. The fifth core-mission MAJCOM, Global Precision Strike Command, would "maximize *operational agility* against advanced adversaries" by integrating "*multi-domain* global precision strike [capability] using a *balanced capabilities mix* of forces in collaboration with joint and multinational partners" (emphasis in original).[9] Any future space-on-space strike capability falls under the umbrella of Global Precision Strike Command. Figure 3 displays a possible realignment of core functions to this proposed core-mission MAJCOM realignment; however, if the Air Force pursued this type of construct, further core-function-alignment analysis would be necessary.



ISR - intelligence, surveillance, and reconnaissance
C2 - command and control
AFMC - Air Force Materiel Command
AETC - Air Education and Training Command
AFR - Air Force Reserve
ANG - Air National Guard

Figure 3. 2035 Air Force MAJCOM organizational structure with core functions

As for acquiring integrated systems and capabilities, all Air Force acquisition should fall under Air Force Materiel Command to better "align with partners to develop interoperable, adaptive domain control capabilities through aviation, space, and cyberspace enterprise development, advocacy, training, and combined acquisition programs."[10] In addition to consolidating acquisition, prudent organizational alignment of multidomain acquisition within Air Force Materiel Command would drive integrated acquisition for core-mission solutions and capabilities.

Regarding the Air National Guard, Air Education and Training Command, and Air Force Reserve, they would continue to perform their current missions to educate, train, and integrate across all Air Force commands. If the service were to pursue this MAJCOM realignment, then further analysis and work would be necessary to properly align US-based numbered air forces and wings across the five core-mission

MAJCOMs. However, physically relocating numbered air forces and wings would be unnecessary.

The further we align our mission to the MAJCOMs and make our defense strategy a practical reality for our Airmen, the more we ingrain the war-fighter spirit and combat readiness into our troops. With the new MAJCOM structure, integration and technology will drive the Air Force's ability to fight and win our nation's wars and low-intensity conflicts. Integration of weapon systems and people will establish a culture of "my mission" rather than "my weapon system," helping ensure propagation of the war-fighter mind-set. Integrated capabilities (air, space, and cyber) to support core missions will develop from inception instead of piecemeal among weapon-system-class MAJCOMs (the current MAJCOM structure). Flexibility is necessary here because air, space, and cyberspace technologies advance at disproportionate paces. Air and space have much longer development cycles and fewer companies developing technologies than does the cyberspace industry. Within the information technology industry, commercial technology advances at a much faster pace than can ultimately be delivered by any defense contractor developing cyber solutions, oftentimes rendering weapon systems unintentionally obsolete on delivery. There are simply myriad cyber companies developing new technologies and techniques not even dreamed of when the DOD and Air Force established requirements and/or released a contract for a specific capability or weapon system procurement.

Besides aligning to core-mission MAJCOMs, the *Air Force Future Operating Concept* asks how Air Force forces will evolve and conduct the core missions to help overcome national security challenges in the future. To further establish our war-fighter mentality, we should propose divesting regional MAJCOM headquarters (United States Air Forces in Europe, US Air Forces Africa, Pacific Air Forces, and US Air Forces Central Command) and transferring the staffing for all regional air forces (numbered air forces and wings) to their respective combatant commands (COCOM)—US European Command, US Pacific Command, and US Central Command—as forward-deployed forces, using our most recent conflicts in Iraq and Afghanistan as organizational examples or starting points. Since United States Air Forces in Europe / US Air Forces Africa, Pacific Air Forces, and US Air Forces Central Command are predominantly operation-and-maintenance commands that do not acquire major weapon systems or develop capabilities, the regional MAJCOM headquarters should merge necessary staff into the regional COCOM headquarters to support the additional force structure responsibilities. This idea does not propose to realign the COCOM organizational structure, and any residual regional MAJCOM staff would come back to the core-mission MAJCOM headquarters.

Needless to say, a structural overhaul like the one suggested above will entail extensive training, which provides further opportunity to instill the war-fighter spirit throughout the force. The Air Force needs to begin training its space war fighters on how to fight in the space domain using war gaming as well as other modeling and simulation efforts that fit into the confines of current space policy and space treaties. The service's space and cyber squadrons should begin forward-deploying as units with other war fighters rather than deploying one or two Airmen at a time. Doing so will enable the entire squadron of space and cyber war fighters to see and feel the effects of their mission as they are conducted. Too often, the Air

Force's space and cyber operators deploy while the rest of their unit remains back at home station, unaware of the conflicts that their fellow Airmen are experiencing. We need extensive training and motivation modules to bridge this gap between our Airmen and to help units understand that the days of supporting space and cyber from the safety of a desk are gone. We are now all war fighters.

Finally, to further instill our war-fighting spirit across the Air Force, the long-term effort requires changes to national space policy and space doctrine, both of which have dictated for years that the United States employ no weapons in space. These policies need to change to allow both offensive and defensive operations there. We must look to the capabilities and possible strategies of our competitors for the space and cyber domains and plan our defense strategy accordingly. Offensively, space weapons should be allowed in space to conduct missions in a contested environment. Their presence will permit the United States to hold aggressors at substantial risk with offensive space weapons, and we as a country can deter an aggressor from damaging or destroying our critical mission satellites.

As we have learned and witnessed over the Air Force's history, the service has always innovated leveraged technologies and been willing to adapt the MAJCOM organizational structure to meet the ever-changing national security environment. By altering our organizational structure to meet the current threat in a real and viable way, we not only encourage but also ingrain the war-fighting spirit into the everyday lives of our Airmen. By aligning our MAJCOMs to best meet the current threats, by establishing intensive training of our troops to bridge the gap between experienced fighter and home-front hero, and by signaling our stance to the world through our national policy and doctrine, the Air Force will instill the right war-fighter mind-set to face the current war. ✪

Notes

[1] Edward Cody, "China Confirms Firing Missile to Destroy Satellite," *Washington Post*, 24 January 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/23/AR2007012300114.html; and Bill Gertz, "Russia Flight Tests Anti-satellite Missile," *Washington Free Beacon*, 27 May 2016, http://freebeacon.com/national-security/russia-flight-tests-anti-satellite-missile/.

[2] Tom Vanden Brook and Michael Winter, "Hackers Penetrated Pentagon Email," *USA Today*, 7 August 2015, http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/.

[3] Headquarters US Air Force, *America's Air Force: A Call to the Future* (Washington, DC: Headquarters US Air Force, July 2014), http://airman.dodlive.mil/files/2014/07/AF_30_Year_Strategy_2.pdf; Headquarters US Air Force, *Air Force Strategic Environment Assessment 2014–2034* (Washington, DC: Headquarters US Air Force, 2014); Gen Mark A. Welsh III, "Global Vigilance, Global Reach, Global Power for America," *Air and Space Power Journal* 28, no. 2 (March–April 2014): 4–10, http://www.airpower.maxwell.af.mil/digital/pdf/articles/2014-Mar-Apr/SLP-Welsh.pdf; and Headquarters US Air Force, *Air Force Future Operating Concept: A View of the Air Force in 2035* (Washington, DC: Headquarters US Air Force, September 2015), http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf.

[4] Headquarters US Air Force, *America's Air Force*, 9; and Headquarters US Air Force, *Air Force Future Operating Concept*, 47.

[5] Headquarters US Air Force, *Air Force Future Operating Concept*, 18.

[6] Ibid., 23.

[7] Ibid., 14.
[8] Ibid., 21.
[9] Ibid., 29, 30.
[10] Ibid., 21.

Capt Justin Ryan Thornton, USAF

Captain Thornton (BS, University of Wyoming; MS, University of Technology and Project Management) is the deputy branch chief, Special Programs, Program Objective Memorandum, Headquarters Air Force Space Command, Peterson AFB, Colorado. Prior to his current assignment, he served as the special programs planner for Headquarters Air Force Space Command.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

Inside China's Grand Strategy: The Perspective from the People's Republic by Ye Zicheng (edited and translated by Steven I. Levine and Guoli Liu). University Press of Kentucky (http://www.kentuckypress.com), 663 South Limestone Street, Lexington, Kentucky 40508-4008, 2010, 314 pages, $35.00 (hardcover), ISBN 978-0-8131-2645-6.

Inside China's Grand Strategy is a rewarding read although much of this gratification does not come easily due to the difference between a Western reader's and the author's perspective. This work of nonfiction was written for a Chinese audience to lay out a pragmatic way ahead for the Chinese state as it navigates its economic and geopolitical rise. The study focuses on several of China's internal challenges; the key strategic decisions it must make; and vital external relationships with the United States, other rising powers like Russia, and China's geographic neighbors. Now expertly translated to allow the author's worldview to shine through, it offers readers keen perception into how the world looks from Beijing. To appreciate this worldview, Western readers—particularly those from the United States—may initially squirm, but perseverance will yield valuable insights.

A smaller struggle stems from idiosyncrasies in Ye's writing. Often, especially early on, Ye relies on lists of figures to argue his points without providing the greater context necessary to make the argument truly stick. Additionally, this book was first published over a decade ago, and although some figures were updated for the translation in 2008, significant changes have occurred in China in the intervening eight years. In most cases, the absence of updated data is not a problem because Ye's arguments are strategic enough to remain insightful, often foreshadowing what has since occurred or highlighting decisions still in the making. In a few cases, however, China has already made choices that deviate from Ye's proposed path forward. He offers a good basis for understanding China, but Ye's is not the faultless voice of either the people or the party; nor is it a sparse voice—each of the book's six chapters averages well over 40 breathless pages.

A lead professor of international studies at Peking University, Ye can be considered a moderate or even progressive member of China's academia. Throughout his book, he usefully outlines and then deconstructs hard-line Chinese preconceptions of China's current role in world affairs. In turn Ye advocates that China prioritize the economy over the military, begin empowering democracy, become more transparent in governance, and boldly face domestic challenges. He sees war between the United States and China as both catastrophic and unlikely, advocates friendly relations with neighbors, and concludes that the resolution of reunification with Taiwan requires ample prosperity, peace, and patience. Still, for Western readers, many fundamental elements of his arguments and conclusions will cause discomfort.

Ye questions readers' assumptions regarding the United States' geopolitical role and intentions by appearing to advocate the subordination of free speech to stability, the necessity of China's becoming a world power and reclaiming Taiwan, a path to democracy that allows room for the postponement of individual liberty, and China's not only seizing opportunity but also creating it. These and other views hang in the background of the entire work, coloring what are often pragmatic conclusions with biases and assumptions that are at times frustrating, arrogant, unsupported, and frightening from a Western perspective. However, opposing these notions may prove futile since the elements of disagreement are often founded in the reader's point of view rather than in facts. Indeed, these apparent and at times infuriating qualities of the book will likely act as a mirror for the reader's own biases. As someone from the outside looking in, I could not help thinking that the historic biases of American exceptionalism and virtue must invite similar skepticism and concern abroad.

Inside China's Grand Strategy is a worthy read for those who seek a better understanding of China's actions and motivations in the coming years from the perspective of an insider, as well as for those willing to have their own views forged and tempered by the challenging ideas of a moderate Chinese academic.

Capt Stefan G. DePaul, USAF
Defense Intelligence Agency, Washington, DC

An Untaken Road: Strategy, Technology, and the Hidden History of America's Mobile ICBMs by Steven A. Pomeroy. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402, 2016, 304 pages, $44.95 (hardcover), ISBN 978-1-61251-973-9.

The emerging field of Cold War history receives a new addition with *An Untaken Road*, an account of mobile intercontinental ballistic missiles (ICBM) in America. Steve Pomeroy, a history professor and former missileer himself, delves into one of the least known areas of America's nuclear weapons history as he explores the Air Force's efforts to mobilize its ICBMs.

Pomeroy uses established historical theory of technological development to enlighten the reader as to how mobile ICBMs came about—and ultimately failed—in the context of the Cold War. Employing a modified version of historian Thomas Hughes's five-phase model of technological innovation, he shows how each succeeding mobile missile program ultimately did not garner the momentum required to become operational. Putting his subject in the context of the evolving politics of the time, Pomeroy makes a convincing case for why there are no trains with ICBMs currently traveling the railroads of the West.

An Untaken Road follows the early development and limitations of ICBMs—limitations that made static basing difficult (never mind the idea of moving them around). From here the divergence is well documented regarding how static ICBMs became the weapon of choice, and various mobile options showed great promise but never achieved stability as programs. The author effectively uses his formal training as a historian to explain the shortcomings of rail-mobile, large-plane, superhard-shelter, and pool basing (even an underground tube-tunnel basing concept); he also documents why these approaches found sufficient favor to justify research but never enough to be deployed. Each proposal reached one of the stages of development but failed to proceed to the all-important final stage of stability—a status that would grant it funding and operational implementation.

The book facilitates a strong understanding of how military procurement works and thus influences today's multi-billion-dollar projects. The paradigm that Pomeroy generates is one of coalescing crucial factors at the right time to breathe life into a program. Many of the systems he describes were prototyped and tested but always lacked a key element to make them viable. So often political support was present, but the technology was not—or the technology was mature, but the driving Air Force leadership necessary to deploy a system failed to emerge. The text makes a strong argument that if a system of systems is to work, an entirely separate military-industrial-political system must be functioning efficiently.

Although written as a history, this study offers a lesson to current procurement teams. Its underlying theme is stability, and thus it rightly shines a bright light on Gen Bernard Schriever, the man responsible for the ICBM force. His systems approach to problems and dual focus on disruptive and sustaining innovations set the standard—one that slowly relaxed after his retirement. By contrasting the successful development and deployment of three ground-based ICBM systems with the repeated failures of mobile systems, *An Untaken Road* puts a stark spotlight on the degrading quality of systems engineering in military procurements. Without question, this is a book for any member of a program office.

By learning from our history, so well documented by Professor Pomeroy, we as a nation and military-industrial complex can make better decisions. The procurements he describes were often larger than those for the fighter jets, satellites, and ships we purchase today, and they suffered from the same shifting political tides and needs of the Department of Defense—so the lessons remain pertinent. We would do well to apply the book's paradigm of technological development and determine whether the big-ticket items we are buying today are still worth the cost. Too many times, historians admonish leaders for not learning the lessons of history and for repeating failures, but in this case the accusations are true. We can act on these lessons and apply them to things we do every day.

To make these arguments, the book uses open-source documentation on the political and public debates, as well as a wealth of newly declassified data, clearly showing why each proposal failed to gain the needed momentum. Pomeroy provides copious notes although most of the technical details of these wondrous projects are from primary sources available only in archives.

Regrettably, the text contains only a fraction of the presentation slides and available pictures of the considered options for mobile basing. One of the areas for future research could involve more indulgence in the technological aspects and a more detailed description of the massive ICBM carriers that never materialized. Some of the planes and tunnel-based ideas that Pomeroy describes deserve their own treatments, just to illustrate how bold and complex were the concepts that the Air Force seriously considered.

An Untaken Road establishes a solid foundation for the study of the service's truncated ICBM efforts, a subject that deserves more recognition than it receives because of its failings. The proposals and programs described all came to nothing because of inherent issues with their ability to advance through the developmental phases needed to sustain a program. Today's procurements are no different in terms of their cost and national security implications, making the book's lessons learned critical to the decision making of any officer tasked with procuring a new system.

Daniel Schwabe
Whittier, California

Emblems of Exploration: Logos of the NACA and NASA by Joseph R. Chambers and Mark A. Chambers. National Aeronautics and Space Administration (https://history.nasa.gov/what.html), NASA History Program Office, 300 E Street SW, Washington, DC 20546, 2015, 149 pages. Free (softcover or e-book), ISBN 978-1-62683-028-8. Available online at http://history.nasa.gov/monograph56.pdf.

Emblems of Exploration: *Logos of the NACA and NASA* is a monograph that describes the history of the emblems used by the nation's air and space exploration agencies. The father and son coauthors have over 73 years of combined experience as technical and historical researchers and writers for the National Aeronautics and Space Administration (NASA), the senior Chambers (Joseph) having earned NASA's Exceptional Service Medal. The book represents a 20-year project of collaboration between the two, their extensive research having determined the roots and rationale behind some of the most famous government logos in history.

Although *Emblems of Exploration* is an examination of organizational logos, it provides fascinating insight into the bureaucratic thought behind the organizational history of American civilian air and space exploration. Beginning with the establishment of the National Advisory Committee for Aeronautics (NACA), the story runs through the establishment of NASA and the origins of its famous "meatball," "swoosh," and "worm" logos. Even though much of this information is deeply esoteric and of most interest to hardcore space history fans, the story of the NACA and NASA emblems is deeply intertwined with the history of aviation, the space race, and the organizational challenges of a storied agency after its greatest triumphs.

The first half of the study describes logos of the NACA, which coordinated American aeronautical research from 1915 to 1958, and directed such famous projects as the first supersonic flight. Interestingly, in the context of this book, the NACA had no standardized logo for its first 25 years of existence, gaining a winged emblem only on the eve of World War II. Aside from historical information on the NACA and its emblems, this section is intriguing for its extensive photography, including excellent pictures of early experimental aircraft in NACA livery; fascinating views of early Langley Field, Virginia; and images of artifacts like Eddie Rickenbacker's NACA security badge.

With the beginning of the space race, the NACA grew into NASA, which required a new organizational look and culture to go with a new domain of exploration. The coauthors describe the competition to design NASA's logo and show images of the unselected design finalists. They also account for the origins of each element of the "meatball" emblem in a perceptive, human way by relating the stories of contributors who felt slighted by the official history. This section includes early medals given to pioneers like Alan Shepard and reveals the public's harsh critical response to the early NASA emblem.

The "meatball" design flew on all of NASA's early manned missions, including Mercury, Gemini, and Apollo, identifying an organization and its historic achievements. However, in 1974, under the Federal Graphics Improvement Program, NASA's organizational emblem underwent a redesign and simplification by the same graphic design studio that created the 1976 bicentennial logo. The new logo, a highly stylized red linotype of "NASA" that went so far as to eliminate the crossbars of the "As" became known, somewhat derisively, as the "worm." This design flew on all NASA aircraft and space missions from 1975 until 1992, including the groundbreaking X-29 forward-swept-wing airplane and the *Challenger* space shuttle. This portion of *Emblems of Exploration* boasts excellent color photographs from a fascinating era in aeronautics and the early days of the space shuttle program.

By the early 1990s, NASA was suffering from organizational malaise, and the new administrator saw the return of the "meatball" emblem as a means of signifying continuity with triumphs of the past. In the final part of the book, the authors discuss the return of the original logo, development of the simplified "swoosh" emblem in the 1990s, and uses of the NASA logos on applications from stationery to automotive license plates from 1992 to the present.

Emblems of Exploration: Logos of the NACA and NASA is an authoritative deep dive into an esoteric topic in aviation. It enhances the reader's understanding of the importance of emblems to the organizational identity of two trailblazing agencies, but the authors never ascribe mission success or failure to a logo. Rather, this is history for its own sake, without agenda or broad thesis. The monograph, with its excellent collection of photographs, should be a terrific reference for historians of early aviation and of the culture of NASA. More casual fans should enjoy this book for its extremely detailed, behind-the-scenes look at an always visible but often-overlooked aspect of American air and space history.

Maj Andrew L. Brown, USAF
Maxwell AFB, Alabama

No One Avoided Danger: NAS Kaneohe Bay and the Japanese Attack of 7 December 1941 by J. Michael Wenger, Robert J. Cressman, and John F. Di Virgilio. Naval Institute Press (http://www.usni.org/navalinstitutepress), 291 Wood Road, Annapolis, Maryland 21402-5034, 2015, 208 pages, $34.95 (hardcover), ISBN 978-1-61251-924-1.

Fascinated by the events before, during, and after World War II, I anxiously awaited the arrival of *No One Avoided Danger: NAS Kaneohe Bay and the Japanese Attack of 7 December 1941*. From an academic perspective, I felt a bond with authors J. Michael Wenger, Robert J. Cressman, and John F. Di Virgilio's introductory game plan and closing material. They explain how their book would fill a significant, historic gap in the literature by highlighting the efforts of those who faced danger and overwhelming odds, as did the warriors at Pearl Harbor. The authors annotate the extent of their scholarship by acknowledging an extensive network of resources, including in-depth interviews. Exploring their inclusion of extensive footnotes and an impressive bibliography, I felt that they covered the bread slices with hints of meat, condiments, and other edibles needed for an exciting journey.

Cliff-diving into chapter 1, I pondered whether Wenger, Cressman, and Di Virgilio had gleaned their presentation from the opening scene of the movie *Saving Private Ryan*. My bewilderment increased through rereads of the first three chapters. The overwhelming barrage of personal information, families, locations, logistics, aircraft descriptions, unit designations, aircraft movements, medical status, military jargon, acronyms, and a plethora of other details reminded me of the nausea those Soldiers felt on Omaha Beach. Like some of those warriors, I wondered if I would make it off the beach.

Exacerbating the stimulus overload, the approach used by Wenger, Cressman, and Di Virgilio to discuss individual behavior and aircraft movements often mirrored another film—*Pulp Fiction*. Whether describing the NAS Kaneohe buildup prior to 7 December or the attack in chapters 2 and 3, they narrate the actions of one or more individuals at one location and move their story forward. They would then set the clock back when mentioning a new individual or group and advance their timeline. Instead of providing a fluid chronology, the authors place the burden on readers to create a timeline for both the American and Japanese forces. If readers make it to chapter 4, the account of the attack's aftermath, they will be welcomed by a smooth chronology and storyline before the narrative suddenly stops. Perhaps this style reflects the authors' intent to pique their readers' curiosity and entice them to explore future books in the series.

Stylistically, an audience that appreciates an overabundance of military jargon and acronyms; tactical-level military logistics, aircraft, and weaponry detail; and nonlinear timelines will enjoy this book. Readers who prefer character development, smooth story flow, and prose that does not sound like a technical manual could find it difficult to read and choose something else. The presentation makes me wonder if the depth of research unknowingly influenced the authors to cram as much detail as possible into a relatively short book—the first in a series. Take, for example, the following passage:

> The new arrivals reported just in time to participate in the station's commissioning ceremony, which commenced at 1500 on 15 February 1941, at which time the station's ten officers and 118 enlisted men mustered at the base of the flagpole in front of the Administration Building, forming a hollow square with Cdr. Martin and the officers facing north, the Marine Detachment west, the Navy enlisted men east, and the Navy band south (pp. 5–6).

In this passage and several other sentences, Wenger, Cressman, and Di Virgilio could have elaborated on several concepts. The approach would have enlightened readers to the authors' purpose, including cursory details instead of keeping the audience guessing.

As Paul Harvey was wont to say, here's "the rest of the story." Stylistic difficulties notwithstanding, the level of detail here is impressive. The authors' collective passion to convey what those individuals felt and thought on a "day that will live in infamy" leaves readers with both a chill and an invigorating sense of pride. Caught off guard and believing the Japanese aircraft were Army Air Corps planes conducting an exercise, the NAS personnel could have allowed communication difficulties to result in complete destruction. Instead, their collective warrior ethos inspired them to defend NAS Kaneohe despite serious injuries, and their team effort allowed them to develop work-arounds to fire and rearm available weapons, establishing a legacy for our Department of Defense. The tactical problems likely influenced present-day early warning systems, satellite tracking, and multiple communication channels to verify incident reports, as well as other programs to protect personnel and property.

The book's elaborate photo display is captivating. Looking into the eyes of both the Americans and Japanese serves as a stark reminder of the need for tactical-level details to enhance a story, reinforcing my belief that a nation's most versatile and game-changing weapon is its people. Before-and-after photos of property destruction—obviously not recorded by drones or sophisticated zoom-lens cameras—struck a chord because they were taken decades before the advent of cell phones and almost instantaneous media. The people at NAS Kaneohe knew the importance of the event and preserved history that we and our successors will never forget.

I applaud the authors for conducting their extensive research and for sharing this piece of history. Documenting experiences through interview transcripts and preserving memories remind us to honor our World War II veterans. Because of their efforts and sacrifice, many others have the privilege to serve our nation either in uniform or as civilian employees. I am not certain that I will read another book in this series. However, I may do so because surviving the struggle with this one resulted in enlightenment and greater pride in the legacy of our armed forces.

Dr. Katherine Strus, Lieutenant Colonel, USAF, Retired
San Antonio, Texas

Go, Flight! The Unsung Heroes of Mission Control, 1965–1992 by Rick Houston and Milt Heflin. University of Nebraska Press (https://www.nebraskapress.unl.edu), 1111 Lincoln Mall, Lincoln, Nebraska 68588-0630, 2015, 368 pages, $36.95 (hardcover), ISBN 978-0-8032-6937-8.

A mission to the moon is conducted by astronauts—some in zero gravity and some in a one-g control room located southeast of Houston, Texas. Although history best remembers those who escaped Earth's gravity, the primary focus of *Go, Flight!* is the mission controllers' actions, stories, and impact on our nation's space program. Mr. Houston's journalism background rings through the celestial narratives re-created in the pages of this history book that spans the National Aeronautics and Space Administration's (NASA) projects from Gemini to the space shuttle. Credit for the incredibly accurate technical detail goes to Mr. Heflin, who, as a former NASA flight director, lived through most of the covered events firsthand. Through first-person recollections and interviews with the former mission controllers, the authors have developed a masterful narrative history of American manned spaceflight.

Houston and Heflin begin their tale at the creation of the Manned Space Center, the penultimate name of what is today known as the Johnson Space Center in Houston, Texas. Readers learn that NASA did not attract top-tier talent from universities like MIT and Stanford in favor of "not quite as brilliant . . . team players" from bigger state schools (p. 49). In spite of that limitation, legends like flight director Gene Kranz and electrical engineer John Aaron were born after successes like the lunar landing and *Apollo 13*'s safe recovery. The authors cover the eclectic mix of controllers after explaining what the many stations in the Mission Operations Control Room (MOCR) were designed for. Several operators are developed more fully than others, giving the book a movie-like quality of having stars and supporting actors. Where interviews were insufficient, quotations from books by a controller-turned-author, data from voice recordings, and photos of genuine NASA checklists offer a more real-life, behind-the-scenes perspective than an amateur science reader could have hoped for. The concentration on the astronauts in the MOCR sometimes leaves the reader wondering what was happening in the spacecraft—similar to how the controllers must have felt. This writing style makes the book quite suspenseful during dramatic retellings of the momentous spaceflights.

Go, Flight! supplies more perspective in the pages covering historical flights—such as Ed White's Gemini spacewalk, the ill-fated *Apollo 1*, Neil Armstrong's *Apollo 11*, and the nationally unifying *Apollo 13*—than those on less salient stellar sojourns. This practice is especially true with the treatment of the shuttle program, which, aside from the 1986 *Challenger* tragedy, seems almost an afterthought during the fewer than 50 pages dedicated to the post-Apollo era. The book easily could have ended up twice as long had chapters been divided more equitably, so perhaps this was by design since the pace of the book seems to mirror the American people's interest in manned spaceflight: national pride ebbed and flowed with the heroism that certain NASA missions demonstrated. A reader hoping for an all-inclusive anthology of data from the missions in between will be disappointed, but one searching for a new view of history's famous spaceflights will be handsomely rewarded.

Someone who picks up *Go, Flight!* having never followed NASA missions is likely to struggle to grasp the magnitude of some background details spilled in this extensively researched text. Although it reads conversationally, the depth of information assumes that the reader has a baseline knowledge of American space exploration. That technique does not detract from the book, but it tailors the audience to more scientifically educated readers. Perhaps the best quality of *Go, Flight!* is that it offers no political or prophetic message, just an entertaining retelling of history. Messrs. Houston and Heflin accomplish exactly what they set out to do: provide background stories of MOCR operators during NASA's heyday. Anyone who fits that description or wonders exactly how Gene Kranz came up with his "failure is not an option" line from the film *Apollo 13* should dive into this highly educating summary of spaceflight.

Capt James Maday, USAF
Davis-Monthan AFB, Arizona

Developing National Power in Space: A Theoretical Model by Brent Ziarnick. McFarland (http://www.mcfarlandpub.com), Box 611, Jefferson, North Carolina 28640, 2015, 268 pages, $45.00 (softcover), ISBN 978-0-7864-9499-6.

As we move further into the twenty-first century, space continues to play an increasingly significant role in the world. Among its myriad applications, space is instrumental to global communications, transportation, weather prediction, business, and military operations. For the past 60 years, the United States has enjoyed its position as the world's preeminent space power, sending men to the moon, launching satellites to the farthest depths of the solar system, and dominating the modern battlefield with space technology. However, other nations such as China are rapidly expanding their national space power, and the United States, while still strong, is losing ground.

In *Developing National Power in Space: A Theoretical Model*, author Brent Ziarnick, an instructor at the US Air Force's Space Education and Training Center in Colorado Springs, Colorado, and an award-winning writer on military space issues, intricately details a military-type strategic theory for a nation's space program. He does so by analyzing the significant characteristics of national space programs and examining how nations can maximize their political, economic, and military advantages gained from space operations. Through his strong grasp of military and economic theory, Ziarnick lays out a General Theory of Space Power, which he asserts can guide the United States in developing its national space power and maintaining its leading position in the world.

Ziarnick's General Theory of Space Power is impressive in both its scope and predictive ability. Indeed, his unique theory is comprehensive across all forms of space activity, including commercial, civil, political, and military. The universality of the theory means that any space professional or enthusiast who reads this book will gain a better understanding and appreciation of the interconnectedness of these diverse areas. For example, space enthusiasts who typically focus on space-related current events or science fiction will learn about classic military and economic theories as applied to space, as well as strategic lessons for space power development derived from military history. Military professionals will be exposed to the presently unfamiliar territory of interstellar flight and a future Deep Space Force.

Ziarnick also uses his theory to analyze both the successes and failures of past and present space program organization and activities, as well as to describe preferred future actions for aspiring space powers. In particular, he draws many insightful parallels between the current American situation in space and the rise of US naval power in the early twentieth century, claiming that the United States' space power innovation will not happen overnight and will need to be a deliberate, long-term process. Thus, *Developing National Power in Space* is a valuable tool in understanding space power in both its applications and historical context.

Ziarnick is quite adept at describing problems with the division of America's current space program between civilian and military sectors and its concentration on mission-based rather than capability-based development. Not surprisingly, he is especially critical of the so-called von Braunian vision of space—a government-led, mission-oriented approach meant to devote the space program to one overarching objective, such as NASA's Apollo program to send men to the moon. With his practical approach to space power development, he is perhaps a bit too harsh in his criticism of knowledge gained via science and exploration as an end unto itself. Although such basic space research may not be a direct goal of national space power, it does play an important role in motivating future scientists and engineers to pursue careers in the space industry, helping us understand our place in the universe and developing new technologies inherently required to carry out far-reaching science and exploration missions.

Nevertheless, Ziarnick is quite successful in detailing a compelling vision for the American space program's future via his unique space power theory. Although the purely theoretical sections can at times be pedantic, the author provides many meaningful examples to illustrate his theory's main tenets, and his commentary on America's past and present space development problems and the recommended solutions are particularly engaging. Ziarnick writes with a sense of urgency and warning, clearly detailing the importance of setting the American space program on the right path for the future.

By discussing an extensive range of space development issues from the commercial, civil, political, and military perspectives and tying them into a General Theory of Space Power, Ziarnick offers excellent insights into synthesizing the efforts of these distinct space communities. Therefore, *Developing National Power in Space* should appeal to any space professional, enthusiast, policy maker, or planner interested in developing a wider comprehension of national space power and determining how a nation's space assets can be applied towards a unified vision.

1st Lt Keegan S. McCoy, USAF
Vandenberg AFB, California

The Cadet, Wild Blue U, Book 1, by Doug Beason. WordFire Press (http://wordfirepress.com), P.O. Box 1840, Monument, Colorado 80312-1840, 2015, 491 pages, $19.99 (softcover), ISBN 978-1-61475-289-9.

"A nuclear explosion. A star going nova. It was an event so sudden, so unexpected, and so cataclysmic that Rod could never have imagined it unless he had experienced it himself" (p. 73). This passage is just one of many throughout Doug Beason's novel *The Cadet* that seems simple but at the same time completely foreign to some readers, a memory to others, and complex to those who have never experienced life at the United States Air Force Academy. Overall, Beason presents an enticing tale about the beginning of this institution—one that is both historical and entertaining.

One of the best aspects of the novel is the fact that it includes elements that will connect with everyone in the military, not just cadets or graduates of the Air Force Academy or sister institutions. Parts of the book strike that eternal chord of military camaraderie, purpose, desire, and dedication that exist in everyone who has gone through some type of basic military training, regardless of the branch of service. The true gem, however, is the author's glimpse into some of the history of training that occurs at the academy—enlightening to people who have seen only the dorms and chapel from Colorado Springs or viewed the cadets through rose-tinted glasses. Although *The Cadet* is the first installment in what Beason hopes will be a Wild Blue U series of novels, it is, of course, important to note that the story takes place in a historical setting different from today's environment at the academy. Yet, Beason lays the foundation for a heritage that, hopefully, will appear in later novels as the series develops.

The author effectively blends fiction and history in this work to both educate and entertain readers regarding the origins of the Air Force Academy. The characters have unique stories; some who make only cameo appearances are actual cadets of the class of 1959. Regardless, the main character and supporting characters are people and family members who are realistic and not overly complex—individuals with whom the reader can identify. They are present as both the Air Force and the academy are developing, and they experience an incredibly exciting time that includes the first two decades of the Cold War and the period following the Korean conflict. Beason uses historical elements to add color to the story and highlight some of the glory of both the Air Force Academy and the service itself.

Despite the sweeping, dramatic, and emotional plot, parts of the story are somewhat predictable. This minor drawback does not necessarily detract from the overall quality of the work, however. Indeed, regardless of this predictability, readers find themselves "power reading" to get to the suspected resolution because they feel connected to some of the characters and want to share in their victory or defeat.

I highly recommend *The Cadet* to everyone, not just individuals who have attended, are attending, or wish to attend the Air Force Academy. Twice I have passed this novel along to new readers who have enjoyed the story and characters. Beason effectively keeps the reader involved and educated about both this institution and aspects of the early US Air Force. One can only hope that the author continues his Wild Blue U series and expands on the historical fictions in other periods and venues involving the Air Force Academy.

Capt Richard P. Loesch III, USAF
Laughlin AFB, Texas

Let us know what you think! Leave a comment!

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