NOVEMBER–DECEMBER 2015
VOLUME 29, NO. 6
AFRP 10-1

Senior Leader Perspective

An Airman's Story | **4**
General John E. Hyten, USAF

Feature

A Call to Action | **12**
Aid Geostationary Space Situational Awareness with Commercial Telescopes
Capt Daniel Moomey, USAF

Departments

31 | Views

Purposeful Development of the Intelligence, Surveillance, and Reconnaissance *for* Space Cadre | **31**
SMSgt Mitchell R. Overton, USAF

Space-Policy Education | **43**
Contexts and Constraints, Content and Methodology
Dwight Rauhala

49 | Commentaries

How to Make Disaggregation Work | **49**
Dr. Peter Wegner
Dr. Thomas C. Adang
Maureen Rhemann

Personnel Recovery in Space | **56**
Lt Col Mari Manifold, USAF

60 | Schriever Essay Award Winners

Preparing for the Cyber Battleground of the Future | **61**
2nd Lt Chris Babcock, USAF

Defending Our Satellites | **74**
The Need for Electronic Warfare Education and Training
Lt Col E. Lincoln Bonner, USAF

Developing Tomorrow's Space War Fighter | **83**
The Argument for Contracting Out Satellite Operations
Maj Sean C. Temple, USAF

91 | Book Reviews

Reconsidering the American Way of War: US Military Practice from the Revolution to Afghanistan 91
Antulio J. Echevarria II
Reviewer: Capt Ian S. Bertram, USAF

Predator: The Secret Origins of the Drone Revolution 92
Richard Whittle
Reviewer: Lt Col Cameron S. Pringle, USAF

The Spirit of Attack: Fighter Pilot Stories 93
Bruce Gordon
Reviewer: 1st Lt Keegan S. McCoy, USAF

Every Citizen a Soldier: The Campaign for Universal Military Training after World War II 94
William A. Taylor
Reviewer: Amanda B. Biles

NASA's First A: Aeronautics from 1958 to 2008 95
Robert G. Ferguson
Reviewer: Maj Jason M. Newcomer, DBA, USAF

Shadow Wars: Chasing Conflict in an Era of Peace 96
David Axe
Reviewer: Capt Nicholas A. Reinhold, USAF

Wiki at War: Conflict in a Socially Networked World 97
James Jay Carafano
Reviewer: Maj William R. Giles, USAF

A Low-Visibility Force Multiplier: Assessing China's Cruise Missile Ambitions 99
Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan
Reviewer: Lt Col John S. Meiter, USAF

Editorial Advisors

Allen G. Peck, Director, *Air Force Research Institute*
Lt Gen Bradley C. Hosmer, USAF, Retired
Prof. Thomas B. Grassey, *US Naval Academy*
Lt Col Dave Mets, PhD, USAF, Retired, *School of Advanced Air and Space Studies (professor emeritus)*

Reviewers

Dr. Christian F. Anrig
Swiss Air Force

Dr. Bruce Bechtol
Angelo State University

Dr. Kendall K. Brown
NASA Marshall Space Flight Center

Col Steven E. Cahanin
Director of Technologies and Information
Air Force Personnel Center

Dr. Norman C. Capshaw
Military Sealift Command
Washington Navy Yard, DC

Dr. Stephen D. Chiabotti
USAF School of Advanced Air and Space Studies

Dr. Mark Clodfelter
National War College

Dr. Christopher T. Colliver
Wright-Patterson AFB, Ohio

Dr. Charles Costanzo
USAF Air Command and Staff College

Col Dennis M. Drew, USAF, Retired
USAF School of Advanced Air and Space Studies
(professor emeritus)

Maj Gen Charles J. Dunlap Jr., USAF, Retired
Duke University

Dr. James W. Forsyth
USAF School of Advanced Air and Space Studies

Lt Col Derrill T. Goldizen, PhD, USAF, Retired
Westport Point, Massachusetts

Col Mike Guillot, USAF, Retired
Editor, *Strategic Studies Quarterly*
Air Force Research Institute

Dr. Grant T. Hammond
USAF Center for Strategy and Technology

Dr. Dale L. Hayden
Air Force Research Institute

Col S. Clinton Hinote
Military Fellow
Council on Foreign Relations

Dr. Thomas Hughes
USAF School of Advanced Air and Space Studies

Lt Col Jeffrey Hukill, USAF, Retired
Curtis E. LeMay Center for Doctrine Development
and Education

Lt Col J. P. Hunerwadel, USAF, Retired
Curtis E. LeMay Center for Doctrine Development
and Education

Dr. Mark P. Jelonek, Col, USAF, Retired
Aerospace Corporation

Col John Jogerst, USAF, Retired
Navarre, Florida

Col Wray Johnson, USAF, Retired
School of Advanced Warfighting
Marine Corps University

Mr. Charles Tustin Kamps
USAF Air Command and Staff College

Dr. Tom Keaney
Johns Hopkins University

Col Merrick E. Krause, USAF, Retired
Defense Contract Audit Agency

Col Chris J. Krisinger, USAF, Retired
Burke, Virginia

Dr. Charles Krupnick
Troy University

Dr. Benjamin S. Lambeth
Center for Strategic and Budgetary Assessments

Dr. Richard I. Lester
Eaker Center for Professional Development

Dr. Adam Lowther
School for Advanced Nuclear Deterrence Studies

Mr. Brent Marley
Huntsville, Alabama

Mr. Rémy M. Mauduit
Air Force Research Institute

Col Phillip S. Meilinger, USAF, Retired
West Chicago, Illinois

Dr. Richard R. Muller
USAF School of Advanced Air and Space Studies

Col Robert Owen, USAF, Retired
Embry-Riddle Aeronautical University

Lt Col Brian S. Pinkston, USAF, MC, SFS
Civil Aerospace Medical Institute

Dr. Steve Rothstein
Colorado Springs Science Center Project

Col John E. Shaw
Peterson AFB, Colorado

Dr. James Smith
USAF Institute for National Security Studies

Col Richard Szafranski, USAF, Retired
Isle of Palms, South Carolina

Lt Col Edward B. Tomme, PhD, USAF, Retired
CyberSpace Operations Consulting

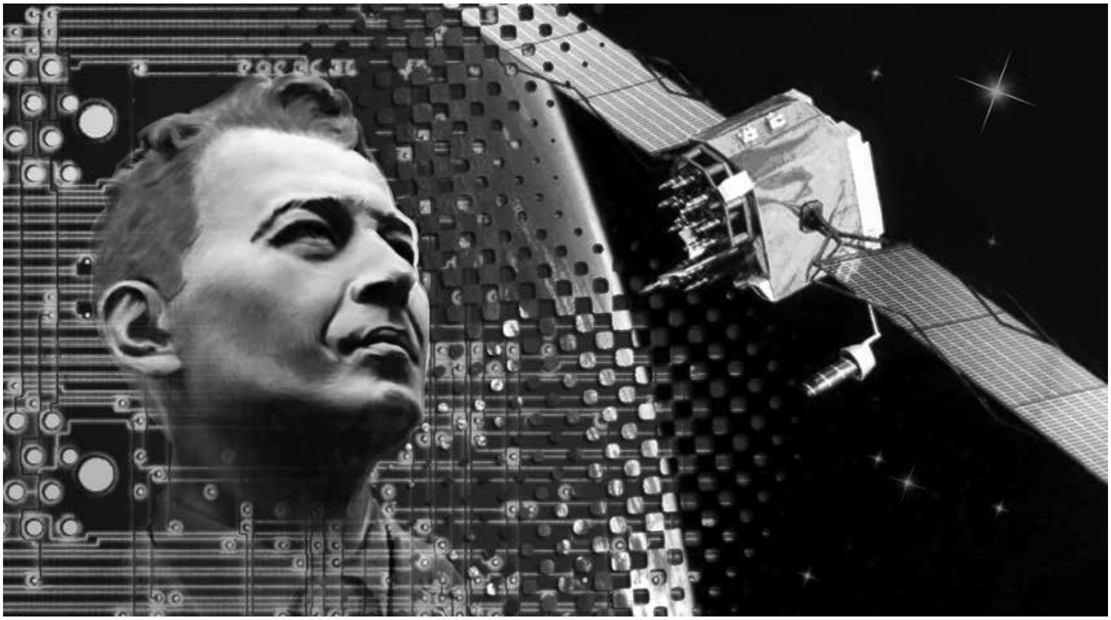
Lt Col David A. Umphress, PhD, USAFR, Retired
Auburn University

Col Mark E. Ware, USAF, Retired
Twenty-Fourth Air Force

Dr. Xiaoming Zhang
USAF Air War College

An Airman's Story

General John E. Hyten, USAF



Every U.S. military operation across the planet, across the entire spectrum of conflict, depends on space and cyberspace to accomplish its mission. From humanitarian operations to full spectrum combat, our Joint force would not be as lethal or effective in the prosecution of our missions without space and cyberspace. They are perhaps the most joint of all the operational domains. All Services rely equally upon the capabilities delivered by, from and through these domains—but space, in particular, is an Airman's story. However, it is a story that Airmen, in general, don't tell particularly well. We should.

The Airman most associated with space is General Bernard Schriever. Most Airmen know him as the "Father of Air Force Space and Missiles." Schriever Air Force Base is named in his honor. He led the development of the ICBM as well as the CORONA satellite program in the late 1950s and early 1960s. Some know that then Major General Schriever was on the cover of *Time* Magazine in April of 1957 and in the article discussed the future of space and missiles. Very few of us know that two months earlier, in February of 1957, he made the inaugural address to the Air Force Office of Scientific Research Astronautics Symposium in San Diego. In this address he stated:

> In the long haul, our safety as a nation may depend upon our achieving "space superiority." Several decades from now, the important battles may not be sea battles or air battles, but space battles, and we should be spending a certain fraction of our national resources to ensure that we do not lag in obtaining space supremacy. Besides the direct military importance of space, our prestige as world leaders might well dictate that we undertake lunar expeditions and even interplanetary flight when the appropriate technological advances have been made and the time is ripe.[1]

It is most remarkable to realize that this great Airman was talking like this and leaning forward even before the launch of Sputnik in October of 1957—when the rest of the world thought the space race began. The race was already underway, and General Schriever was talking about it—leading our Air Force into the future—which leads to consider another visionary Airman and space leader: The 4th Air Force Chief of Staff, General Thomas D. White.

In 1958, shortly after Sputnik, General White coined the term "aerospace." In early 1959, as he sat in front of a skeptical House committee to testify on the importance of space, General White used this word twelve times. He explained "Air and space comprise a single continuous operational field . . . there can be no operational boundary between them."[2] It is important to note the words he chose. He did not try to claim that aerospace was a single physical domain—it was a continuous operational field—with no operational boundaries. Even in 1958, he was trying to focus the world on the operational effects that would be enabled and generated from and through space and that the power of the Air Force would be found in integrating and applying them together to create advantages over our adversaries. General White clearly understood the advantages space could bring to military operations.

Which then brings us to General Jerome (Jerry) O'Malley. In the late 1970s and early 1980s, as the Vice Chief of Staff of the Air Force, based on a belief the space domain had the potential to fundamentally change warfare and improve the ability of our Air Force to conduct operations, he became convinced of the need for the Air Force to establish a separate space command. Almost all space capabilities were highly classified at the time, and most warfighters were not even aware of the existence of military satellites in a variety of mission areas (weather, communications, intelligence-surveillance-reconnaissance (ISR), missile warning, etc.). He began pushing the AF leadership to create an operational command focused on using space capabilities to support the warfighter. He had the support of many others, but he was the driving force. His efforts eventually resulted in the creation of Air Force Space Command in 1982—and the operational focus of space in the military really began to accelerate.

Schriever, White, and O'Malley—three of the most important pioneers and legends of the space business in our Air Force. Most remember the role of General Schriever, but few remember the roles of General White and General O'Malley—but these three pioneers are responsible for much of what we have today and for the transformation of warfare from the industrial age to the information age. And what did they all have in common? They were not Aerospace Engineers. That field of study did not even exist when they were in college, nor was term even created. They were not "space professionals" or even "space officers." They were all aviators and, more importantly, they were Airmen—and that is why space, although incredibly Joint today, is an Airman's story and a story every Airman should be able to tell. Most of us do not remember this legacy, but we need to study it and learn from it because new challenges are looming. We must prepare to respond to new threats in space—and in cyberspace—and we must ultimately ask ourselves, is cyberspace an Airman's story as well?

Our Dependence on Contested Domains

At the time General White gave his testimony, there were only two countries remotely capable of placing a satellite in orbit: The United States and the Soviet Union. There were only a handful of man-made objects in space, all of which reentered the atmosphere in relatively short order. The number of threats to our space assets were minimal. As more countries have become space-faring nations, several, including the United States (Operation Starfish Prime, ASM-135 (F-15) program, SM-3) have demonstrated anti-satellite capabilities. Our perspective of space has changed from "safe haven" to "contested" and from "sanctuary" to "theater."

All remotely piloted aircraft (RPA) depend on space systems, just one example of which is the Global Positioning System (GPS). Without GPS, the RPA does not have the ability to enter a theater, nor does the pilot have the ability to know its position. Beyond basic flight, the RPA operator would not be able to use precision weapons or perform ISR missions with confidence.

Degradation or denial of GPS would have worldwide civil implications as well. Civil aviation, Wall Street and the agricultural community are just a sample of organizations poised to suffer serious impacts if position, navigation and timing were not available. Senator Jeff Sessions of Alabama recently said "[Our adversaries] stand to undermine the space-enabled advantages our country has benefited from for nearly sixty years."[3] He was not just speaking about military capability; his perspective included civilian applications as well.

The cyberspace domain faces similar situations on a daily basis. Joint, worldwide military operations depend on information delivered by this domain—everything from F-35 helmets to loadmaster checklists and from special operations equipment to the software in the USS *Ford*, the Navy's newest aircraft carrier. The information and data missions within cyberspace are vital to accomplishing Joint missions. Precision operations require the information not only be available and expedient but to be accurate as well. Anything from a simple power surge to a complex manipulation of data can render all decisions, from tactical to strategic, much less effective and questionable. Not coincidently, civil aircraft, Wall Street and the agriculture community face the same dire impacts if civil cyberspace is unavailable as well. While these domains are very different, any disruption by an adversary has the same outcome on capability and mission effectiveness.

These dependencies create vulnerabilities, and thus create centers of gravity for potential adversaries to exploit. Joint Publication 5-0, *Joint Operation Planning*, clearly states the Characteristics of Centers of Gravity (COG).[4] Space and cyberspace fit every criteria, not only for our adversaries, but for the United States as well. Most telling is the characteristic "Can endanger one's own COGs."[5] This has never been truer than with space and cyberspace. If the effectiveness of space and cyberspace operations were diminished, the effectiveness of the land, air and sea forces would all be diminished as well. For example, if an adversary ever denied us the ability to operate in space, the United States would be forced to use pre-space tactics to conduct land operations. Which begs the question: If we are not prepared to defend or oppose an adversary in the space or cyberspace domains, are we prepared to use a World War II mindset to win? World War II was fought using completely different doctrine and principles. If space and cyberspace were removed from today's joint capabilities, the United States would need a mass of force to replace the precision, agile force the world has come to expect. The Department of Defense would require large global footprints to replace the agile expeditionary logistics we have come to rely on. Not all changes would occur at the tactical level. If space and cyberspace were removed from our Joint doctrine, commanders at all levels would be forced to regress to predictive assessments instead of using the conclusive analysis of intelligence we use today.

Whether you subscribe to Col John Warden's "five-ring" model of strategic attack or the Clausewitz Center-Of-Gravity theory, the United States' dependence on space and cyberspace is undeniable. The Department of Defense must protect these domains, not just for military superiority, but for the Nation's diplomatic and economic Instruments of Power as well.

Air Force Space Command Is Changing to Meet Future Challenges

> *To each there comes in their lifetime a special moment when they are figuratively tapped on the shoulder and offered the chance to do a very special thing, unique to them and fitted to their talents. What a tragedy if that moment finds them unprepared or unqualified for that which could have been their finest hour.*
>
> —Sir Winston S. Churchill

As the Department of Defense realizes the dependencies and vulnerabilities of our space and cyberspace situations, there is a single indisputable fact: the Air Force and Air Force Space Command must adapt to meet and defeat these challenges.

Prior to space and cyberspace entering the battlefield, land commanders would require significant time prior to executing mass maneuver. It used to take hours or days for tactical warfighters to pass intelligence, relay damage assessments or request more forces. Now, space and cyberspace capabilities are used to facilitate the flow of information, empower faster decisions, and build knowledge of the theater for even the most tactical warfighter. A land commander can, within mere moments, coordinate precision maneuvers with concentrated firepower, and relay follow-up orders based on near-real-time feedback from the results. This can all happen while National decision-makers monitor the battle in near-real-time from the opposite side of the globe. Space and cyberspace create accuracy, availability and speed for the warfighter, the likes of which the world has never seen before.

While the entire Joint force requires these capabilities, the Air Force needs to answer a single question: what does the Air Force need to do to ensure these capabilities are available if challenged by an adversary? The answer: the Air Force must build Airmen who are ready to respond effectively and in a timely manner in the space and cyberspace domains. The answer, while simple, requires deliberate planning and execution.

First, Air Force Space Command is building a robust architecture to gain complete situational awareness. Air Force Space Command is the oldest non-regional Major Command in the Air Force with the least operational domain awareness. This concept is basic to all warfare. This easily equates to awareness of the airspace. Compared to the space domain, Joint Combatant Commanders have a clear understanding of their airspace at all times. There are several layers of redundant systems to identify, distinguish and track friendly, civilian, or hostile aircraft. However, Air Force Space Command's Area of Responsibility (AOR) is 73 trillion cubic miles. The difficulties and complexities required to identify and track satellites are enormous. In addition, "we have to develop new space tactics and doctrines, to account for a contested space environment."[6]

The same can be said for the cyberspace domain. The world's first man-made operational domain is already known for its dependencies, but its vulnerabilities are not completely understood. The cyber breach of the Office of Personnel Management became public in June 2015, and it became one in a series of high-profile penetrations targeting valuable information. This is also a highly-contested domain. To drive home the point, the U.S. Army Cyber Command, in its website recruiting video, blatantly asks: "Are you ready to step onto the cyberspace battlefield?"[7] Understanding what is over the next "cyberspace hill" requires Air Force Space Command to explore and gain awareness of the cyberspace domain. As we build deliberate cyberspace situational awareness, it is important to keep in mind the newness of this domain. Air Force Space Command is still appreciating the possibilities of this domain. As we shift our understanding, we must not fool ourselves. Deputy Secretary of Defense Bob Work points out that the "sanctuary . . . and the margin of technological superiority upon which we have become so accustomed to [in space and cyberspace] is steadily eroding."[8] Adversarial aggression in these contested domains is being deterred and defended against every day.

Second, Air Force Space Command must fundamentally change the presentation of Forces to Combatant Commanders. This also requires a shift in the command and control of these forces, and how we train our forces. Air Force Space Command is currently developing the Space Mission Force, and portions of the Cyber Mission Force, to meet this need. Space and cyberspace professionals will be receiving specialized training to fluently understand our domain capabilities to respond to adversarial threats. This is absolutely congruent with Joint Publication 3-0, which requires this understanding for Joint Operations.[9]

Third, joint commanders must be aware of the complexities of the space and cyberspace domains, and the operations required for safety of flight and mission assurance. There is an absolute uniqueness to both space and cyberspace. Space and cyberspace provide mission support to the joint fight, but they are domains and AORs as well. Space and cyberspace cannot be thought of in the context of a traditional "Area of Responsibility." In a geographical AOR, the air, land and sea domains can be separated from those of another AOR. For example, aircraft flying in one AOR are of little concern to an AOR on the other side of the world. This is not true with space or cyberspace. The space, or cyber, domain of one AOR cannot be separated from that of another AOR. These two domains are inherently global. A satellite in orbit, friend or foe, is of equal concern for AORs around the world and cyber operations transit global networks continuously and at the speed of light. It is equally important to keep in mind the capabilities these domains provide directly influence the flow of information. Because of this, defending information, and preventing it from getting in the wrong hands, is a vital concern.

To be clear: "Space" and "Cyberspace" are not missions; they are unique operational domains in which global military operations and missions are performed. It is important to understand that space and cyberspace are operational domains to engage and defeat adversarial aggression, not simply support functions to enhance joint air, land and sea operations.

Strategic leverage derived from space and cyberspace capabilities has created a fundamental shift in the nature of warfare. No longer does the advantage lie with the largest military or the force with the largest arsenal. Nor does it lie with the biggest weapon or most defensible position. These can all be countered with the integration of space and cyberspace capabilities by delivering warfighting decision superiority across all military missions.

As such, before any possible conflict, commanders must understand how space and cyberspace assets in these two domains must be protected. The organization of space and cyberspace domains under one command is a natural placement. While some may argue against this construct, there is a simple, logical reason: space and cyberspace create the same effects for every mission.

Space and cyberspace support every one of the five Air Force Core Mission areas: (1) air and space superiority; (2) ISR; (3) rapid global mobility; (4) global strike; and (5) command and control. It is worth pointing out: every Air Force Core Mission will fail unless we maintain the freedom to operate and conduct missions in the space and cyberspace domains.

Air Force Space Command continues to build a defendable space and cyberspace enterprise as we restructure to build capabilities for United States Strategic Command and United States Cyber Command. While Joint Forces Air Component Commanders have been using this model for years, this construct requires a fundamental shift in thinking for the space and cyberspace domains. These two contested domains are facing threats, and in some cases attacks, every day.

No person, military or civilian, should ever want a war in space or cyberspace. However, if there is, our nation has the right to defend itself, and we must be ready. The United States has the inherent right to self-defense, and we need to be prepared to exercise that right at any time, if required.

Conclusion

> *It is no use saying, "We are doing our best." You have got to succeed in doing what is necessary.*
>
> —Sir Winston S. Churchill

> *To be prepared for War is one of the most effectual means of preserving peace.*
>
> —George Washington

Adversarial challenges within the space and cyberspace domains are not imminent; they are already here. The future of our space and cyberspace superiority depends on our actions today.

Our requirement to prepare for conflict is unavoidable. The Department of Defense's dependencies on space and cyberspace capabilities require our operators to win against adversaries in these contested domains.

The Department of Defense is reliant on the 24/7 availability of space and cyberspace. Space and cyberspace systems have given us a near-real-time capability to correlate information and data across all National Instruments of Power. Global space and cyberspace information provides the "nervous system" for our Air Force and the Joint Force. This gives our commanders and National leaders the decision superiority needed to preserve peace, which we must be prepared to defend. Air Force Space Command is committed to improving our situational awareness and operational mindsight in order to effectively control our AOR when needed so that we can continue to support joint missions worldwide. This is an Airman's responsibility—and an Airman's story. ✪

Notes

1. Maj Gen Bernard Schriever, "ICBM—A Step toward Space Conquest" (address to the Air Force Office of Scientific Research Astronautics Symposium, San Diego, 19 February 1957).

2. House, *Gen Thomas D. White, Chief of Staff, USAF, Testimony before the House Committee on Science and Astronautics, Missile Development, and Space Sciences*, 86th Cong., 1st sess., 3 February 1959.

3. Senator Jeff Sessions (R-AL) (opening statement in transcription of the Senate Armed Services Subcommittee on Strategic Forces hearing on military space programs, 29 April 2015, page 3), http://www.armed-services.senate.gov/hearings/15-04-29-military-space-programs-.

4. Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011, III-23, fig. III-11, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

5. Ibid.

6. Deputy Secretary of Defense Bob Work (speech to the GEOINT Symposium 2015, Washington Convention Center, Washington, DC, 23 June 2015), http://www.defense.gov/News/Speeches/Article/606685.

7. "Army Cyber Protection Team," video, 4:11, US Army Cyber Command, accessed 27 August 2015, http://www.arcyber.army.mil/index.html.

8. Deputy Secretary of Defense Bob Work (speech to the China Aerospace Studies Institute, RAND Corporation, Arlington, VA, 22 June 2015), http://www.defense.gov/News/Speeches/Article/606683.

9. Joint Publication 3-0, *Joint Operations*, 11 August 2011, IV-5, fig. IV-2, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

General John E. Hyten, USAF

General Hyten (Bachelor's degree in engineering and applied sciences, Harvard University; Master of Business Administration degree, Auburn University) is Commander of Air Force Space Command, Peterson Air Force Base, Colorado. He is responsible for organizing, equipping, training and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands around the world. General Hyten oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition. He leads approximately 38,000 space and cyberspace professionals assigned to 134 locations worldwide.

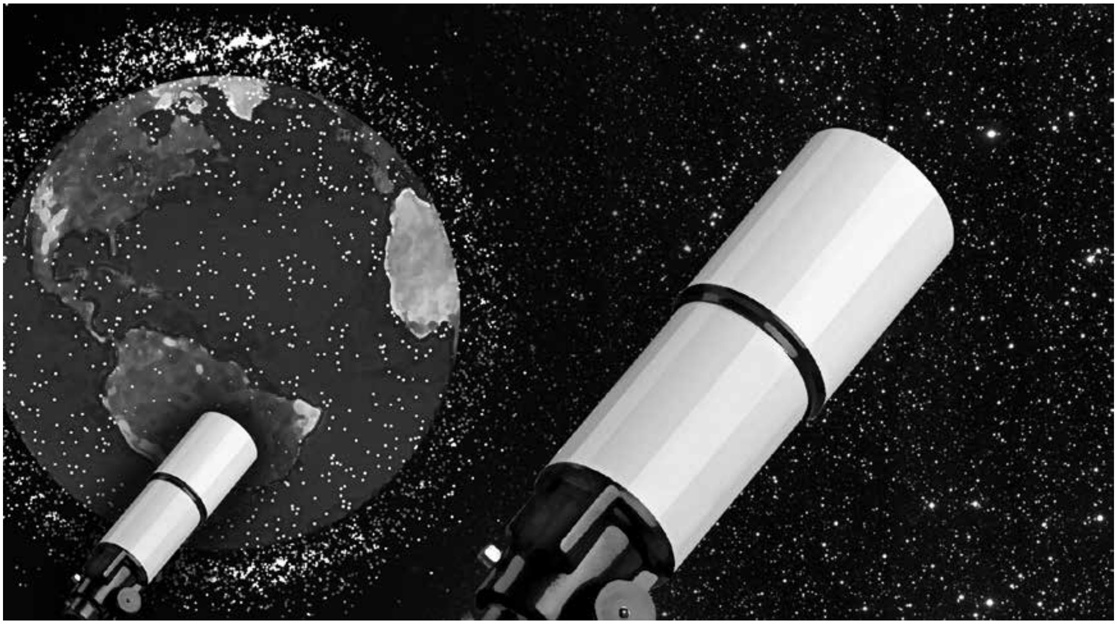
Let us know what you think! Leave a comment!

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

A Call to Action

Aid Geostationary Space Situational Awareness with Commercial Telescopes

Capt Daniel Moomey, USAF



The accumulation of man-made objects in Earth orbit increases with each space launch. Early in the space age, congestion of the common Earth orbit regions was of little concern, but after more than 50 years of launches, satellites now orbit our planet with closer spacing to one another than ever before. This article addresses this issue, particularly for the geostationary (GEO) orbit region.

The congested, contested, and competitive space domain could have a global impact on people's lives because the likelihood of an on-orbit satellite collision is continually increasing.[1] In addition to civil services' dependence on space-based assets, the US military has become more reliant on them and places a high value on those assets. As space becomes not only more congested but also more contested, the types and numbers of resources required to gain and maintain space situational awareness (SSA) must increase.

Maintaining accurate orbit estimations for all man-made Earth-orbiting objects (also known as resident space objects [RSO]) has become quite difficult because of their steadily growing numbers. The US Air Force created and maintains the satellite catalog, which is also one of the missions for the Joint Space Operations Center (JSpOC), located at Vandenberg AFB, California. To facilitate this mission, the Air Force maintains a global network of radar and optical telescope sites collectively known as the Space Surveillance Network (SSN). This network is primarily responsible for generating and reporting on the locations and trajectories of RSOs to the JSpOC.[2] Over the decades, the size of the satellite catalog has grown, taxing the resources of the SSN. According to the *Enabling Concepts for Space Situational Awareness* document (2007), "The existing Space Surveillance Network . . . was not designed, and is insufficient, to support Space Control needs (e.g. Inadequate coverage to provide persistent surveillance of threats)."[3]

The additional demand on sensor tracking resources has become especially true for SSN sensors tasked to track GEO RSOs. New tracking assets have recently come online that can observe dim objects (down to the 21st visual magnitude [vm]).[4] For example, two separate collection surveys have independently observed a bimodal brightness distribution of objects in and around GEO. Figure 1 depicts this distribution collected during both the 2006 European Space Agency (ESA) Space Debris Survey and the 2010 Air Force Research Laboratory (AFRL) Panoramic Survey Telescope and Rapid Response System (Pan-STARRS or PS1) GEO Survey. Throughout both surveys, observations were taken of objects that traversed the camera's field of view. The detection threshold of the PS1 system drops off at higher vm with higher rates of transit, shown in the dashed, dotted, and solid lines, and is measured in arcseconds per second (as/s).[5]

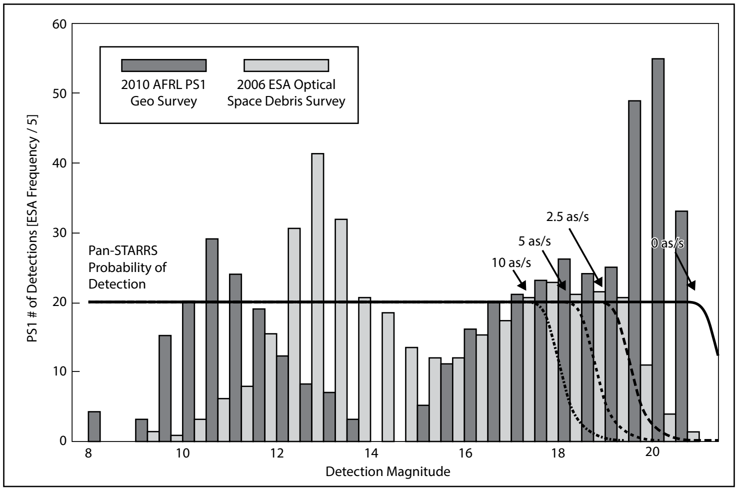


Figure 1. GEO survey brightness histogram. (Reprinted from Mark Bolden, Paul Sydney and Paul Kervin, "Pan-STARRS Status and GEO Observations Results" [paper presented at the Advanced Maui Optical and Space Surveillance (AMOS) Technologies Conference Proceedings, Maui, HI, 2011], [2], "Figure 2: AFRL & ESA Geo Survey Comparison," http://www.amostech.com/TechnicalPapers/2011/Orbital_Debris/BOLDEN.pdf.)

The figure shows a substantial population density curve of relatively bright and presumably large objects between 8th and 16th vm. In addition, another substantial population of much dimmer objects exists between 15th and 21st vm. This bimodal distribution indicates the existence of a substantial population of presumably small, dim objects not typically observed by the SSN. Although existing operational tracking systems can observe this class of objects, a lack of available sensor time caused by the demands of higher priority taskings has largely prevented the consistent tracking of these objects. Thus, most of them are not regularly maintained as part of the satellite catalog. Without regular orbit maintenance, they cannot be screened for conjunction analysis, leaving an unquantified risk of collision for objects in GEO.[6]

According to *Continuing Kepler's Quest: Assessing Air Force Space Command's Astrodynamics Standards*, "The committee [for the Assessment of the US Air Force's Astrodynamic Standards] believes that the primary limitation in the current system for objects not experiencing significant drag is not the accuracy of the algorithms, but rather the quantity and the quality of the sensor tracking data. The key system limitations are current sensor coverage, understanding of the quality of the observations, and the challenge of fusing disparate data from different systems and phenomenology. Understanding the quality or statistics of the observations is necessary for obtaining a realistic covariance, which is needed for computing an accurate probability of collision."[7]

In an attempt to alleviate the problem of an overburdened SSN and to increase coverage, the Department of Defense has in the past sparingly employed commercial off-the-shelf (COTS) electro-optical telescope systems for space surveillance purposes. Recent technological developments in the design of mounts, optics, and focal planes have produced lower-cost, higher-capability, and higher-accuracy COTS astronomical equipment.[8] The current operational and fiscal environment has created a greater need to find effective, suitable, and more cost efficient solutions to operational problems. In an attempt to apply these principles to aid the GEO SSA mission, this article considers the following question: *Can a large-scale employment of small-aperture COTS telescopes augment the SSN's observing capacity of the geostationary belt without degrading the quality of orbit estimations?*[9]

The results from the study offer a good indication that COTS equipment could serve the Air Force's mission needs and enable the Department of Defense to reallocate tasking time on the existing larger, more capable optical SSN assets to observe smaller, dimmer, lower-priority objects that have thus far remained largely undetected and/or uncataloged. Such a change should occur in a manner consistent with the committee's remarks (see above) and should follow the principles of SSA:

- integration
- accuracy
- relevance
- timeliness
- fusion
- accessibility and security

- survivability/sustainability/deployability
- unity of effort
- interoperability[10]

Perhaps most importantly, achieving such a state would aid the goals and vision of the commander of Air Force Space Command (AFSPC) towards realizing SSA:

1. predictive intelligence of all threats to space-related systems
2. persistent coverage of threats (e.g., no loss of track)
3. timely attribution of attacks/threats
4. integrated SSA, fusion of intelligence, surveillance, reconnaissance, and environmental
5. determination of the adversary's capability, purpose, and intent[11]

To validate the above, the study used the following method to design and test a system that addresses each of the AFSPC commander's needs. First, a basic systems engineering approach determined an appropriate system specification using optical COTS equipment and software that could reliably observe high-value GEO RSOs to meet the commander's five mission requirements. Next, the author devised a test system to determine the feasibility of applying such a concept to the operational environment. Doing so required the capture, processing, analysis, and comparison of observations from a small optical COTS system with the operational SSN systems. Consequently, the first objective was to determine the accuracy of the satellite metric observations of the test system. Such observations are represented as a series of numerical values such as time, right ascension, and declination. The second objective called for determining the feasibility and quality of performing an orbit determination and differential correction of the observed RSOs by using the most recent published orbit estimations in two-line element (TLE) set format from the JSpOC. Only the observations from the test system were included to perform differential corrections on the TLEs with the intent of including as much angular coverage as possible to increase the orbit determination accuracy.

Using only COTS equipment and commercial or free software, the study demonstrated a method to optically observe high-value GEO RSOs, create high-accuracy metric observations, and use those observations to converge on an update to the JSpOC-published TLE. Additionally, satellite ephemerides were computed and modeled in a Systems Tool Kit simulation for illustrative comparison against the respective TLEs. Having established the accuracy, the study then conducted a performance comparison of metric accuracies between the experimental setup and the current SSN systems.

Assumptions and Limitations

Assumptions for the project as a whole began with an expectation of how the SSA mission will proceed in the future. The study first assumed that the demand for timely, accurate, and complete SSA capabilities will continue to grow. It also assumed that the primary burden for SSA operational tasking, collection, processing, exploitation, and dissemination will continue to fall to the JSpOC.[12] The center will proceed with development of its Mission System, employing a scalable server architecture and providing additional processing capacity necessary to ingest the observations generated by this study's proposed system for satellite catalog maintenance. In addition, although not invariably true, the study assumed that existing GEO-observing SSN sites are tasked, by and large, with high-priority observation of high-value GEO RSOs, which are typically sizable and relatively bright. This provides the foundation to reduce high-priority taskings for the existing GEO SSA assets.

Consequently, the observations collected were limited to large, bright, geostationary satellites in the visible band, using inexpensive COTS equipment. The number and quality of the collections were affected by the weather, local sky brightness, and limitations of the equipment. The angular accuracy and precision of the observations were also constrained by image processing techniques such as the ability to determine precisely the time at which the observation was created. Synchronizing the computer's clock, which stored the images, with the US Naval Observatory's master clock from the observatory's website established an accurate time of capture. The stated accuracy for the observatory and the National Institute of Standards and Technology time servers is to the nearest whole second (±0.5 second).[13]

Analysis of the observations utilized general-perturbation TLEs published by the JSpOC for a baseline comparison. When the study used general-perturbations accuracy, the difference between the observed position and the expected position of the satellites was typically within the average accuracy of a JSpOC GEO TLE. Because of this finding and the relatively short time span of the observing periods, the study could not treat the TLEs as a suitable truth reference from which to validate a sensor bias value for the test system.

Because the study was constrained to address the stated goals/vision of the AFSPC commander for the case of the high-value assets along the geostationary belt, the work focused on a single-point design analysis. The analysis sought to optimize the system design by minimizing the diameter of the primary aperture and maximizing the observable vm while making reasonable worst-case assumptions about the nature of an RSO and the observing conditions. In constraining the study to concentrate on system design and observation-quality analysis, the author recognizes other principles of SSA—primarily security, deployability, and sustainability—as important, addressing them in the next section but not analyzing them in depth.

Operational System Design and Specifications

According to the AFSPC commander, additional SSA capabilities are required to augment current capacity. From the stated mission need to the derivation of mission requirements, measures of effectiveness, and measures of performance, the study will present a notional system specification and system performance to show how a large-scale implementation of COTS equipment can aid the GEO SSA mission. Here, this implementation is referred to as the Small Aperture Deep Space Surveillance system (SADSS). The requirements shown in table 1 were developed specifically for this study and derived from the AFSPC commander's goals and vision to attain SSA. The mission requirements are intended to address the five goals. From the requirements, measures of effectiveness are derived in table 1 as well. The goals of the measures of effectiveness are to serve as indicators of the system's ability to meet each of the mission requirements. From the measures of effectiveness, design parameters and measures of performance are also established (see table 2). For quantitative values of the measures of performance, refer to the author's original thesis work.[14]

Table 1. Mission requirements and measures of effectiveness for SADSS

MR1	System shall be able to create observations with the capability to produce element sets for GEO objects, which are as accurate or more accurate than element sets created using observations from the current SSN (addresses goal 1)	
	MOE 1-1	Sensor metrics accuracy
	MOE 1-2	Ephemeris accuracy
MR1	System shall be capable of observing high-value space assets at all longitudes of the geosynchronous belt (addresses goals 1 and 2)	
	MOE 2-1	Probability of detection of a high-value GEO RSO
	MOE 2-2	Coverage area
MR3	System shall be capable of providing persistent coverage for targets of interest anywhere along the geosynchronous belt (addresses goal 2)	
	MOE 3-1	Coverage time
MR4	System shall be capable of providing near-real-time observations of high-value GEO RSOs to the JSpOC (addresses goal 3)	
	MOE 4-1	Observation sample rate
	MOE 4-2	Astrometry plate solution success ratio
MR5	System shall be capable of providing observations in a format ingestible to its customers (addresses goal 4)	
	MOE 5	Differential correction from TLE using SADSS observations
MR6	System shall be capable of providing information useful for determining capabilities and purpose of the observed RSOs (addresses goal 5)	
	MOE 6	SNR of RSO's point spread function over time

MR = mission requirement
MOE = measure of effectiveness
SNR = signal-to-noise ratio

Table 2. SADSS final system specification and measures of performance

MR	*MOE & Effect*	*Design Parameters & Specifications*			*MOP*	
MR1	MOE 1-1 High accuracy sensor metrics	Pixel field of view *2 arcsec (12 micrometer pixel pitch)*	Precision of image time *< ±0.133 sec*		MOP 1-1-1	Sensor sigma
					MOP 1-1-2	Sensor bias
	MOE 1-2 High confidence and accuracy of generated ephemeris	Sun angle limits *0°–100°*	Sensor sigma *Timing precision + imaging precision = 5 arcsec (est.)*		MOP 1-2-1	Orbit solution covariance matrix
					MOP 1-2-2	RMS of orbit solution
MR2	MOE 2-1 High probability of detection	Aperture diameter *25 cm*	RSO area *$\geq 4\ m^2$*	Band avg. CCD QE *75%*	MOP 2-1-1	Detected signal
	MOE 2-1 High probability of detection	CCD Noise *Read 8 e-/pix* *Dark .2 e-/pix/sec*	Sky noise *Diego Garcia + $2vm/arcsec^2$*		MOP 2-1-2	Detected noise
	MOE 2-2 Large coverage area	Focal length 1.25 m	Film format *30.5 x 30.5 mm*		MOP 2-2	FOV
MR3	MOE 3-1 Coverage time	Sun angle limits *0°–100°*	Number of sites *5*		MOP 3-2-1	Observed orbit
					MOP 3-2-2	Minimum elevation
MR4	MOE 4-1 Increased observation rate	Exposure time *1 sec*	Processing time *< 6.5 sec*		MOP 4-1	Exposure time + Processing time
	MOE 4-2 High astrometry solution ratio	FOV *$2^{\circ 2}$ (1.4°x1.4°)*	Aperture diameter *25 cm*		MOP 4-2-1	no. of stars detected
	MOE 4-2 High astrometry solution ratio	Focal length *1.25 m*	Aperture diameter *25 cm*		MOP 4-2-2	Image distortion
MR5	MOE 5 Successful differential correction	Calibrated data *Requires validation*	Compatible message *GEOSC format*		MOP 5	Residual rejection %
MR6	MOE 6 Actionable information	SNR sample rate *Observation sample rate*	SNR error *Requires customer input*		MOP 6	Quality of light curve metrics

MR = mission requirement
MOE = measure of effectiveness
MOP = measure of performance
arsec = arcseconds
vm = visual magnitude
CCD = charge coupled device
FOV = field of view
SNR = signal-to-noise ratio
QE = quantum efficiency
GEOSC = geoscience
RMS = root mean square

From the mission requirements, two fundamental differences emerge between previous efforts to incorporate small-aperture COTS solutions and the work presented here. From MR2, the proposed system would be charged with observing only high-value GEO RSOs. According to Mark Bolden, Paul Sydney, and Paul Kervin, "It has been theorized and widely accepted that the bright object population (< 16th VM) is dominated by artificial satellites both active and inactive, while the faint object population is composed mostly of debris."[15] Thus, the study assumed that high-value GEO RSOs, by and large, are brighter than 16th vm. MR3 also differs from that in previous studies since it requires persistent coverage of an RSO. To address this requirement, the study configured the sensors to employ rate tracking of a particular longitudinal band of the GEO belt. Rate tracking affords several advantages, such as an increased probability to detect an RSO during partly cloudy sky conditions; furthermore, it offers the capability to perform sustained-event monitoring during hours of darkness on RSOs of interest. Current optical SSN sensors can observe in rate-track mode but typically operate in sidereal mode in an effort to expand the coverage area with the limited number of telescopes.[16] As a result, existing SSN systems observe each satellite for only seconds per day.

Perpetual rate tracking fulfills MR3 in providing persistence, but it carries a fundamental trade. That is, the surveillance area of the system is static with relation to the GEO belt, leaving the rest of the sky unsurveilled. To overcome this deficiency, one must supply the system as a whole with multiple sensors at multiple sites, each observing a different portion of the belt and spanning its entirety (fig. 2). The total proposed system architecture would employ an array of approximately 60 telescopes at each of the five sites. The list of locations includes the three Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) locations (Maui, Hawaii [1]; Socorro, New Mexico [2]; and Diego Garcia [3]), as well as the planned space surveillance telescope site in Exmouth, Australia (4), and, finally, an additional array on Ascension Island (5). The five locations shown in figure 2 with numbered coverage fans were chosen to address system sustainability and deployability considerations in terms of security, maintenance personnel, and common communications architecture—already established at each of the proposed sites.

Figure 2. Notional sensor coverage for the SADSS network at 33° elevation

From the specifications above, the study chose a design using a Takahashi CCA250 astrograph ($17,000 each) paired with an e2V CCD230-42 camera ($42,000 each) as a reference that meets the system specifications. With mounting and housing costs combined with the equipment, the price per site for 60 sensors totals approximately $3.5 million before installation. By comparison, the GEODSS telescopes cost $3.3 million per site in fiscal year 2000.[17] Therefore, as a rough order of magnitude, acquisition of the two systems is estimated at near cost parity.

Method

Several analyses determined the selection of the system outlined above. First, an analysis of satellite brightness as a function of size, reflectivity, and lighting angle would establish conditions that would yield a 16th vm signal to the observer. To determine a single value for reflectance of a high-value RSO, the study used the reflectance value for multilayered insulation satellite coating. Heather Rodriguez and her colleagues performed a spectral analysis to determine the optical properties of multilayered insulation. Figure 3 shows the reflectance band in the visible spectrum for the insulation sampled.[18] The study assumed a value of 15 percent reflectance and chose a maximum lighting angle (beta angle) of 100° so the system could offer at least 8 hours of continuous track time per night for the purpose of tracking a sufficient orbit length to create highly accurate orbit estimations.[19]

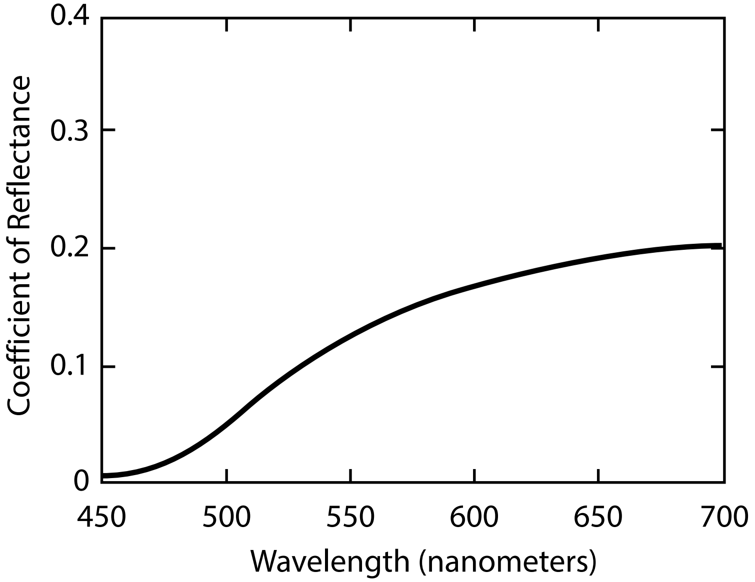


Figure 3. Reflectance of copper-colored Kapton multilayered insulation. (From Heather Rodriguez et al., "Optical Properties of Multi-Layered Insulation" [paper presented at the AMOS Conference Proceedings, Maui, HI, 2007], "fig. 9," [page 9], http://www.amostech.com/TechnicalPapers/2007/Poster/Rodriguez.pdf.)

Next, the study computed the contribution of atmospheric attenuation as a function of elevation angle.[20] From this finding, a reasonable worst-case observing scenario was chosen—specifically, from the Diego Garcia GEODSS site with a minimum viewing angle of 33° elevation with a gibbous moon 45° from the sight line. Though the GEODSS sensors were designed to perform at elevation angles as low as 20°, for the chosen SADSS sites, full global coverage of the GEO belt occurs with a minimum of 33° elevation. With these reasonable worst-case conditions and constraints defined, the study applied radiometric equations to determine that an RSO of four square meters (4 m^2) could be observed at 16th vm (fig. 4).[21]

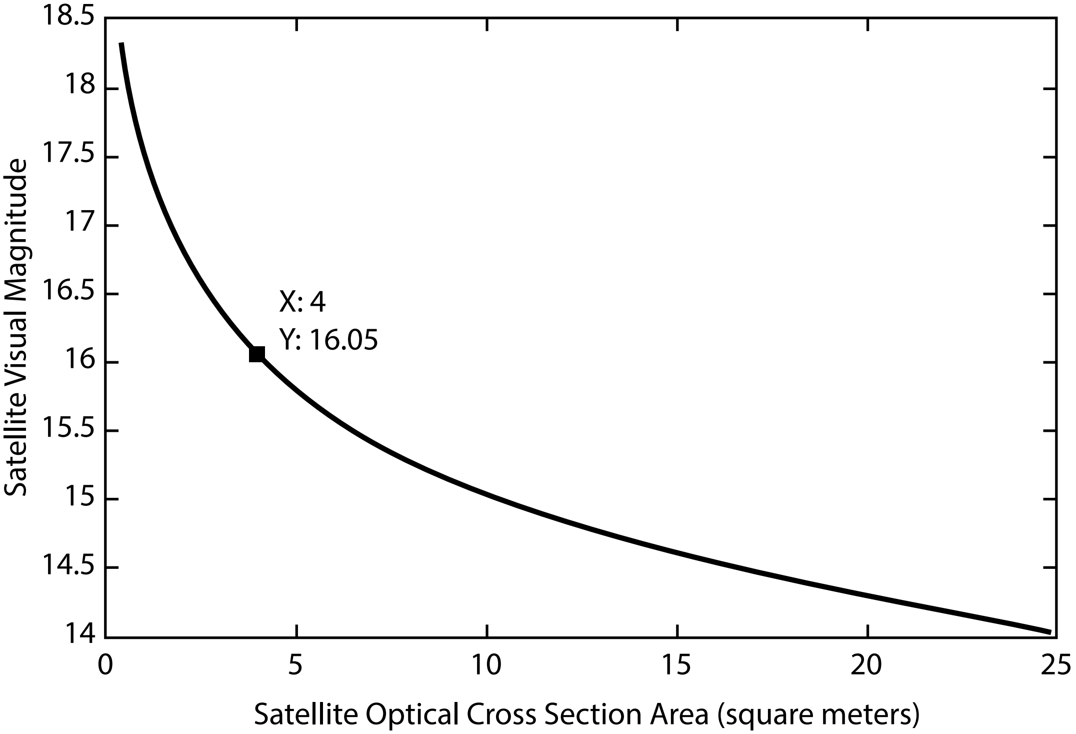
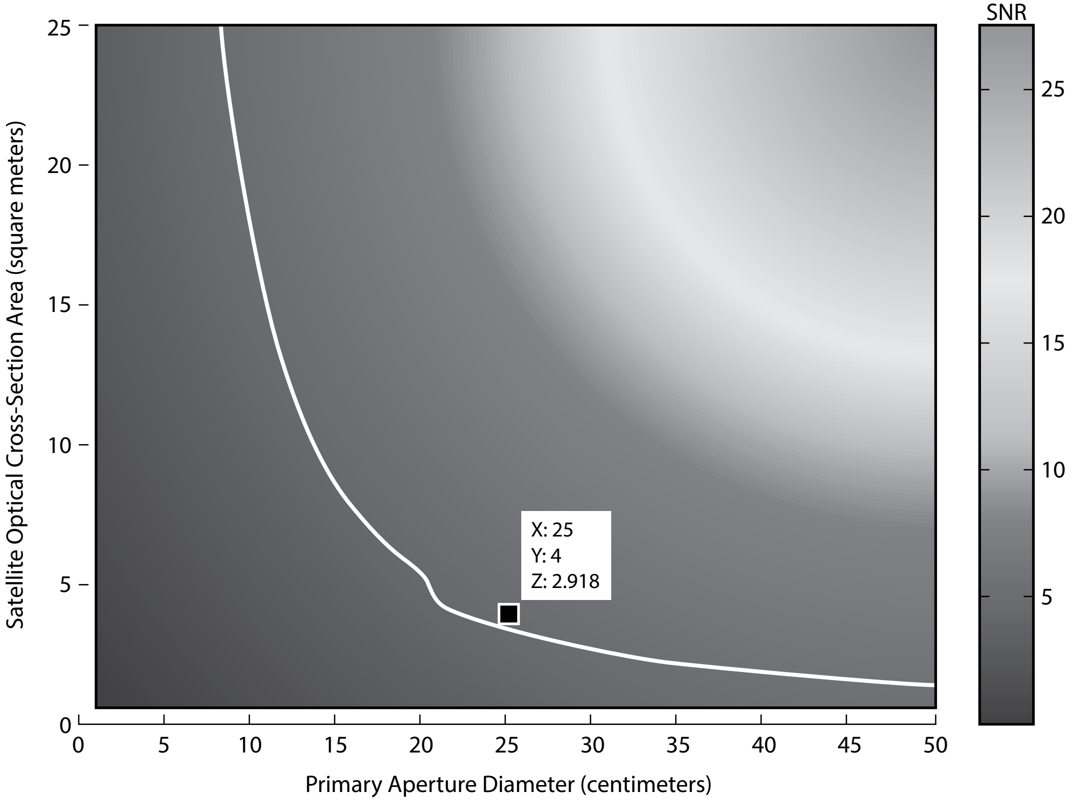


Figure 4. Satellite visual magnitude versus surface area at 100° sun angle

To determine the percentage of GEO satellites that a 4 m^2 detection threshold corresponds to, the study generated a list of GEO RSOs from Space-Track.org and used the McCants radar-cross-section satellite list to cross-reference for radar-cross-section values.[22] The cross-referenced list identified 77 percent of the RSOs to be ≥ 4 m^2 radar cross section.

After applying assumptions and constraints to radiometric equations, the study completed its analysis of the trade space between detectable surface area and primary aperture diameter. The result is shown in figure 5, where the white isoline represents a signal to noise ratio of 2.5—chosen as the minimum threshold for detection.[23] For apertures of 20 centimeters (cm) and below, the study assumed a refracting instrument and, for above 20 cm aperture, applied a reflecting telescope with a 30 percent obscuration, which accounts for the horizontal shift in the line at the 21 cm aperture value. Figure 5 predicts a necessary aperture of 22 cm for detecting a 4 m^2 object. With the common availability of 25 cm COTS optical designs and the margin of performance offered from the reasonable worst-case imaging scenario, the study chose a 25 cm optic. The predicted detection threshold with a 25 cm aperture for a 4 m^2 RSO yields a signal to noise ratio of 2.9. Although the system is designed to track a 4 m^2 object, it is possible to track smaller objects by using a more restrictive sun angle. The maximum angle profile for a 2 m^2 object using a SADSS sensor is estimated to be 81°, still allowing for an annual average of seven hours of track time per night.



SNR = signal-to-noise ratio

Figure 5. RSO surface area versus primary aperture at 100° sun angle

With the system specifications determined and parts selected, the next step involved testing the equipment in an operationally relevant environment. Unfortunately, the institute did not have SADSS-comparable equipment on hand with which to validate its performance. Instead, the existing Air Force Institute of Technology

TeleTrak network of telescopes and computer-control equipment was used to collect the sample observations. The telescope chosen was an Orion 80 mm short tube with a .5 focal reducer / field flattener mated to an Astrovid Stellacam II camera on a Meade LX200GPS mount. Table 3 outlines the difference between the SADSS-proposed sensor and the test article equipment.

Table 3. Differences between SADSS and TeleTrak test equipment

	Cost	*Aperture*	*Sample rate*	*FOV*	*IFOV*	*Time precision*	*Sigma in RA*
SADSS	$70K	25 cm	7.5 sec	1.4° x 1.4°	2.5 arcsec	< ± 0.133 sec	5 arcsec (est.)
TeleTrak	$500	8 cm	1.07 sec	1.2° x 1.6°	5.6 arcsec	± 0.5 sec	11 arcsec

FOV = field of view
IFOV = instantaneous field of view
RA = right ascension

The field of view produced by the optical camera assembly is approximately 1.2° x 1.6° with an angular pixel resolution of 5.6 arcseconds/pixel. This field of view was chosen deliberately to ensure that the images would contain a sufficient number of bright reference stars for the software algorithms to accurately and repeatedly produce results for the location of RSOs relative to the inertial reference frame provided by the background stars—a process known as astrometry. From the astrometry-corrected images, topocentric right ascension and declination angles of detected RSOs are measured by using the highly precise positions of known background stars in the captured images. From these observations, one can perform an orbit determination.

First, a highly accurate star catalog is needed for a baseline reference to the celestial sphere. The stars in the image must then be identified by comparing their positions and relative intensities to each other and then comparing the orientation pattern to the known star catalog for a match. When the telescope is tracking in sidereal mode, the stars in the image can be chosen judiciously to make this identification simpler. However, in rate-tracking mode, the star field is continuously changing, and the use of star-matching software, such as that provided by astrometry.net, can be highly advantageous to aid in processing large data sets with unknown star fields.[24] Once the star field is identified, multiple coordinate transformations must then take place to create an observation in an Earth-centric inertial reference frame, which then allows it to be applied for orbit-determination purposes.

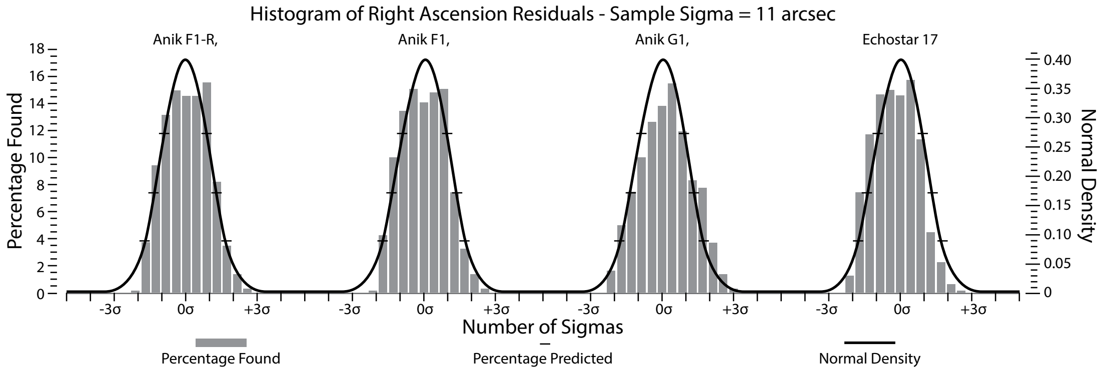
Maintenance of interoperability and compliance with the SSN's standard message format for optical observations, known as a B3 report, require transformation of the topocentric right ascension and declination angular measurements into a South-East-Zenith right-handed orthogonal coordinate system. The angular measurements from this coordinate system are reported as azimuth and elevation angles centered on the observing sensor's location—shown in Vallado's Algorithm 28.[25] Operationally, the JSpOC receives the metric observation report in the sensor's local azimuth and elevation reference frame. These angles are then transformed to an Earth Centered Inertial reference frame. Once in the frame, the most recent TLE for the RSO is applied for comparison with the measurements, and the initial residuals are generated.

From there, the Simplified General Perturbations version 4 (SGP4) algorithm used by AFSPC to differentially correct orbit estimations can be executed, using the new measurements to create an updated TLE. For the research herein, the majority of these steps applied. However, Analytical Graphics Incorporated's Orbit Determination Tool Kit software allows for ingestion of the ground-based right ascension and declination observations in the topocentric reference frame directly with knowledge of the observing site's location. Doing so eliminated the need to manually apply Vallado's algorithms to the observations, thus decreasing the complexity of the processing chain.

In gathering the observations for processing and orbit determination, the study used two observing campaigns. The first, which took place from 26 October 2014, determined the sensor precision, and the second, which occurred over three consecutive nights spanning 16–18 January 2015, was used to perform orbit-determination comparison with JSpOC TLEs. The observing target was the *Anik F1* cluster, located at an elevation of 38° in the southwest portion of the sky from Dayton, Ohio. The cluster consists of the *Anik F1*, *Anik F1-R*, and *Anik G1* satellites. *Echostar 17* leads the Anik cluster by 0.2° in right ascension and was also observed in the field of view. All four of these satellites are relatively large communications satellites.

Results

From the 26 October 2014 data set, the study determined sensor precision values in both the right ascension and declination components for each of the four satellites across all 17,000 valid observations extracted from the 19,000 images (figs. 6 and 7). The right ascension sigma (fig. 6) indicates a secondary systemic error which is presumed to be primarily caused by timing.



arcsec = arcseconds

Figure 6. Sigma histogram of right ascension residuals from 26 October 2014

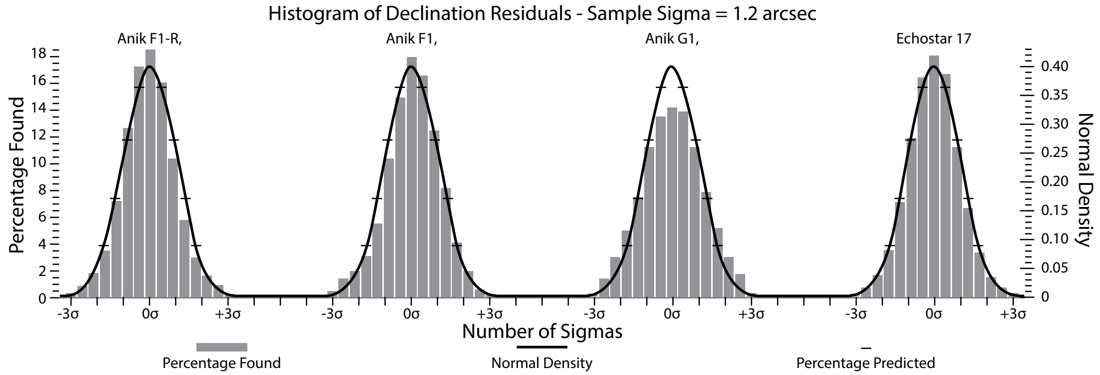


Figure 7. Sigma histogram of declination residuals from 26 October 2014

From the January observing campaign, the ephemeris generated from the 8,000 observations sampled once per 10 seconds shows good correlation to the corresponding JSpOC TLEs. In performing the differential corrections, the study showed that all four of the tracked RSOs converged on a solution directly from the JSpOC's most recently published TLE. Each least squares orbit determination run was initialized using the JSpOC TLE, and each came to a convergence with close resemblance to the TLE. A comparison between the initial TLE and the least squares solution from the TeleTrak observations is shown in table 4. Figures 8 and 9 depict the relative change in position over 24 hours between the generated ephemeris from the test data (EPH) and the JSpOC published TLE. The differential drift rate was reduced by an order of magnitude over test case 2, which saw a difference of about 10 kilometers in semimajor axis between the TLE and the ephemeris. Figure 10 shows how the propagation error grows over the two days after the last observation on the untracked, daylight side of the orbit. The viewing perspective for the following figures was set to a few hundred kilometers above the GEO belt and centered between *Echostar 17* and the Anik cluster. Thus, the relative size of the JSpOC GEO TLE error ellipsoid in figures 8 and 9 is greatly exaggerated with respect to Earth.

Table 4. Ephemeris and TLE comparison from January 2015

SATNO	*Source*	*Epoch*	*Semimajor axis*	*Eccentricity*	*Inclination°*	*RAAN°*	*Arg. of Per.°*	*Arg. of Lat.°*
Anik F1 26624	EPH	16:56:28.395	42166.568 km	0.000341	0.09945	85.22445	100.942810	176.29852
	TLE	16:56:28.395	42165.510 km	0.000083	0.10455	88.00984	180.45842	173.45326
Anik F1R 28868	EPH	16:08:05:930	42166.947 km	0.000207	0.08719	62.59837	201.86272	186.73179
	TLE	16:08:05:930	42165.673 km	0.000276	0.09258	70.54715	266.02396	178.74061
Echostar 17 38551	EPH	09:05:20.377	42164.987 km	0.000295	0.09836	77.39478	185.73116	66.11604
	TLE	09:05:20.377	42165.708 km	0.000253	0.10981	19.17635	201.20691	64.34500
Anik G1 39127	EPH	16:16:29.058	42165.067 km	0.000211	0.09797	75.94122	242.24602	175.41940
	TLE	16:16:29.058	42165.427 km	0.000332	0.07944	75.28374	217.96316	176.11927

SATNO = satellite number
RAAN = right ascension of the ascending node
Arg. of Per. = Argument of Perigee
Arg. of Lat. = Argument of Latitude

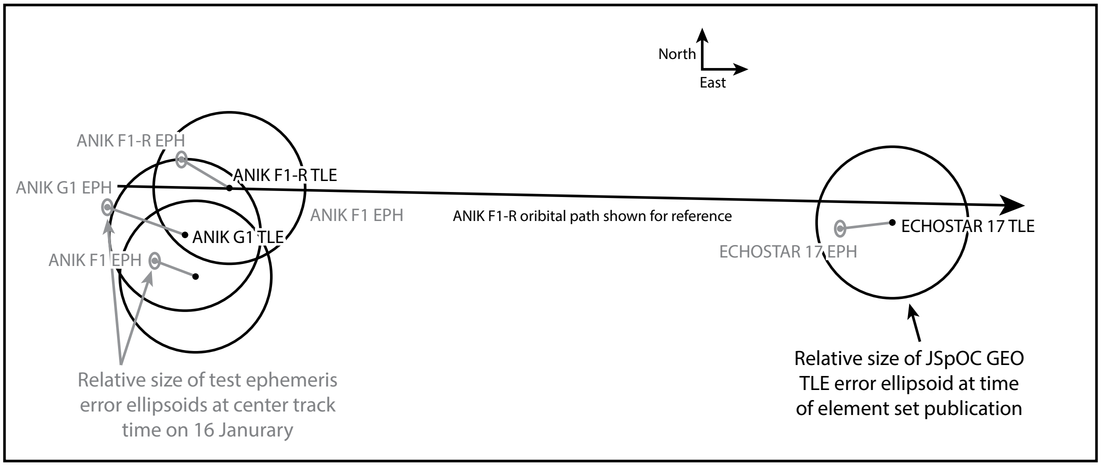


Figure 8. TLE versus ephemeris at center track time on 16 January 2015

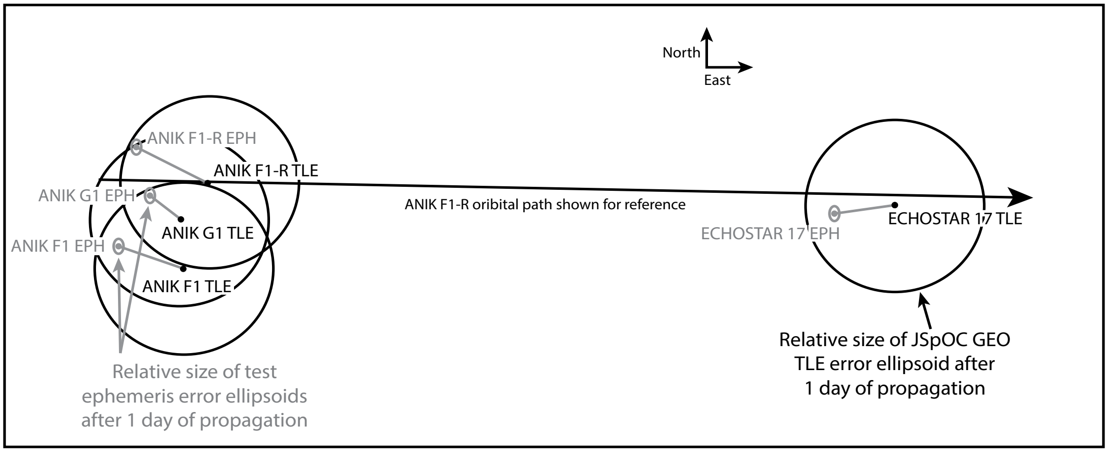


Figure 9. TLE versus ephemeris at center track time on 17 January 2015

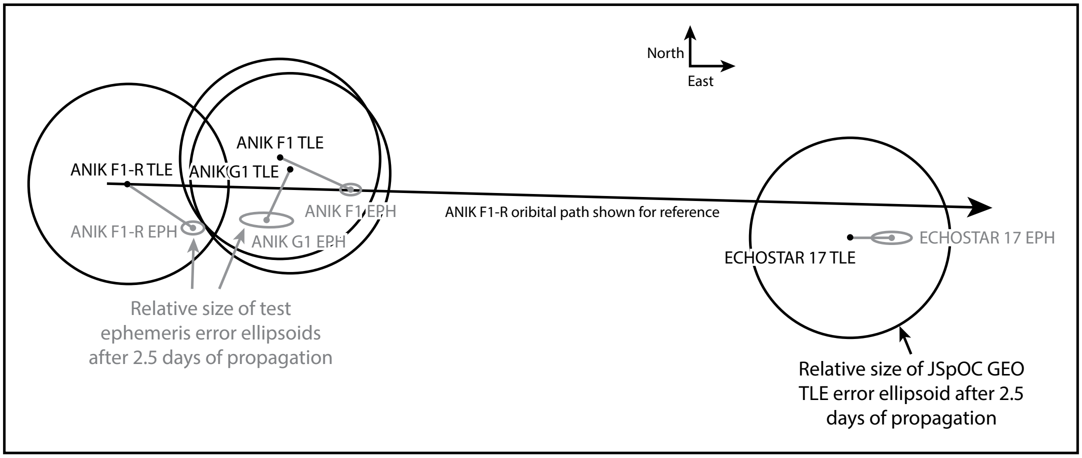


Figure 10. TLE versus ephemeris after 2.5 days of propagation

These test cases produced a proof of concept capable of processing observations from the COTS hardware using only COTS software semiautonomously. In doing so, the JSpOC TLEs were effectively re-created to the average accuracy limits of GEO TLE with only two or three nights of observations. The potential for improvement by performing a similar study over a month's worth of tracking is encouraging. Because of the relatively low fidelity of the TLEs and the lack of transparency of the Analytical Graphics Incorporated special perturbations orbit-determination algorithm and the way it compares to SGP4, though, the causality of the delta between the TLE and the element set created from the test data remains unknown but is probably a mixture of timing accuracy and algorithm mismatch. However, if the SADSS program were to come to fruition, a more comprehensive operational test could be conducted using the current operational algorithms to reduce the unknown errors and come to a more thorough understanding of system performance and its capacity to off-load tasking from the existing optical SSN sensors.

Given the presumption that each object requires an epoch update every 24 hours and that GEODSS is tasked to collect the observations in its normal operational mode, a metric for the GEODSS sensor off-load time can be generated. Assuming an even load across all 9 GEODSS telescopes tracking the 556 SADSS observable satellites, this equates to an average tasking off-load rate of 62 taskings per telescope, requiring 248 observations per night. With a peak generation rate of 116 observations per hour, 2 hours of track time for each telescope could be made free—or 18 observing hours per night of reduced tasking for the GEODSS system as a whole. Given 300 SADSS sensors, each with a 1.4° field of view in rate track mode (15° per hour) and tracking an annual average of 10.5 hours per 24-hour period, the total SSA surveillance rate could be increased by 2,750 degrees squared per hour while also offering much higher persistence for precision orbit determination and event monitoring at a comparable equipment dollar cost to GEODSS.[26]

Conclusions and Future Work

In an attempt to address the AFSPC commander's visions and goals for achieving SSA in the scope of the GEO case, this study developed and tested a system specification to show performance that could observe spherical, low-reflectance GEO RSOs as small as 2 m^2 at an 81° beta angle and 4 m^2 objects out to a 100° beta angle. From a much less capable test system, the study created a method to semiautonomously generate right ascension and declination metric observations. The observation accuracies were found to be 11 to 17 arcseconds in right ascension and 1.2 to 2 arcseconds in declination.

From three nights of TeleTrak observations, element sets were differentially corrected directly from the JSpOC's published TLEs. The corrected orbit estimations had an in-track median covariance of 570 meters at the time of publication and a median vector magnitude with respect to the TLE that was roughly equal to the average accuracy limits of a GEO TLE while utilizing only 5–10 percent of the time span typically used by the JSpOC to generate its GEO TLEs.

Although this result is encouraging, fully answering the research question of *whether a large-scale employment of small-aperture COTS telescopes can augment the SSN's observing capacity of the geostationary belt without degrading the quality of orbit estimations* requires further study. An attempt should also be made to validate the sensor sigma and bias values using the operational sensor calibration processes through the AFSPC A2/3/6SZ office. A SADSS system requirement of 0.133-second timing precision requires at least a factor of four improvement. Ultimately, though, collecting observations from a SADSS-like sensor from one or more of the proposed Department of Defense sites over an entire lunar or maneuver cycle is desirable.

More in-depth trade analysis of the mission needs is also desirable. Such an analysis could address a variety of existing COTS hardware components, mixing and matching parts to find a more optimal solution to satisfy the established requirements. Furthermore, by examining the design over varying observing conditions such as elevation and RSOs known to inhabit a particular sensor field of view, a multipoint design analysis could help to further minimize the cost of the network by employing lower-cost systems along more favorable sight lines.

The overall program cost also needs further investigation and refinement. Provided here was a simple, rough order of magnitude cost for most of the equipment, neglecting installation, computer processing, and operation and maintenance expenses. With a refined program acquisition and sustainment cost, alternative analysis could then determine if building a SADSS network is the best choice for the funds allocated to AFSPC to carry out the GEO SSA mission.

If the Air Force is to formally acquire the system proposed here, then other considerations not discussed within the scope of this effort must be addressed. Such considerations include funding, development, and developmental and operational testing of the system to verify and validate its performance against the system requirements. The developing System Program Office, the Air Force Operational Test and Evaluation Center, and/or the 17th Test Squadron would likely perform these actions, once tasked by AFSPC. To ensure that the data ingested into the SSA mission could be trusted, the AFSPC A2/3/6ZS number validation office would need to actively monitor sensor calibration, as occurs with all other SSN sensors. The other logistical considerations, such as security, communications, and maintenance plans previously discussed, are also prerequisite to operationalization of the system. However, it is presumed that the risk of these issues would have been partially mitigated by co-locating the SADSS sensors with other actively operated government optical systems. Still, a more in-depth analysis of these considerations should occur prior to moving forward to acquire the system.

Regardless of the chosen solution, the Air Force needs to solve the problem of SSA in order to create and maintain an accurate common operating picture for space. As the mission requirements for achieving and maintaining SSA continue to grow, so will the resource demands to conduct the mission. The questions then become, What is being done now, and what needs to be done to address the needs of today and the problems of tomorrow? ✪

Notes

1. Patrick J. Payte, “Orbit Determination and Prediction for Uncorrelated Target Deterction and Tracking” (MS thesis, Department of Aeronautics and Astronautics, Air Force Institute of Technology [AFIT], Wright-Patterson AFB, OH, 2008); Christine M. Schudrowitz, “The Effects of Observations and Maneuvers on Oribt Solutions” (MS thesis, Department of Aeronautics and Astronautics, AFIT, Wright-Patterson AFB, OH, 2012); and Committee for the Assessment of the US Air Force’s Astrodynamic Standards, *Continuing Kepler’s Quest: Assessing Air Force Space Command’s Astrodynamics Standards* (Washington, DC: National Academies Press, 2012).

2. Headquarters Air Force Space Command / Space Situational Awareness, Command and Control Operations, and Integration Branch (A3C), *Enabling Concept for Space Situational Awareness (SSA)* (Peterson AFB, CO: Headquarters Air Force Space Command/A3C, October 2007).

3. Ibid., 8. See also Payte, “Orbit Determination and Prediction.”

4. The apparent visual magnitude (vm) scale is such that the higher the value, the dimmer the object. Each integer increase in order, such as first to second vm, is a decrease in visual brightness by a factor of two-and-a-half. For more information, see “The Astronomical Magnitude Scale,” *International Comet Quarterly*, accessed 17 September 2015, http://www.icq.eps.harvard.edu/MagScale.html.

5. Mark Bolden, Paul Sydney and Paul Kervin, “Pan-STARRS Status and GEO Observations Results” (paper presented at the Advanced Maui Optical and Space Surveillance Technologies [AMOS] Conference Proceedings, Maui, HI, 2011), http://www.amostech.com/TechnicalPapers/2011/Orbital_Debris/BOLDEN.pdf.

6. Committee for the Assessment of the US Air Force’s Astrodynamic Standards, *Continuing Kepler’s Quest*, 18; and Bolden, Sydney, and Kervin, “Pan-STARRS Status.”

7. Committee for the Assessment of the US Air Force’s Astrodynamic Standards, *Continuing Kepler’s Quest*, 2–3.

8. Anthony D. Gleckler and Michael C. Butterfield, “Viral Space Situational Awareness” (paper presented at the AMOS Conference Proceedings, Maui, HI, 2012), http://www.amostech.com/TechnicalPapers/2012/Data_Services/GLECKLER.pdf.

9. Daniel Moomey, “Aiding Geostationary Space Situational Awareness Using Small Aperture Commercial Telescopes“ (MS thesis, Department of Aeronautics and Astronautics, AFIT, Wright-Patterson AFB, OH, 2015), 3.

10. Headquarters Air Force Space Command/A3CD, *Enabling Concept*, 12, 22–24.

11. Ibid., 14.

12. Ibid., 10.

13. “US Naval Observaroty Master Clock,” US Naval Observatory, accessed 30 July 2014, http://tycho.usno.navy.mil/what.html; and “NIST Internet Time Service (ITS),” National Institute of Standards and Technology, US Department of Commerce, accessed 30 July 2014, http://www.nist.gov/pml/div688/grp40/its.cfm.

14. Moomey, “Aiding Geostationary Space Situational Awareness.”

15. Bolden, Sydney, and Kervin, “Pan-STARRS Status,” [1].

16. Walter J. Faccenda, "GEODSS: Past and Future Improvements," MITRE Corporation, 2000, https://www.mitre.org/sites/default/files/pdf/geodss_faccenda.pdf.

17. A. Thompson, "A GEODSS Sourcebook," 19 October 2008, http://www.fas.org/spp/military/program/track/geodss.pdf.

18. Heather Rodriguez et al., "Optical Properties of Multi-Layered Insulation" (paper presented at the AMOS Conference Proceedings, Maui, HI, 2007), http://www.amostech.com/TechnicalPapers/2007/Poster/Rodriguez.pdf.

19. Joshua T. Horwood, Aubrey B. Poore, and Kyle T. Alfriend, "Orbit Determination and Data Fusion in GEO" (paper presented at the AMOS Conference Proceedings, Maui, HI, 2011), http://www.amostech.com/TechnicalPapers/2011/Astrodynamics/HORWOorbit determination.pdf.

20. Carolin Früh and Moriba K. Jah, "Detection Probability of Earth Orbiting Objects Using Optical Sensors," *Advances in Astronautical Sciences* 150 (2014): 13; W. Jody Mandeville et al., "Sky Brightness Analysis Using a Million Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) Observations" (paper presented at the AMOS Conference Proceedings, Maui, HI, 2012), http://www.amostech.com/TechnicalPapers/2012/POSTER/MANDEVILLE.pdf; and Kevin Krisciunas and Bradley E. Schaefer, "A Model of the Brightness of Moonlight," *Astronomical Society of the Pacific*, no. 103 (1991): 1033–39.

21. Früh and Jah, "Detection Probability"; Steve B. Howell, *The Handbook of CCD Astronomy*, 2nd ed. (Cambridge, UK: Cambridge University Press, 2006), 73; and Ryan D. Coder and Marcus J. Holzinger, "Sizing of a Raven-Class Telescope Using Performace Sensitivities" (paper presented at the AMOS Conference Proceedings, Maui, HI, 2013), http://www.amostech.com/TechnicalPapers/2013/Optical_Systems/Corbit determinationER.pdf.

22. JFCC SPACE/J3, "Space-Track.org," Air Force Space Command, 28 January 2015, https://www.space-track.org/#/queryBuilder; and Mike McCants, "Mike McCants' Satellite Tracking Web Pages," 5 September 2014, https://www.prismnet.com/~mmccants/programs/qsmag.zip.

23. Früh and Jah, "Detection Probability."

24. "Astrometry.net," US National Science Foundation, US National Aeronautics and Space Administration, and the Canadian National Science and Engineering Research Council, 2015, http://www.astrometry.net/.

25. David Anthony Vallado and Wayne D. McClain, *Fundamentals of Astrodynamics and Applications*, 4th ed. (El Segundo, CA: Microcosm Press, Kluwer Academic Publishers, 2013), 272.

26. Robert F. Bruck and Capt Robert H. Copley, USAF, "GEODSS Present Configuration and Potential" (paper presented at the AMOS Conference Proceedings, Maui, HI, 2014), http://www.amostech.com/TechnicalPapers/2014/Poster/BRUCK.pdf; and Thompson, "A GEODSS Sourcebook."

Capt Daniel Moomey, USAF

Captain Moomey (BA, University of Toledo; MS, Air Force Institute of Technology) serves on active duty in the United States Air Force. He is a flight commander for the 17th Test Squadron at Schriever AFB, Colorado, overseeing operational testing and evaluation of US Air Force space systems. His previous assignments include a one-year tour overseas to Thule, Greenland, as a crew commander for the 12th Space Warning Squadron where he performed space surveillance and missile warning duties. Captain Moomey served as the space battle manager and operations liaison to the Unified Space Vault at the Joint Space Operations Center, performing space situational awareness duties. He was selected to rebuild, reinitiate, instruct, and administrate Air Education and Training Command's space surveillance training course for the 533rd Training Squadron at Vandenberg AFB, California. He then was competitively selected to attend the Air Force Institute of Technology at Wright-Patterson AFB, Ohio, where he completed an MS degree in space systems. Captain Moomey is coauthor of "Revisiting the Chlorine Abundance in Diffuse Interstellar Clouds from Measurements with the Copernicus Satellite," *Astrophysical Journal* 744, no. 2 (January 2012): 1–7.

Let us know what you think!
Leave a comment!

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

Purposeful Development of the Intelligence, Surveillance, and Reconnaissance *for* Space Cadre

SMSgt Mitchell R. Overton, USAF*

> *Protecting space assets is critical to AF ISR operations and the nation's full spectrum joint operations. Purposefully developing ISR Airmen who understand ISR for and from space is the initial step we will take to ensure this critical capability.*
>
> —Lt Gen Robert P. Otto

The Air Force recognizes three domains—air, space, and cyberspace. Of these domains, a war in space is the least likely and certainly the least desired for two reasons. First, the Outer Space Treaty of 1967, signed and ratified by 103 countries, including the United States, acknowledges the common interest of using outer space for peaceful purposes. Those states that agreed to the treaty forbade placing weapons in orbit around the earth and held liable the state whose space launch caused damage to another state's property on the earth or in air, space, or outer space.[1] Second, military commanders enjoy virtually uninhibited, uninterrupted access to space, leaving the war fighter to believe that space capabilities will always be available. For these reasons, an attack on US space assets seems an unlikely scenario. However, the threat to space has changed since 1967. Enhanced and readily available counterspace capabilities threaten the survivability of military space systems. Despite this reality, threats to space are not treated with the same level of severity as those to the air and cyberspace domains. The Commission to Assess United States National Security Space Management and Organization (also known as the Space Commission), chaired by former secretary of defense Donald H. Rumsfeld, published a report on 11 January 2001 asserting that "the U.S. is more dependent on space than any other nation. Yet, the threat to the U.S. and its allies in and from space does not command the attention it merits from the departments and agencies of the U.S. government charged with national security responsibilities.

---

*This article would not have been possible without the invaluable thoughts and perspectives provided by Col Gay "Charlie" McGillis, USAF, retired, and SSgt Marie L. Foster, USAF.

Consequently, evaluation of the threat to U.S. space capabilities currently lacks priority in the competition for collection and analytical resources."[2] Although progress has been made, the commission's findings remain relevant 14 years later.

During a visit to Buckley AFB, Colorado, in December 2014, Gen John E. Hyten, commander of Air Force Space Command (AFSPC), stressed a mind-set of constant protection and the importance of recognizing and acting on the threat to space: "To be honest, the folks who work here on our operations floor and the folks who work at the (50th and 21st Space Wings), don't think very much about these threats today because we still have a mindset that space is a benign environment. It is not."[3] For example, a nondirected nuclear antisatellite attack—the most devastating threat to space—is possible for rogue nations who possess a launch vehicle and nuclear weapon. If carried out successfully, such a strike could eliminate critical national defense satellites. Rogue nations like Iran and North Korea have neither ratified (Iran) nor signed (North Korea) the Outer Space Treaty, but they possess launch vehicles and have, or intend to have, a nuclear capability. In addition to a nuclear threat, less technologically advanced options such as satellite jamming and space ground-segment attacks are relatively inexpensive and plausible. The ability to anticipate potential attacks requires predictive analysis that enables a commander's decision making either to eliminate a threat or mitigate its effects.

The existence of such threats will shorten the space commander's decision cycle. His or her ability to detect and act on a threat must be enhanced from the tactical, operational, and strategic levels. Toward this end, the Air Force must improve its threat analysis and develop effective countermeasures. Analysis is driven by a demanding customer, one who understands the commander's intelligence requirements and can translate them into the form of intelligence needs or requests for information, which in turn drives the intelligence community's efforts. Countermeasures in the form of tactics, techniques, and procedures are developed only if timely, relevant intelligence is delivered to the operational space unit. Improved analysis of space threats and countermeasures can occur by enhancing the capabilities of the Air Force's most critical asset—its intelligence Airmen. This article identifies gaps in the Air Force's current force-development construct for the ISR *for* space Airman. It seeks to recommend improvements that the Air Force's space and ISR communities can make in the education, training, and experience of its ISR *for* space Airmen. These recommendations are designed to purposefully develop ISR *for* space professionals who are better educated, better trained, and more experienced to support space and to protect and defend efforts.

Gaps in Intelligence, Surveillance, and Reconnaissance *for* Space Development

During his speech to the 2013 Air Force Association's Air and Space Technology Exposition, Lt Gen Robert P. Otto, deputy chief of staff for intelligence, surveillance, and reconnaissance, stressed the "need to leverage the experience of our people and develop a cadre of ISR professionals that can answer the unique questions associated with these increasingly congested and contested domains."[4] The knowledge and ability of our Airmen to provide ISR *from* space—ISR collected from space-based assets—is well established. However, the development of ISR Airmen *for* space—those Airmen capable of addressing ISR requirements to protect and defend space assets—is not and must keep pace with this rapidly changing domain. If force development for space ISR remains the same, the Air Force, over time, will find itself unable to adequately confront unique questions of the operational space commander—most notably, the commander of the Joint Functional Component Command for Space. According to the Space Commission report, "As space education, career development and training in the Department of Defense are enriched, a cadre of space professionals will develop."[5] It is paramount that the Air Force create a purposeful force-development path that enhances the capabilities of its ISR *for* space professionals.

The current force-development path for intelligence Airmen falls short of fulfilling the ISR demands of AFSPC and the war fighters it supports. Consider the following scenario if intelligence Airmen within Air Combat Command (ACC) received the same level of education, training, and experience as those in AFSPC.

Airman First Class Johnson, a 1N031 operations intelligence apprentice, arrived at her first duty station supporting the F-16 weapon system. Technical school did not prepare her to support this mission. Her instructors primarily had space experience—the focus of her three-level training. An F-16 intelligence formal training unit (IFTU) did not exist. Instead, an Air IFTU provided a basic overview of ACC and its missions.

Technical Sergeant Smith is an experienced 1N071 operations intelligence craftsman. His previous two assignments supported the Space-Based Infrared System and the Defense Support Program. Like Airman Johnson's assignment, this is his first one supporting an air-based weapon system. Despite his lack of knowledge and experience, Sergeant Smith was the F-16 intelligence-support subject-matter expert for a recent exercise. After the exercise, he was deemed incompetent because of his lack of F-16 knowledge and the way it could support the primary Air Force mission of protecting space assets. Sergeant Smith is relieved that his next assignment will be at the Joint Space Operations Center (JSpOC) and will return him to a more traditional ISR assignment.

Captain Wallace, a 14N intelligence officer, is Airman Johnson's and Sergeant Smith's officer in charge. A Weapons School graduate, she predominantly had exposure to intelligence support for space but little else. Captain Wallace tried to incorporate space-targeting practices into local procedures but has faced resistance to her proposed changes. She attempted to have Technical Sergeant Smith enrolled in the Air Force Weapons School's Advanced Enlisted Mission Planning Course (AEMPC) but was unable to do so because of a lack of ACC funding. The course primarily focuses on space systems—none of the AEMPC instructors have air domain experience. She made strides in improving weapons and tactics support for the F-16 but realizes that it falls short of the weapon system's ISR requirements. This frustration will be temporary since officers do not typically receive successive air assignments.

As the director of ISR for ACC for a year now, Brigadier General Stevens is just starting to understand the challenges that Colonel Lopez, his numbered air force A2, faces in delivering the necessary ISR support to the air component commander. Along with Chief Lee, the enlisted intelligence functional manager for the major command, they have been successful in incorporating air domain knowledge into technical school training and even *established an air IFTU within the command. However, the fact that the dominant percentage of Airmen across the Air Force does not support an air mission makes it difficult to incorporate necessary air domain knowledge into ISR technical training and career-field education and training. Brigadier General Stevens and Colonel Lopez, both prior commanders, never served in an ACC assignment. They rely heavily on experts like Captain Wallace and her team to get them up to speed on issues that affect ISR support to ACC weapon systems.*

Context

The above scenarios would seem unthinkable to ACC but are very much a reality for Airmen entering their first—and many times, only—AFSPC assignment. These Airmen are faced with

- technical school that does not adequately prepare them for their first space mission;
- an IFTU that does not provide in-depth knowledge of the adversary threat and weapon system capability;
- inadequate knowledge of space domains, exposed in major exercises because the necessary education, training, and experience do not exist;
- subject-matter expertise that fails to grow because of an all-too-common "one and done" space assignment rotation; and
- the assignment of senior intelligence leaders with no previous space experience to lead their command's ISR directorate.

Would this situation be acceptable in the air world? Most Airmen would probably answer this question with a resounding "No!" Will this situation continue to be accepted in the space domain? This question may best be answered with the question "How did we get to this point?"

Force Development

Force development is designed to be a dynamic, deliberate process that builds institutional and occupational competencies in Airmen through education, training, and experience. Occupational competencies, the focus of this article, develop through specialized training relative to an Airman's Air Force specialty code (AFSC). Additionally, force development leverages the continuum of learning, a career-long process of individual development whereby challenging experiences combined with education and training produce Airmen with the tactical expertise, operational competence, and strategic vision to lead and execute the full spectrum of Air Force missions.[6]

The building of occupational competencies begins at an AFSC-awarding course. Development continues at the middle pay grades, where skill-level enhancement takes place through a mix of advanced education, training, and experience. Airmen fully mature within the continuum of learning at the senior officer and senior noncommissioned officer (NCO) ranks, becoming leaders who drive the Air Force's strategic vision. Improving occupational competencies through education, training, and experience is necessary to enhance the capabilities of the ISR *for* space professional. However, certain roadblocks prevent the Air Force from getting there.

In accordance with Air Force Instruction (AFI) 36-2623, *Occupational Analysis*, skill-level training must emphasize only those training tasks performed by 30 percent or more of the personnel within a career field.[7] The number of ISR Airmen assigned to support AFSPC or other space missions is not substantial enough to incorporate ISR *for* space training in technical school and does not warrant the creation of advanced space ISR courses. This gap in knowledge is somewhat closed through a series of AFSPC-provided initial qualification training, space intelligence formal IFTU (SIFTU), and unit-led mission qualification training.[8] Additionally, AFSPC's Advanced Space Operations School (ASOpS) and Air Education and Training Command's National Security Space Institute (NSSI) offer various educational opportunities for ISR Airmen, but these courses are not mandatory. Space education and training provided by the ASOpS and NSSI are not designed to develop an ISR *for* space professional.

The approximately 1,611 enlisted active and Reserve ISR personnel within AFSPC make up 46 percent of the total enlisted force within the command; enlisted active and Reserve space operators represent 1,506 or 43 percent of the enlisted force within AFSPC; and the command includes 581 intelligence officers—9 percent of the total officer force compared to the 3,380 space officers or 52 percent of AFSPC's total officers.[9] Understandably, education and training within AFSPC is geared toward development of the 4,886 space AFSCs—easily the majority of personnel within the command. However, the contributions that are being made and those yet to be realized for the 2,192 ISR Airmen are—and will continue to be—critical in protecting our nation's space assets. If Airmen do not receive the necessary ISR *for* space education and training within technical school, ASOpS, or NSSI courses, where do they obtain them?

The reality is that required space education and training for ISR Airmen do not exist and that investments are not being made in cultivating experienced ISR *for* space professionals. The lack of a structured career path for such professionals, as evident in the common "one and done" assignment pattern, has done little to enrich the ISR curriculum in space education and training courses. Additionally, it has not sparked the creation of more advanced ISR training opportunities for Airmen within the command. Quite simply, deliberate force development for the ISR *for* space Airman does not exist.

Further Examination

The table below depicts a small sample of Airmen within AFSPC, including but not limited to space control, space warning / situational awareness, space command and control, and various leadership positions. This sampling is indicative of the ISR force structure within the command. The few junior officers and enlisted

Airmen entering their first assignment do not receive the necessary education and training in AFSC-awarding training and certainly do not have the experience as newly minted technical school graduates. They often look to the more seasoned ISR Airmen in the O-3 to O-4 and E-4 to E-7 pay grades to prepare them for their first space assignment. However, these Airmen are in the same boat—no previous space education, space training, or space experience. In essence, the majority of AFSPC ISR Airmen are going through the same thing—learning ISR *for* space for the first time. By the time these Airmen have learned and advanced their space skills, they are on to more "traditional" ISR assignments, slowing progress toward evolving development of the ISR *for* space Airman. Very few ISR Airmen are retained within AFSPC after their first assignment and are unable to fully develop at the operational level or even approach the strategic level of expertise.

Table. Billet structure for space ISR

Officer	*14N*	*Enlisted*	*1N*
O1–O2	7	E1	0
O3	29	E2	0
O4	36	E3	8
O5	16	E4	22
O6	5	E5	75
		E6	56
		E7	33
		E8	9
		E9	1
Total	93	Total	204
Grand Total 297			

Enhancing education, training, and experience of the ISR *for* space professional is supported by the *National Security Space Strategy*, which acknowledges people as the nation's greatest asset. Consistent with Lieutenant General Otto's commitment to strengthening the ISR *for* space cadre, the strategy calls for the development of "current and future national security space professionals . . . who can acquire capabilities, operate systems, analyze information, and succeed in a congested, contested, and competitive environment." The strategy also calls for focused education and training as well as purposeful utilization of personnel, specifically by enabling and developing "intelligence professionals who can provide greater scope, depth, and quality of intelligence collection and analysis."[10] Purposeful development of the 2,192 ISR Airmen within AFSPC is needed to follow the direction provided by the *National Security Space Strategy*.

The Road Map—How to Get There

Force development addresses common principles for education, training, and experience within the Air Force: build skill-set expertise, prepare for change, create depth of expertise, train to mission demands, train like we fight, make education and training available, and validate education and training through war games and exercises.[11] In terms of education and training, the tactical level of expertise is traditionally developed in recently commissioned officers and junior enlisted pay grades when these Airmen receive primary skill training. The operational level of expertise can be found within the O-3 and E-5-and-above pay grades; education for those Airmen concentrates on furthering expertise, and training builds operational and tactical skills and professional competence. Airmen who are O-5s and above, as well as E-9s and a select few E-7s to E-8s, make up the strategic level of expertise, where education emphasizes institutional, joint, interagency, business, and international views. Education and training are validated through exercises and war games.[12] Following the guiding principles of senior leadership, the Space Commission report, the *National Security Space Strategy*, and force development, the Air Force can establish a career road map to better develop ISR *for* space Airmen at the tactical, operational, and strategic levels.

Recommendation 1: Improve Current Education and Training Programs to Build Requisite Expertise

Initial skill and follow-on training for ISR Airmen traditionally addresses the air domain or a specific intelligence discipline respective to an AFSC. This training is beneficial in establishing the foundational knowledge to be successful in assignments that dictate the preponderance of the course curriculum, but it ill prepares Airmen to succeed at their first space assignment. Although progress occurred by introducing space to initial and follow-on education and training curricula, the subject must be enhanced to adequately prepare ISR Airmen to support the space commander.

To keep pace with the rapidly changing space environment, ISR *for* space professionals must have education and training that hone their tactical, operational, and strategic expertise. With the exception of SIFTU, no ISR courses prepare the ISR *for* space Airman. The current SIFTU course is appropriate for acquiring basic knowledge, but it does not provide the necessary familiarity with space systems. A unit-led space-system IFTU (e.g., a Global Positioning System IFTU) should be created to train Airmen in fundamentals and concepts that enhance their understanding of space systems and their capabilities. The IFTU course should familiarize students with threats such as antisatellite weapons or jammers as well as prepare them to conduct a mission-planning briefing for space operators. Enhanced follow-on mission qualification training for ISR duty positions within a space unit will further cement a knowledge of space systems.[13] In addition to unit-led IFTU, ASOpS and NSSI courses should enhance the ISR curriculum to educate space operators regarding what ISR *for* space personnel can provide as well as help the ISR *for* space Airman understand the space community's needs for protection and defense.

Recommendation 2: Build Experience by Placing Select ISR Personnel on a Space-Centered Career Path, and Provide Advanced Training Opportunities

Upon completion of their first space assignment, a select percentage of ISR Airmen should serve at least one more space assignment. Doing so will enable them to build on their tactical space knowledge as well as provide an opportunity to enhance professional growth for both their Airmen and themselves. Company grade officers and NCOs can hone their operational knowledge. Field grade officers and senior NCOs will build their space functional expertise to become senior leaders skilled in understanding strategic-level issues. Space-tracked ISR Airmen will have a better chance at achieving depth and breadth of experience within space. In accordance with AFI 36-3701, *Space Professional Development Program*, for nonspace AFSCs, "depth . . . generally equates to two or three space-related tours and breadth refers to experience with more than one space mission or expanded experience within the particular specialty." Further, enhancing depth and breadth of experience for the ISR *for* space professional will "increase mission effectiveness and reinforce space education."[14] An assignment to the JSpOC, the only command and control element within the military community capable of global space operations, would realize both breadth and depth of experience. Experienced ISR Airmen are greatly needed to lead the JSpOC into the future because a huge majority of Airmen assigned to the center's ISR Division (ISRD) have not had a previous space assignment. A follow-on assignment to the JSpOC would ensure that its ISRD is armed with Airmen who have the necessary space education, training, and experience, thus drastically enhancing support to the Joint Functional Component Command for Space's protect-and-defend mission.

If the investment is made in experience, it must also be made in advanced education and training. Courses like the Air Force Weapons School's Advanced Enlisted Mission Planning Course produce highly trained NCOs capable of supporting mission planning for a combatant command's contingency operations and operations plans. This planning course, which is primarily air platform–centric, should incorporate support to space assets in its curriculum. As they follow that course of study, AFSPC operations intelligence or targeteer Airmen work side by side with space Weapons School students to perfect their mission planning in support of the space combatant commander. Advanced education and training tailored to the ISR *for* space Airman do not exist and should be created to meet the unique mission demands of space systems. ISR *for* space Airmen who graduate from advanced courses will be able to take the skills they acquire back to their units and improve local training programs.

Recommendation 3: Train to Meet Mission Demands and Continuously Evolve ISR for Space Education and Training by Assigning Subject-Matter Experts to ISR **for** *Space Education and Training Programs*

Education and training programs geared toward the ISR *for* space professional should have experienced ISR *for* space subject-matter experts on their staff to help develop curricula. These experts should be charged to assure that education and training meet the mission demands of the space commander. A space-tracked ISR Airman will see to it that skill-level education and training are developed by individuals with the necessary expertise and experience. Team reviews of skill-development training, led by the space and ISR career field managers, should be used as the venue to ensure that current and potential requirements of the operational space community guide ISR *for* space force development. Purposefully developed Airmen will guarantee that experienced, well-educated, and well-trained professionals are available to supply feedback that enhances the ISR *for* space curriculum.

Recommendation 4: Provide Challenging Assignment Opportunities for ISR Professionals in Support of Space

To enhance ISR support, AFSPC and the Air Force ISR community should create basic, superintendent, and command assignment opportunities within space. For example, space units should have a fully manned intelligence support staff within an operations support squadron that provides intelligence preparation of the operational environment, mission briefings, and defense analysis plans (to name a few).[15] The squadron should also manage the proposed space system IFTU courses. These Airmen should be led and managed by a company or field grade officer, a senior NCO, and the intelligence AFSCs needed to address unique mission demands. Space-tracked Airmen who do not serve a follow-on AFSPC assignment should move on to a Twenty-Fifth Air Force or intelligence community assignment that allows them to fulfill ISR requirements that, when answered, provide critical information for the protection and defense of space assets.[16] Strategic-level assignments specific to ISR *for* space should also be created to improve policy making that often prevents information sharing with the space community.

Recommendation 5: Validate ISR for Space Education and Training by Leveraging ISR for Space Professionals to Develop Realistic Exercises and War Game Scenarios (Train Like We Fight)

We know that our adversaries are fully capable of attacking our space assets, the loss of which creates unpredictability for the war fighter. Consequently, every commander must understand the effects that such a loss will have on his or her force. Because a commander's decision cycle will be shortened, it is paramount that Air Force weapon systems reliant on space train and exercise as if such capabilities were threatened or unavailable. Realistic training demands the presence of a space-tracked ISR Airman to supply intelligence to develop realistic exercise and war-game scenarios based on actual threats as opposed to notional ones. These scenarios could be practiced in United States Strategic Command exercises as well as ACC's premier live-fly Red Flag exercise. The JSpOC's ISRD assists exercise-scenario development for Strategic Command. The 547th Intelligence Squadron, known as the "Center of Excellence" for adversary tactics analysis for the Air Force, offers all-source intelligence support for Red Flag. The JSpOC and the 547th should have ISR *for* space Airmen assigned to create realistic threat scenarios that challenge the combat capabilities space provides to the joint war fighter. A knowledge-enabled ISR *for* space professional will better prepare the space community and those who rely on its support to anticipate and plan for attacks as well as prepare them to navigate a degraded space environment.

The controlled environment of war games and exercises provides the best opportunity to ensure that ISR *for* space education and training meets the demands of the space commander. ISR is *the* component for understanding the operational environment, the adversary's operations, and the threat posed to space-based systems. The experience gained in these events is substantial, alerting the ISR and space communities of the existence of beneficial education and training and identifying education and training that needs to be corrected.

Conclusion

Although 30 percent or more of our ISR Airmen do not perform a space mission, one can argue that nearly all of the joint forces they support rely heavily—sometimes exclusively—on space-based capabilities to perform their mission. *This fact necessitates the need to dedicate all possible resources toward the development of an ISR* for *space cadre*. Many personnel within the space and ISR communities have different views regarding the use of intelligence Airmen in AFSPC and the integration of doctrinally sound and proven intelligence processes they bring to space operations. Critics may claim that the cost of investing in the ISR *for* space Airman is too high and unaffordable in a fiscally constrained environment. Such critics should be reminded of General Hyten's warning that space is not a benign environment.

The expense of investing in our ISR *for* space Airmen would be minuscule compared to the cost of losing a multi-billion-dollar satellite constellation. Indeed, space is the war fighter's Achilles' heel. ISR *for* space Airmen offer a critical capability in support of space's protect-and-defend efforts. They should not be viewed merely as intelligence researchers but—with proper education, training, and experience—as skilled professionals who interface with the intelligence community to supply actionable information that protects our nation's satellite constellations. As our adversaries' counterspace capabilities improve and as they become more willing to use them, gaps in our ISR force development will soon be revealed. Today's force-development approach for the ISR *for* space Airman must be adjusted to adequately address these threats. Such an Airman can be created only by following a purposeful career road map that deliberately develops an ISR professional capable of understanding and addressing the space commander's needs. As Gen William "Billy" Mitchell once said about airpower, "One has to look ahead and not backward and figure out what is going to happen, not too much what has happened."[17] If ISR is to keep pace with the changing space environment, then the Air Force must look at the future threat as a guide to how it will develop its ISR *for* space Airmen. It is the initial investment that Lieutenant General Otto called for—the purposeful development of the ISR *for* space cadre. ✪

Notes

1. United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 10 October 1967, http://www.state.gov/t/isn/5181.htm.

2. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: The Commission, 11 January 2001), xiii, http://www.dod.gov/pubs/space20010111.pdf.

3. SrA Phillip Houk, "AFSPC Commander Visits Buckley," 15 December 2014, Air Force Space Command, http://www.afspc.af.mil/news/story.asp?id=123434389.

4. Lt Gen Robert P. Otto, "ISR Roadmap" (speech presented at the Air Force Association's Air and Space Technology Exposition, Washington, DC, 17 September 2013), 8, http://www.af.mil/Portals/1/documents/af%20events/af-130917-AFA-ISRRoadmap.pdf.

5. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission*, 88–89.

6. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 1-1 Force Development," 15 December 2014, 2, https://doctrine.af.mil/download.jsp?filename=1-1-Annex-FORCE-DEVELOPMENT.pdf.

7. Air Force Instruction (AFI) 36-2623, *Occupational Analysis*, 10 September 2012, 6, http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-2623/afi36-2623.pdf.

8. SIFTU is an initial qualification training course designed for ISR Airmen new to AFSPC.

9. See Briefing, AFSPC Space and Cyberspace Professional Management Office, subject: Air Force Space Professional Development, accessed 28 August 2015, https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC1346920FB5E044080020E329A9. (See "CPDP Spread the Word Briefing.")

10. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy: Unclassified Summary* (Washington, DC: Department of Defense and Office of the Director of National Intelligence, January 2011), 8, 10, http://www.defense.gov/Portals/1/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

11. Curtis E. LeMay Center for Doctrine Development and Education, "Annex 1-1 Force Development," 10–11.

12. Ibid., 11.

13. Recommendation provided by SSgt Marie L. Foster, 11th Space Warning Squadron, Schriever AFB, CO.

14. AFI 36-3701, *Space Professional Development Program*, 20 May 2010, 7, http://static.e-publishing.af.mil/production/1/af_a1/publication/afi36-3701/afi_36-3701.pdf.

15. SSgt Foster, recommendation.

16. The Air Force ISR Agency (AFISRA) was redesignated Twenty-Fifth Air Force and assigned under ACC in September 2014. This action was designed to improve ISR support to the operational war fighter.

17. William "Billy" Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009), 18.

SMSgt Mitchell R. Overton, USAF

Sergeant Overton (BS, University of Maryland; MSSI, National Defense Intelligence College) serves as the superintendent, Unified Space Vault Division, Joint Space Operations Center, Vandenberg AFB, California. In this position, he is the senior enlisted leader responsible for the welfare, morale, mission effectiveness, professional development, and military readiness of a selectively manned 52-member joint division. Sergeant Overton enlisted in the Air Force on 11 September 1996. His background includes various assignments within the national intelligence community and Air Force Space Command. His experience spans several mission areas, including signals intelligence operations, collection management, special technical operations, squadron superintendent, and space command and control.

Let us know what you think! Leave a comment!

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

Space-Policy Education

Contexts and Constraints, Content and Methodology

Dwight Rauhala

> *The legacy of success in space and its transformation also presents new challenges. When the space age began, the opportunities to use space were limited to only a few nations, and there were limited consequences for irresponsible or unintentional behavior. Now, we find ourselves in a world where the benefits of space permeate almost every facet of our lives. The growth and evolution of the global economy has* [sic] *ushered in an ever-increasing number of nations and organizations using space.*
>
> —*National Space Policy of the United States of America*, 2010

During a visit to Washington, DC, several months ago, a colleague and I met with Dr. Dana Johnson at the Department of State.[1] The course of our discussion included policy-related issues as they pertain to US space activities. Near the conclusion of our meeting, Dr. Johnson, an adjunct professor at George Washington and Georgetown universities, asked, "How do you teach space policy?" Her question made me think about the various teaching methodologies we use at the National Security Space Institute (NSSI), particularly during the policy-strategy block of instruction within the Space 300 curriculum.[2] It also gave rise to the question, Do we teach the right things effectively?

I've attended a number of forums regarding education and space-related topics but have never participated in a forum dedicated to the discussion of space-policy education. I contacted Dr. Peter Hays and asked whom we might invite to such a discussion.[3] Among the academics recommended by Hays (and Johnson) was Dr. Scott Pace, director of George Washington University's Space Policy Institute, who offered up his venue for a roundtable discussion.[4]

Our roundtable agenda considered the following questions:

1. What is the educational mission and purpose (of a particular institution's curriculum)?
2. What are larger institutional contexts and constraints?

3. What is the nature of the students enrolled in the course/program?
4. What do students think they need, and what do they actually need?
5. What are they likely *to use*?

The agenda also included a survey of different types of instructional methods and their relative pros and cons. Unsurprisingly, we concluded that the answers to all five questions varied and could best be answered with, "It depends." For example, at the NSSI, the students are all military members or civil servants; however, the contexts within which they may need to consider space policies are very diverse. Although their respective jobs differ, most of the students work in space-related positions. Consequently, some of them work—or will work—in space-policy positions while others may deal only tangentially with national policy.[5] Similarly, the needs of students in George Washington's Space Policy Institute and of those in other universities may be just as disparate. For example, some have yet to enter a professional workforce, and some are in—or destined for—civil servant or private industry positions, and they may or may not work directly on space-policy-related issues. Still others may just be interested in learning about various facets of space and may not have a direct need, other than the value of education itself.

Thus, in light of diverse requirements and various fiscal constraints, what types of curricula and methodologies are effective in addressing students' core needs and furthering their professions' organizational goals? NSSI's three-week Space 300 course was designed within contextual constraints, partly due to budgetary considerations and time. The latter holds considerable weight; military services, combatant commands, and other military and intelligence agencies cannot easily deal with personnel absences for extended periods.[6] Conversely, public and private universities traditionally base their programs on a longer-term basis.[7]

Because Space 300 is limited to three weeks, the contact time between faculty and students typically encompasses a full duty day, five days a week. Approximately one-third of this period focuses on national space policy and strategy. With the time constraints, one question we had to address concerned what specifically should be taught about space policy and at what learning level should the material be presented.[8] Simple knowledge or comprehension of a given policy, in itself, is often inadequate. Students may and often have been put in roles in which they have to refer to national-level policy and apply its relevance to a specific situation. Here, they need to be aware of the relevant presidential guidance and other related regulatory and review processes consistent with that guidance and US law. It is not unusual for a person to be put into this process with no prior knowledge or experience and must attain proficiency solely through "OJT."

Some years ago, I found myself in this position as a space policy planner on the Joint Staff.[9] I was the Joint Staff's representative for reviewing requests for commercial remote sensing operating licenses—despite having had no directly relevant experience, training, or education. Many of my duties entailed researching documents with which I had little to no experience. For example, shortly after reporting to the Joint Staff, my task involved preparing Gen Richard Myers for a National Security Council (NSC) Deputies Committee meeting, which would address private remote sensing resolution restrictions.[10] I had little experience with the president's 1996 national space policy and none with the remote sensing policy and other regulatory guidance; obviously, I needed to immerse myself rapidly in all relevant authorities and established policy guidance before preparing and providing a recommended position for the general.[11] I thought there must be a better way to prepare an officer for space-related positions—the purpose of the Space 300 course.[12]

The course addresses various aspects regarding national space-related policy. First, it considers the worldwide geopolitical environment, examining the context within which policy guidance is developed, given, or otherwise handled. Thus, the course begins with a "Geopolitical Foundations" lesson via a discussion format. The rationale is that any examination of space-related policy and issues is related to national security within a specific geopolitical context: that policy development and consideration are contextual in nature.

Consequently, context significantly affects why a policy provides the guidance it does. Space 300's "Evolution of Space Policy" lesson helps to answer the *why*? This lesson scrutinizes the principles—the United States' philosophy—regarding space activities reflected in the 2010 national space policy and compares national space and other policies dating back to the 1950s.[13] During this inquiry, discussion includes what occurred at a particular point in time, why a certain principle was established, and how the principles evolved. This approach contributes to the students' ability to learn not only what is in a given space policy but also *why* it is included.

In addition to dealing with the current, national space-related policies, the Space 300 course familiarizes students with national-level policy formulation within the US interagency. By becoming acquainted with the NSC's organization, its relationship to the interagency, and the way policy is formulated, recommended, approved, and promulgated, students better understand the interplay within the executive government during policy development or execution.[14] They grasp the importance of personalities and the power of influence. They also comprehend that the president's policies are most often the combined effort of many people working within the interagency. At this point, students have a better appreciation for the forces in play during policy development.[15]

This also better prepares them for examining the 2010 national space policy. Student groups are assigned different portions of the policy and tasked with drawing the lineage between sector responsibilities and the policy's principles and goals.[16] The students discuss why certain entries are significant. Instructors emphasize substantive parts of the policy, and students are encouraged to share their perspectives. When we address positioning, navigation, and timing (PNT), as well as space-transportation-specific entries within the national space policy, we discuss how these items affect the extant PNT and space transportation policies, using this opportunity to segue into contemplating substantive points within those policies.[17] Not only do we establish the relationship among these policies but also we examine how they relate to the current national security strategy and national interests.[18]

After a final recap of key themes reflected in the policies, students determine applicable parts of the policy while considering how to react to a real-world situation. The policy exercise is based on a current real-world situation or event—often one where the US government may have made an interim ruling but has not yet decided its final position.[19] After analyzing and applying relevant laws, policies, regulations, and agreements, the students offer potential solutions to the issues in light of where the US government stands and what further actions are anticipated.

By applying national-level guidance to real-world situations as well as determining and analyzing implications among potential alternative courses of action, the students are better prepared to analyze other scenarios. Through our policy exam, we use notional crises as the basis for the students to apply relevant laws, strategies, policies, agreements, and regulatory guidance. They role-play officers on a government staff tasked to prepare and make recommendations to a senior individual who will be attending an NSC committee meeting to discuss the crisis. At the beginning of the exam period, we present a scenario followed by time for each student to reference relevant national guidance. The students then form groups, as if they were staffing the issue. Final preparation follows, when the students prepare their thoughts, organize their references, perform final analysis, and select recommended courses of action. They meet individually with an NSSI instructor who acts as the senior individual destined for the NSC committee meeting. The student presents his or her recommended course of action among those considered, noting rationale and all relevant references.

The NSSI continually assesses whether this approach is effective in teaching space policy. Given the various institutional and environmental constraints and the challenging goal of preparing students to analyze and apply national policy, we do believe it is *one* approach that is effective. ✪

Notes

1. Dr. Dana J. Johnson is the senior adviser for space policy, Office of Emerging Security Challenges, Department of State. As mentioned above, she also teaches space policy at two universities in Washington, DC.

2. The National Security Space Institute is an Air Education and Training Command (US Air Force) institution of learning. It is located at Peterson AFB, CO. Space 300 is one of the courses offered there.

3. Dr. Peter L. Hays is associate director at the Eisenhower Center for Space and Defense Studies and an adjunct professor at George Washington University's Space Policy Institute. He is editor and author of multiple books and articles on outer space activities.

4. The Space Policy Institute is part of George Washington University's Elliott School of International Affairs. The institute focuses on policy-related issues and the interplay between the United States and other nations. Dr. Pace assumed directorship following the retirement of Dr. John Logsdon, a longtime institute director and now director emeritus for the center. Other roundtable participants included the aforementioned Dr. Hays and Dr. Johnson; Dr. Logsdon, director emeritus of the Space Policy Institute; Dr. Howard McCurdy of American University; Dr. Clay Moltz of the Naval Postgraduate School; Dr. Forrest Morgan of the Pardee RAND Graduate School; Dr. William Barry, NASA historian; Deron Jackson of the Eisenhower Institute for Space and Defense Studies; and Jonty Kasku-Jackson and the author, both of the National Security Space Institute.

5. Examples include those military and Department of Defense civil-service positions within the space-policy offices in the Office of the Undersecretary of Defense (Policy) and the Joint Staff. The Department of State and other governmental agencies also have offices that work on space-policy-related issues but, at present, do not send their employees to the NSSI for their space-education needs.

6. Granted, some military and civil servant education programs, such as those found in the services and joint universities, have yearlong or longer programs, and extended postgraduate education fellowships programs are offered to a limited number of civil servants and military members. But many other educational programs are constrained to shorter time periods.

7. Here, I'm referring to degree programs. Many universities and colleges also offer shorter-term, accelerated-certificate (or other) programs.

8. Levels of learning are often characterized as "cognitive levels." One popular such characterization occurs via Benjamin Bloom's *Taxonomy of Educational Objectives*, whereby a hierarchy of learning ranges from simple knowledge level (recalling information without necessarily knowing its relevance) to evaluation (judging the value of some particular information). The other learning levels are comprehension, application, analysis, and synthesis.

9. The National War College, part of National Defense University, offers a curriculum described as a "senior-level course in national security strategy to prepare future military and civilian leaders for high-level policy, command, and staff responsibilities." See National War College, accessed 18 September 2015, http://nwc.ndu.edu. In other words, the education helps students think strategically on national-level issues within a broader international geopolitical context. Title 51, subtitle 6, chap. 601 is part of US law that gives the secretary of commerce regulatory authority for private, space-based remote sensing systems, part of which entails licensing for the systems' operations. The Memorandum of Understanding among the Departments of State, Defense, Commerce, Interior and the Intelligence Community Concerning the Licensing of Private Remote Sensing Satellite Systems offers procedures by which the relevant government organizations, including the Joint Staff (for the chairman of the Joint Chiefs of Staff), review and coordinate the licensing request.

10. Gen Richard B. Myers, USAF, was vice-chairman of the Joint Chiefs of Staff from 29 February 2000 until 1 October 2001, at which time he became the chairman of the Joint Chiefs of Staff.

11. Some of the major, relevant guidance for that time period included, but was not limited to, Presidential Decision Directive (PDD) / National Security Council (NSC) 49, *National Space Policy*, 19 September 1996; PDD/NSC 23, *Policy on Foreign Access to Remote Sensing Space Capabilities*, 10 March 1994; 15 Code of Federal Regulations (CFR) 960, *Licensing of Private Land Remote-Sensing Space Systems*, 25 April 2006; and the Land Remote Sensing Policy Act (now part of title 51, subtitle 6, chap. 601, *Licensing of Private Remote Sensing Space Systems*).

12. Space 300 was developed in 2005, the first prototype taught in the fall of that year. Impetus for its development was largely due to the recommendation of the *Report of the Commission to Assess United States National Security Space Management and Organization* (11 January 2001) regarding the nation's need for expertise in addressing space-related issues.

13. The 2010 national space policy is the current version of that document. See President of the United States, *National Space Policy of the United States of America* (Washington, DC: White House, 28 June 2010), https://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf. Each US presidential administration from presidents Carter through Obama has promulgated at least one national space policy (by that name). Before that time, a substantial number of presidential space policies were developed. Two of the early significant policies from the Eisenhower presidential administration were NSC 5520, *Statement of Policy on U.S. Scientific Satellite Program*, 20 May 1955, and NSC 5918/1, *U.S. Policy on Outer Space*, 26 January 1960. These documents were instrumental in articulating some of the principles reflected in today's national space policy.

14. The NSC, established via the National Security Act of 1947, is embodied in 50 *US Code*, sec. 3021. Consistent with law, each president tailors the NSC system to best serve him, typically articulated in a presidential directive such as President Obama's Presidential Policy Directive 1, *Organization of the National Security Council System*, 13 February 2009.

15. During his administration, President Obama promulgated a new national space policy and space transportation policy. However, the commercial remote and positioning, navigation, and timing policies of President George W. Bush are still largely/wholly in force. The students also learn how to make this determination.

16. Following the treatment on the goals and policies of the administration, the policy is broken down into sector guidelines, which delineate the responsibilities of the various sectors and intersectors as well as commercial, civil, and national security entities (Department of Defense and intelligence community).

17. At the time of the 2010 national space policy's (NSP) promulgation, the then-current positioning, navigation, and timing (PNT) policy and space transportation policy (STP) were from the George W. Bush administration and were technically still in force. In 2013 the administration promulgated a new STP, superseding the Bush-era policy; however, the Obama White House has not promulgated a new PNT policy. As a result, only those specific PNT-related points within the NSP supersede those specific points within the Bush-era PNT, with the rest of the Bush policy technically remaining in effect. Although the current NSP rescinds the G. W. Bush administration's space exploration policy in its entirety, Bush's US commercial remote sensing policy remains in force. We discuss these points with the students and demonstrate how to determine what policies remain in force (in part or whole).

18. In his op-ed "Align U.S. Space Policy with National Interests," Dr. Scott Pace effectively states, "It is my argument that international space cooperation, space commerce and international space security discussions could be used to reinforce each other in ways that would advance U.S. interests in the sustainability and security of all space activities. At present, however, these activities are largely conducted on their individual merits and not as part of an integrated national strategy." Scott Pace, "Align U.S. Space Policy with National Interests," *SpaceNews*, 26 March 2015, http://spacenews.com/op-ed-align-u-s-space-policy-with-national-interests. These remarks do not suggest that the NSP does not otherwise support the US national interests articulated in the national security strategy.

19. The Land Remote Sensing Policy Act of 1992 (now under 51 *US Code*, chap. 601) gives regulatory authority to the secretary of commerce (exercised through the National Oceanic and Atmospheric Administration's Office of Commercial Remote Sensing Regulatory Affairs) for the regulation of private, space-based remote sensing systems. Over time, restrictions to the operation of these high-resolution imaging satellites have gradually changed, enabling the industry to operate more capable satellites and sell increasingly detailed imagery products. As the basis for student exercises, the NSSI will often use instances of the government being in the midst of ruling on a requested change of operating restrictions. It is interesting to note that some (but not all) student groups often come up with recommendations similar to, or the same as, the interim US governmental position.

Dwight Rauhala

Mr. Rauhala (B.Design, University of Florida; MA, Webster University; MS, National War College) is a strategy and policy instructor who supports the Space 300 curriculum of the National Security Space Institute, Colorado Springs, Colorado. A career space and missile operations officer, he served more than 25 years in the United States Air Force, retiring with the rank of colonel. He has held operational and staff positions at the squadron, group, wing, major command, and Air Staff and Joint Staff levels—including three tours at the Pentagon. He was also commander of a Minuteman III intercontinental ballistic missile operations squadron. Additionally, he was designated a joint specialty officer. During the latter of two joint tours, Mr. Rauhala was chief of the Space and Missile Defense Policy Division, Directorate of Strategic Plans and Policy, Joint Staff, serving as principal adviser to the director for strategic plans and policy (J-5) on all matters concerning space and missile defense policy. In this position, he was directly involved with the 2000–2001 Space Commission and was the Joint Staff's primary point of contact for the National Security Council's Space Policy Coordinating Committee and Interagency on issues affecting space-related policy matters.

Let us know what you think! Leave a comment!

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

How to Make Disaggregation Work

Dr. Peter Wegner
Dr. Thomas C. Adang
Maureen Rhemann

> *And so resilience is made up of a number of things. Disaggregation could be a big piece of that, because right now we have a very small number of satellites on orbit and our adversaries know exactly where they are.*
>
> —Gen John Hyten
> Commander, Air Force Space Command

Evolutionary, Not Revolutionary Disaggregation

The concept of disaggregation refers to a means of creating resiliency by spreading capabilities across diverse platforms, including hosted payloads, smaller satellites, and tactical and strategic capabilities. As commercialization continues to usurp more of the space-platform ecosystem, disaggregation of many systems becomes evolutionary rather than revolutionary, allowing government to take advantage of a new architectural paradigm.

Space:
Congested, Contested, Competitive, and Commercialized

In the new millennium, activities in space are rapidly on the rise. The January 2011 *National Security Space Strategy* highlighted that the space environment is increasingly *congested*, *contested*, and *competitive*.[1] At the end of 2012, over 1,000 operating satellites were on orbit, contributing to a global $189.5 billion telecommunications and space industry. Since 2001 satellite industry revenues have nearly tripled, averaging an annual growth of 10 percent. Communication is the primary function of over half the operational satellites, and of those, 38 percent are of a commercial nature.[2] Today, more than 50 countries are represented by at least one satellite orbiting the earth, and the United States leads the pack. With this rapid growth in mind, it seems fitting that an additional descriptor be attached to the space environment: commercialization.

Additional examples of this rapid commercialization of the space domain include NASA's successful strategy to resupply the International Space Station through commercial launch service contracts to SpaceX and Orbital Sciences Corporation, which have demonstrated the capability to launch, dock with the space station, and deliver critical supplies and cargo. Both companies are past the challenging developmental phase and are now moving on to the lucrative launch-service phase of these contracts. Other examples of the rapid commercialization of the space domain include nascent efforts by venture-capital-funded companies such as SkyBox (Google) and PlanetLabs to dramatically reduce cost and timelines to deploy Earth-imaging satellites. Other companies such as Virgin Galactic and Bigelow Aerospace seek to serve the adventure tourism market with a promise of the ultimate adventure—vacations to outer space!

As this industry has evolved over the past 50 years, protection of these assets has taken second place to the spirit of exploration and pursuit of commercial gain. China's successful antisatellite test in 2007 and a series of subsequent tests have proven that US satellites are at risk. Threats to our satellites, either physical or virtual, could leave the United States vulnerable to more serious security threats and wreak havoc with our economy.

A Thoughtful Approach to Disaggregation: Three-Layered Space Architecture

This approach to disaggregation proposes a mission-by-mission process within the context of the threat and risk environment. The Three-Layered Space Architecture model is composed of (1) commercial commodities; (2) resilient tactical components; and (3) strategic space (see the figure below).

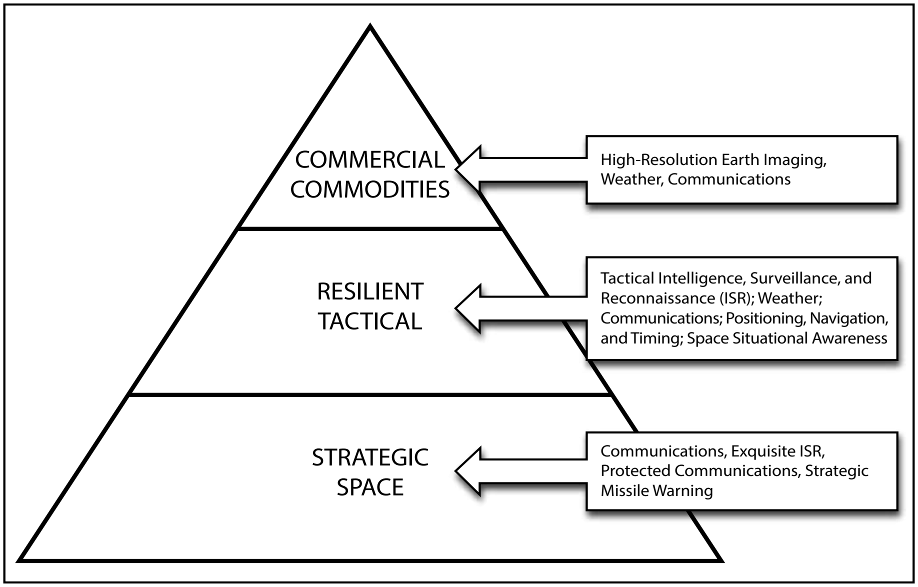


Figure. Three-layered space architecture model. A disaggregated architecture (1) invigorates the space industrial sector, (2) increases the resiliency of the national security space architecture, and (3) enhances the persistence of intelligence, surveillance, and reconnaissance capabilities by means of larger numbers of satellites.

Commercial Commodities Layer

The most dynamic of the three elements—the commercial commodities layer (CCL)—is the most rapidly changing and least expensive since costs continue to decline due to the infusion of new business models and technology. The Department of Defense (DOD) can simply buy capabilities by the picture, bit, or minute. Potentially, it is also the most vulnerable layer because these commercial systems typically will present soft targets to cyber or physical attacks, but through disaggregation and diversity, they may buy back resilience. One anticipates that this layer will grow to provide as much as 80 percent of the total Earth imaging, weather sensing, and communications capabilities used by the DOD—and will feature increased resilience and persistence.

Resilient Tactical Layer

The resilient tactical layer (RTL) will consist of a critical number of tactical intelligence, surveillance, and reconnaissance (ISR) satellites, weather satellites, and communications satellites required to sustain military operations in times of global crisis when commercial space systems may be denied, degraded, or destroyed. This layer will also include capabilities not conducive to development and operation by commercial companies when a profit motive may prove negligible (e.g., signals intelligence systems, space situational awareness systems, etc.). These systems will be smaller and lower in cost than today's national security satellite systems; thus, they can also be used to rapidly reconstitute capabilities that may be lost in the other two layers. An RTL is also beneficial because it is much easier and less costly to use these systems to reconstitute lost space capabilities of a critical nature. These smaller satellites can be launched on less sizable rockets that are cheaper, easier to use, and faster to manufacture and deploy.

Strategic Space Layer

Included in the strategic space layer (SSL) are some of the nation's most advanced and sophisticated space capabilities, such as exquisite ISR, strategic nuclear communications command and control, and strategic missile warning. These technologies are not available in the commercial sector, and in many cases they are highly classified to protect against their dissemination. These systems can be simplified by removing payloads and missions not necessary for their primary functions. Such capabilities will be absorbed by either the CCL or RTL. For example, today the space-based infrared satellites (SBIRS) host payloads for four different functions: strategic missile warning, missile defense, battlespace awareness, and tactical intelligence. The battlespace awareness and tactical intelligence missions could be offloaded to other less complex satellites in the RTL, reducing the complexity, cost, and development time of the SBIRS satellites.

Department of Defense Space-Based Weather Example: Less Costly, More Diverse and Rapid, More Persistent and Resilient

The centerpiece of DOD space-based weather architecture has been the Defense Meteorological Satellite Program (DMSP), which is coming to an end. In the CCL, a budding industry can offer such a service (e.g., PlanetIQ and GeoMetWatch) for requirements such as cloud imaging and profiles of atmospheric parameters (both tropospheric and ionospheric) via Global Positioning System (GPS) radio occultation. The DOD is likely to explore such commercial options with much more rigor. As these companies develop a strong business case in which the DOD is but one customer, the price point for the service will be attractive, and it will prove a valuable addition to capabilities acquired by systems in the RTL and SSL. In the RTL, the Jet Propulsion Laboratory is developing a Compact Ocean Wind Vector Radiometer payload for potential use by the operationally responsive space modular space vehicle for inexpensive demonstration to meet a need from the Joint Requirements Oversight Council. The Small Cloud Imager is a smaller, less complex satellite made by industry with a mass of less than 50 kilograms and a total mission cost of less than $80 million. Currently, the DMSP is the only DOD weather mission in the SSL, but services could be augmented by adding the National Oceanic and Atmospheric Administration's polar-orbiting operational environmental satellites; the Joint Polar Satellite System; and the European Organisation for the Exploitation of Meteorological Satellites—and by extending key requirements through public-public partnerships.

Trend: A Commercial Market Capable of Providing Most Future Requirements

The commercial small space market, which has reached a growth inflection point, could supply 80 percent of future requirements in a disaggregated architecture. Small satellites—microsats in particular—are in the midst of a fourfold growth spurt with longer-term growth implications. Launch-market technical and business innovations are close to achieving dramatic reductions in launch costs—the primary barrier to entry for space enterprise—and may be realized in the marketplace before 2020. Together, these emerging conditions are setting the stage for technological and economic revolution in the space business. According to recent analysis, the following key emerging trends will continue to redefine the satellite market, remaking it into a "network agnostic" and "device agnostic" crossroad for data distribution:[3]

- The market is rapidly segmenting between large-complex systems and small, lower-cost, lower-risk, and adequately functional systems.
- The global satellite market is showing emerging fractures as nontraditional content providers chip away at global markets.[4]
- Lower-cost satellites made with off-the-shelf components are driving capabilities up and costs down. Reducing satellite mass and employing commercially viable components and manufacturing processes create appropriate governmental

capabilities for 80 to 90 percent less than costs commonly attributed to current satellite fleets.

- Launch costs are declining in response to technical and business innovation.
- Demand for commercial satellites able to provide imaging, measurement, and signature observation capabilities is increasing as the use of commercial satellite imagery and data continues to supplement or replace less efficient means of discovery, measurement, and verification.
- Cloud computing and mobile wireless applications continue to create new innovations, spawning new means for utilization, new market demand, new deployed capabilities, new users, and new data sets.
- New investment in the small satellite market is on target to approach the billion-dollar mark by 2016. Investors are attracted to the growing industrial and consumer-level demands for data and related services, such as small imaging and sensing satellite market models.
- Small satellite technology models are merging with mobile wireless M2M (machine to machine) architectures and should be able to provide additional persistent and ad hoc capacity for supporting text messaging, payment processing, mobile shipment tracking, crop and disaster imaging, parking telemetry, remote asset analysis, remote diagnostics, and health-care applications such as remote patient monitoring, among many others.
- Low-cost imaging plus low-cost cloud computing and mobile wireless distribution will allow users new real-time data streams that they can use to further understand, promote, and manage critical functions such as energy infrastructure management, shopping patterns, crop yield projections, shipping management, and insurance underwriting.

Low-cost imaging satellites are on track to take "precision agriculture" to the next level by advancing remote management and diagnostics, further improving efficiency, crop yield, and return on investment. This capability will build upon the 30 percent productivity improvement to crop yields delivered by the GPS over the past decades.

Continued Investment for the Disaggregated Space Architecture Vision 2025

Pushing the cost and technological envelope is not without risk. However, such peril can be vetted and metered by maintaining an entry point for technology refreshment, operational prototyping, and replenishment of urgent-need capabilities. Congress has already authorized these functions through the Operationally Responsive Space Office.[5] Continued advances can be made through investments phased over a three-to-four-year time frame with a cost of approximately $50–60 million per year.

Commercial companies are beginning to disrupt space, just as technological innovations have disrupted media and communications. Today one can invest in the common enabling technologies and processes necessary to realize, for national security, the two new layers proposed in this three-layered space architecture: the RTL and CCL. We recommend that these investments be coordinated by a single DOD program to leverage investments across the DOD, intelligence community, and the civil and commercial space sectors. Finally, we propose that an independent board of advisers be assembled to review these investment plans, execution strategies, and organizing constructs.

Three-Layered Architecture: Resiliency, Affordability, and Technology Refreshment

Creating an architecture that is resilient, affordable, and expandable need not be an "all or nothing" approach to disaggregation but a "mission by mission" approach. As technological prowess grows and technology life cycles shorten, opportunities for more capable and lower-cost architectures become possible through infusing smaller satellites. As the cost of smaller satellites continues to decrease and as they become able to pack advanced technologies into more compact payloads, they offer augmentation and replacement for existing architectures and complementary coexistence. ✪

Notes

1. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy: Unclassified Summary* (Washington, DC: Department of Defense and Office of the Director of National Intelligence, January 2011), 1, http://www.defense.gov/Portals/1/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

2. Satellite Industry Association, "State of the Industry Report" (Washington, DC: Satellite Industry Association, 2014).

3. Chris Quilty, Raymond James Financial, "Satellite Industry & Wall Street" (presentation at World Space Risk Forum, Dubai, 2014), Trends Digest Database, http://worldspaceriskforum.com/2014/wp-content/uploads/2014/05/2A_WHERE-THE-CAPITAL-COMES-FROM_QUILTY.pdf; and [Maureen Rhemann], "Trend Watch: Five Reasons Why Smallsats Are about to Disrupt Telecom, Space, and Anything Else They Touch," *Trends Digest*, [January 2015], http://trendsdigest.com/.

4. See Scott Hubbard, "Roundtable Discussion: Growing the Future of Commercial Space," *New Space Journal* 1, no. 1 (March 2013): 3–9, http://online.liebertpub.com/doi/pdfplus/10.1089/space.2013.1501.

5. See John Warner National Defense Authorization Act for Fiscal Year 2007, Public Law 109-364, 109th Cong., 17 October 2006, sec. 913, Operationally Responsive Space, http://www.gpo.gov/fdsys/pkg/PLAW-109publ364/pdf/PLAW-109publ364.pdf.

PHOTO
NOT AVAILABLE

Dr. Peter Wegner

Dr. Wegner (BS, University of Arizona; MS, Stanford University; PhD, University of Wyoming) is the chief technology officer of Spaceflight Industries. He has more than 20 years of experience in the research, development, design, and operations of advanced spacecraft, rockets, and ground control systems. Prior to joining Spaceflight Industries, he held a director-level position with USU / Space Dynamics Lab where he led investments in new technologies and systems to solve some of the nation's most critical emerging space problems. Dr. Wegner was also a founding member and ultimately the director of the Department of Defense's (DOD) Operationally Responsive Space Office at Kirtland AFB, New Mexico, where he directed a budget in excess of $120 million per year and a staff of over 60 persons chartered with the responsibility for implementing a national strategy to develop new and innovative techniques to design, build, test, and operate space systems to support DOD missions. This strategy included developing the ability to rapidly reconstitute and augment critical space capabilities in a time of crisis. Dr. Wegner has also held positions as the technical adviser to Air Force Space Command's Directorate of Requirements and as a research engineer with the Air Force Research Laboratory's Space Vehicles Directorate where he developed many key innovations such as the Evolved Expendable Launch Vehicle's Secondary Payload Adapter ("ESPA Ring"), which has helped open the door for many small satellite programs to find a ride into space. Dr. Wegner has been a lead inventor and coinventor on five US patents.

Dr. Thomas C. Adang

Dr. Adang (BS, Purdue University; MPM, Saint Louis University; PhD, University of Arizona) is the senior technical adviser (The Aerospace Corporation) in the Operationally Responsive Space (ORS) Office at Kirtland AFB, New Mexico. In this position, he is responsible for providing technical leadership and strategic engagement support to the ORS Office as it develops and provides responsive space capabilities for joint force commanders and other users. Dr. Adang has more than 40 years of experience in atmospheric sciences, as well as in aircraft and space vehicle development, testing, and operations. Prior to supporting the ORS Office, he served a two-year federal appointment with the National Oceanic and Atmospheric Administration (NOAA) in a Senior Executive Service position as the NOAA technical director for integrated observations and data management. He joined The Aerospace Corporation in October 2000 as a senior project engineer supporting the National Reconnaissance Office (NRO). In March 2002, he established the Silver Spring Program Office supporting the NOAA Satellite and Information Service and served as that office's systems director. Prior to joining The Aerospace Corporation, Dr. Adang completed a distinguished 27-year career in the US Marine Corps and US Air Force, including assignments with the NRO, Air Force Space Command, Strategic Air Command, and Air Combat Command; he also served as the Air Force deputy director of weather and as commander, Detachment 085, Air Force ROTC, University of California–Berkeley. Dr. Adang is a graduate of the Air War College.

PHOTO
NOT AVAILABLE

Maureen Rhemann

Ms. Rhemann (BS, University of Maryland; Executive MBA, Houston Baptist University) is the senior executive and director of the Reperi Analysis Center where she has been responsible for managing Reperi's Applied Research and Development and Futures practice for the last 17 years. She has also led the Reperi team in more than 100 studies and strategic engagements involving trends and futures across emerging/converging technologies including space, mobile wireless, computing, and related markets. Ms. Rhemann has also been involved in the development of algorithms used to more accurately anticipate and predict critical disruptive trends and market changes well in advance of their occurrence.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

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

Personnel Recovery in Space

Lt Col Mari Manifold, USAF

Because of the incredible physical and ethical challenges of personnel recovery in space, the United States needs to take action now to codify recovery methods and expectations for future space travelers. Department of Defense (DOD) Directive 3002.01, *Personnel Recovery in the Department of Defense*, states that preserving military members, DOD civilians, and DOD contractors on US-sponsored missions is one of the department's highest priorities.[1] The Air Force's pararescue fact sheet elaborates by describing the nation's responsibility for personnel recovery as "a moral imperative."[2] If personnel recovery is one of the highest priorities of the DOD and a moral imperative, then what is the DOD doing to prepare for that operation in space? This article discusses the impact of terrestrial personnel recovery and the potential for recovery in space before suggesting use of a Civil Reserve Space Fleet (CRSF) and clarified codes to enable the United States to achieve its objectives.

The US "Airman's Creed" and "Soldier's Creed" assert that fallen Airmen and Soldiers will never be left behind.[3] This culture meets political reality in Department of Defense Instruction 1300.23, *Isolated Personnel Training for DoD Civilians and Contractors*, which points out that "the Department of Defense has a moral obligation to protect its personnel, prevent exploitation of its personnel by adversaries, and reduce the potential for captured personnel being used as leverage against the United States."[4] Failing to recover personnel can lead to public and political pressure to withdraw from the area of operations, as occurred during the Blackhawk Down incident in Mogadishu in 1993. Public outcry over the failure to recover US personnel led to President Clinton's decision to withdraw US forces from Somalia.[5]

In 2001 the Commission to Assess United States National Security Space Management and Organization concluded, "We know from history that every medium—air, land and sea—has seen conflict. . . . Space will be no different."[6] Accepting the idea of conflict in space, Colin Gray assumes that the strategic history of space power is likely to follow the pattern already traced by sea power and airpower.[7] He declares that "anything of great strategic importance to one belligerent, for that reason has to be worth attacking by others."[8] History has seen enemy forces seize ships and commandeer remotely piloted aircraft, and it is inevitable that such adversaries will attempt to take control of strategic vehicles in space.[9]

James Oberg writes, "At some time in the future, the physical presence of humans in space will be necessary to provide greater situational awareness."[10] Given the increased presence of humans in that medium, it is possible that a country may "seize" low Earth orbit (LEO), as Dr. Everett Dolman posits in his book *Astropolitik*, and take US LEO occupants as space prisoners of war—"capturing" them physically by docking onto their spacecraft or electronically by taking remote control of it.[11] Alternatively, if the US military takes over LEO and holds it by emplacing outposts of astronaut-Soldiers as human trip wires, other countries could challenge this action by commandeering the outposts and taking US occupants prisoner. As odd as these scenarios sound, Thomas Schelling points out "a tendency in our planning to confuse the unfamiliar with the improbable."[12] The purpose of taking prisoners in space would be the same as doing so on Earth: to weaken national will, degrade the US image domestically and internationally, influence international partners to withdraw from US-backed coalitions or alliances, and gain concessions, all the while limiting strategic freedom of movement.[13] If the United States cannot successfully sell its strategic narrative on why it is in space, then public support for US space operations could wane.

The best solution to space personnel recovery involves the United States setting up a CRSF agreement with civilian space companies to ensure the availability of recovery space lift. Like the Civil Reserve Air Fleet (CRAF) arrangement with civilian airliners, the Personnel Recovery CRSF would prevent the wasteful redundancy of a dedicated military fleet and would align with Presidential Policy Directive 4, which authorizes the government to purchase and use commercial space capabilities where available.[14] Speaking about the Marine Small Unit Space Transport and Insertion (SUSTAIN) concept, which also explored dual-use space lift, Brig Gen Richard C. Zilmer told a Senate subcommittee that "there exists a tremendous potential synergy that will mitigate the otherwise prohibitive expense of a solo-DOD technology/capability thrust."[15] CRSF carriers must maintain federal certifications and commit to having a vehicle ready when tasked, regardless of other paying missions slated to launch. Civilian space companies like SpaceX and Orbital Sciences, which already have NASA and US Air Force contracts, could fulfill this need in addition to their commercial business at one-third the cost of a government effort.[16] In return, the government would offer CRSF companies its peacetime space-lift business. The government would need to enlist multiple companies to provide system redundancy. These companies would supply the flight crew, and the military would provide the rescue team. Training and research would mitigate rescue team difficulties with unfamiliar equipment and safety considerations regarding breaching and the use of lethal force in pressurized space containers.

The US government should implement CRSF as soon as possible because astronauts are already living aboard the International Space Station.[17] Personnel recovery was so important to senior civilian leaders that they delayed the opening of operations in Afghanistan in 2001 until sufficient rescue forces could become operational in-theater; similarly, the United States needs to have space personnel recovery capabilities in place before adversaries exploit the weakness.[18] Publicly exercising the capability for recovery in space might deter potential enemies from trying to capture US personnel there since "capabilities that are untested, unknown or unproven cannot be expected to deter."[19]

In addition to securing capabilities, it is necessary to codify current legal norms for space personnel recovery. An important question is whether the Geneva Conventions apply to prisoners in space and, if so, to what degree. The United States must shape this international norm before leaning on it during a prisoner situation. According to United Nations Resolution 1721, international law—which the UN defines as treaties, agreements, conventions, and so forth—applies to outer space.[20] The 1967 Outer Space Treaty defines outer space as our solar system, encompassing its celestial bodies, orbits, and trajectories to or around them.[21] Consequently, adversaries should afford space prisoners of war their rights under the Geneva Conventions.

The US Air Force's *Operational Concept for Personnel Recovery* states that the service should provide rescue options for "anyone, anywhere, anytime."[22] To whom should the space rescue policy apply? The 1967 Outer Space Treaty asserts that states shall "regard astronauts as envoys of mankind in outer space and shall render to them all possible assistance" and that "in carrying on activities in outer space and on celestial bodies, the astronauts of one State Party shall render all possible assistance to the astronauts of other States Parties."[23] The current DOD personnel recovery obligation applies only to US government missions, but does the treaty obligate the United States to use its CRSF capability for all astronauts—civilian, military, foreign, and US? The United States should also clarify how far into space the assistance obligation applies—LEO, the moon, and Mars are economically and technologically different levels of commitment to space rescue. The United States should resolve these issues before human life is at stake.

Personnel recovery will be just as strategically important in space as it is in terrestrial conflicts. Therefore, the United States must establish a Personnel Recovery CRSF that uses private space-lift carriers similar to the airlift CRAF currently in place. It must also clarify personnel recovery material to delineate which recovery norms hold in space, for whom, and how far. Although the idea of personnel recovery in space is unfamiliar, now is the time to take these measures before an incident occurs. ✪

Notes

1. Department of Defense Directive 3002.01, *Personnel Recovery in the Department of Defense*, 16 April 2009 (incorporating change 1, 4 April 2013), 2, par. 41, http://www.dtic.mil/whs/directives/corres/pdf/300201p.pdf.

2. "Pararescue - 1T2X1," fact sheet, United States Air Force, 28 August 2006, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104514/pararescue-1t2x1.aspx.

3. "Airman's Creed," US Air Force, accessed 10 February 2014, http://www.airforce.com/learn-about/airmans-creed/; and "Soldier's Creed," US Army, accessed 10 February 2014, http://www.army.mil/values/soldiers.html.

4. Department of Defense Instruction 1300.23, *Isolated Personnel Training for DoD Civilians and Contractors*, 20 August 2003, 2, par. 4.1, http://www.dtic.mil/whs/directives/corres/pdf/130023p.pdf.

5. Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: Atlantic Monthly Press, 1999), 331.

6. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission to Assess United States National Security Space Management and Organization* (Washington, DC: The Commission, 11 January 2001), x, http://www.dod.gov/pubs/space20010111.pdf.

7. Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 258.

8. Cited in M. V. Smith, "Spacepower and Warfare," *Joint Force Quarterly* issue 60 (1st Quarter 2011): 42, http://www.dtic.mil/doctrine/jfq/jfq-60.pdf.

9. Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer (Video)," *Christian Science Monitor*, 15 December 2011, http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

10. James E. Oberg, *Space Power Theory* (Washington, DC: US Government Printing Office, March 1999), 129, http://www.au.af.mil/au/awc/space/books/oberg/ch05.pdf.

11. Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass Publishers, 2002), 157.

12. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission*, xv.

13. Col Lee Pera, Paul D. Miller, and Darrel Whitcomb, "Personnel Recovery: Strategic Importance and Impact," *Air and Space Power Journal* 26, no. 6 (November–December 2012): 88–89, http://www.airpower.maxwell.af.mil/digital/pdf/articles/2012-Nov-Dec/F-Pera-Miller-Whitcomb.pdf.

14. "Fact Sheet: The National Space Policy" (Washington, DC: White House, Office of the Press Secretary, 28 June 2010), http://www.whitehouse.gov/the-press-office/fact-sheet-national-space-policy.

15. Jeff Wright, "Why We Must SUSTAIN Human Spaceflight," *Space Daily*, 13 October 2003, http://www.spacedaily.com/news/oped-03zzj.htmlhttp://www.spacedaily.com/news/oped-03zzj.html.

16. "Launch Manifest," SpaceX, accessed 19 February 2014, http://www.spacex.com/missions; Orbital ATK, accessed 19 February 2014, http://www.orbital.com/HumanSpaceExplorationSystems/COTS/; and "Falcon 9 Launch Vehicle NAFCOM Cost Estimates," NASA Associate Deputy Administrator for Policy, August 2011, http://www.nasa.gov/pdf/586023main_8-3-11_NAFCOM.pdf.

17. Maj M. V. Smith, *Ten Propositions Regarding Spacepower*, Fairchild Paper (Maxwell AFB, AL: Air University Press, 2002), 37, http://aupress.maxwell.af.mil/digital/pdf/paper/fp_0009_smith_propositions_regarding_spacepower.pdf.

18. Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002), 150–52.

19. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission*, xvi.

20. "Definition of Key Terms Used in the UN Treaty Collection," United Nations Treaty Collection, accessed 10 February 2014, https://treaties.un.org/Pages/Overview.aspx?path=overview/definition/page1_en.xml.

21. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, United Nations Office for Outer Space Affairs, 19 December 1966 (hereafter Outer Space Treaty), http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.

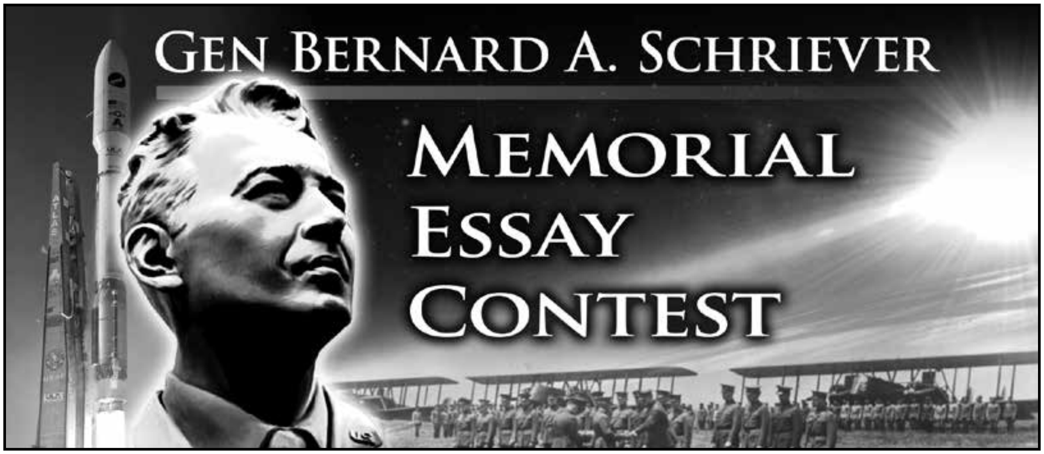
22. Gen Norton A. Schwartz, *Operational Concept for Personnel Recovery* (Washington, DC: Headquarters US Air Force, 3 September 2009), 20.

23. Outer Space Treaty.

Lt Col Mari Manifold, USAF

Lieutenant Colonel Manifold (USAFA; MS, Embry-Riddle Aeronautical University) is an AC-130H pilot who has deployed multiple times in support of Operations Enduring Freedom and Iraqi Freedom. She has also served in staff positions at the group, wing, numbered air force, and major command levels, recently serving as the Twenty-Third Air Force director of staff at Hurlburt Field, Florida, and now as the deputy chief of strategic and capabilities-based planning at Air Force Reserve Command, Warner Robins AFB, Georgia. A summa cum laude graduate of Embry-Riddle Aeronautical University and a distinguished graduate of both the C-130 Qualification Course and Air Command and Staff College, Lieutenant Colonel Manifold recently graduated from the School of Advanced Air and Space Studies, Maxwell AFB, Alabama.

Let us know what you think! Leave a comment!



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

2nd Lt Chris Babcock

"Preparing for the Cyber Battleground of the Future"

Second Place

Lt Col E. Lincoln Bonner

"Defending Our Satellites: The Need for Electronic Warfare Education and Training"

Third Place

Maj Sean C. Temple

"Developing Tomorrow's Space War Fighter: The Argument for Contracting Out Satellite Operations"

Honorable Mention

Col John Wagner and Lt Col Nathan Yates

"The AOC Model for Space C2: Enhancing the Future of Joint Operations"

Lt Col Greg McCulley

"Towards the Battle: Recommendations on Cyberspace Training"

Maj Elisabeth White

"Reconsidering the Cyberspace Human Capital Strategy"

The winning essayists received trophies and $1,000 for first place, $750 for second place, and $500 for third place.

Preparing for the Cyber Battleground of the Future

2nd Lt Chris Babcock, USAF

For space and cyber Airmen, tomorrow's fight will be determined largely by the concept of cyberspace dependency. That term, as defined by the author, is the degree to which a military capability relies on supremacy over a portion of the cyberspace domain in order to cause or carry out its effects.[1] Cyber dependency is rapidly growing due to the cyberspace domain's exponential nature, the trajectory of market forces in the civilian world, and the strategic integration by the military of computer technology in the land, maritime, and air domains.[2]

Unlike employment in the three traditional war-fighting domains, the present employment of capabilities in the space domain *cannot* be achieved without cyberspace.[3] The recognition of this unique relationship between space and cyberspace has profound implications for recruitment; initial, intermediate, and advanced training; and development in the space and cyber career fields. A transition from the current force-development system towards one that acknowledges the unique relationship between space and cyberspace will have the additional benefit of informing the greater operational community as war fighters in the land, maritime, and air domains continue to become increasingly dependent upon cyberspace and space. This article discusses the implications of cyber dependency and proposes six recommendations to ensure that from recruitment to advanced training, space and cyber Airmen are prepared to excel in their interconnected domains.

Space Cyber Dependency

> *The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace, and a critical portion of cyberspace can only be provided via space operations.*
>
> —Joint Publication 3-12 (R),
> *Cyberspace Operations*, 5 February 2013

All space operations currently performed by the US military are cyberspace dependent (fig. 1).[4] Space operations take place in the physical space domain, not within cyberspace. But because those who perform space operations are not physically present in space, they must rely entirely on control of their segment of cyberspace to transmit their commands to space vehicles in order to carry out space operations.[5]

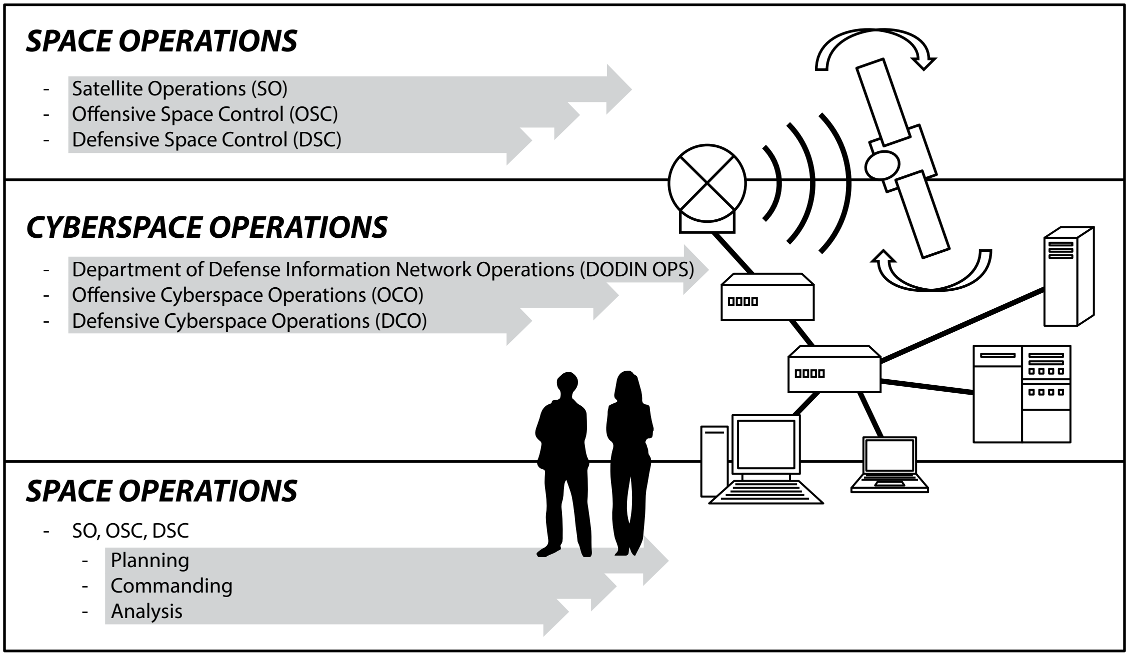


Figure 1. Space and cyberspace operations. Due to physical limitations, space operations take place on both sides of the cyberspace domain.

If a military space operation were to involve a pilot physically residing in a space vehicle, reacting to the environment in order to carry out effects in space, this would describe a space operation that is not reliant entirely on cyberspace supremacy.[6] In the absence of that scenario, space operators must use specialized computers and computer programs to transmit information to and from their space vehicles—which are themselves complex information systems—over a computer network.[7] Space's cyber dependency demands that special attention be paid to the cyber defense of space capabilities, but it also foreshadows the future state of the traditional war-fighting domains.

The physical network layer of cyberspace includes the information systems with which space operators command their satellites, the circuits connecting those information systems to the ground equipment, and the ground equipment itself. The logical network layer of cyberspace is embedded in each piece of the physical network. The cyber-persona layer describes the space operators who rely on the physical and logical network layers to perform space operations (fig. 2).

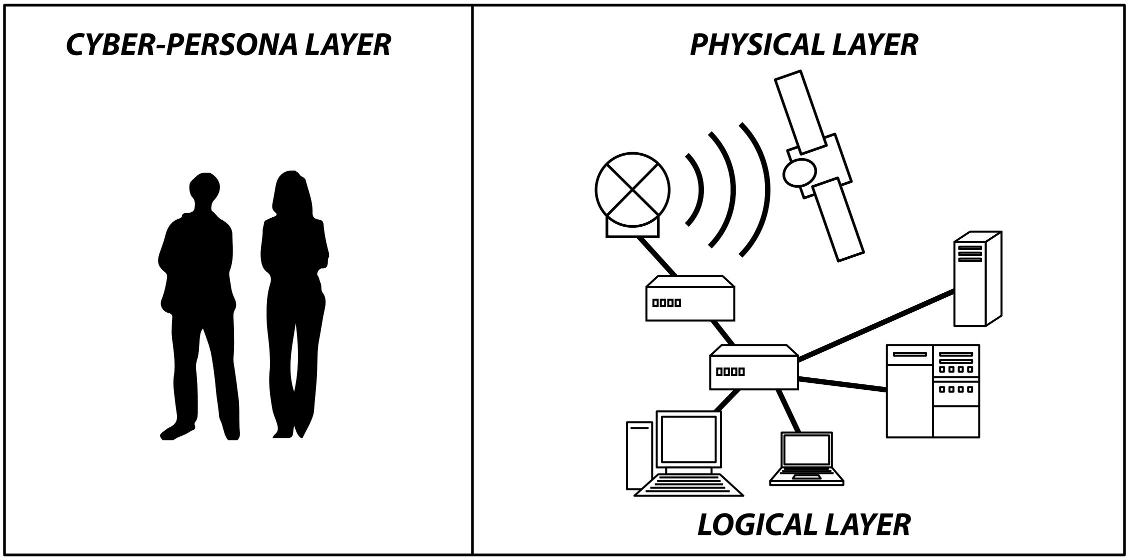


Figure 2. Cyber layers in space operations

The Exponential Domain

> *But if you think you're safe in cyber, when you wake up tomorrow, everything is different.*
>
> —Gen John E. Hyten, Commander
> Air Force Space Command

Ever since Intel cofounder Mr. Gordon Moore observed in 1965 that the capability of computer circuitry grows exponentially over time, it has been widely understood that innovation in computer technology expands at a rate unmatched in human history.[8] Innovation begets innovation, and the changing nature of information technology poses unique challenges for military operators in the cyberspace domain compared to those of the first four war-fighting domains.[9]

First among those challenges is that the private sector has now begun to advance far more rapidly than the defense industry in several areas of technological innovation.[10] This can mostly be attributed to the molasses-like procurement and configuration management processes in the Department of Defense's large technological programs relative to the nimbleness of a Silicon Valley start-up company.[11]

A second serious challenge is that the asymmetry of cyberspace allows attackers to more quickly and more easily utilize rapid changes to their advantage than can defenders.[12] At a fundamental level, cyber defenders attempt to ensure that software and hardware work the way they are supposed to while cyber attackers attempt to break software or hardware to cause harmful effects.[13] In this matchup, the aggressor will almost always have the advantage. Additionally, the exponential nature of cyberspace causes institutional knowledge and individual skill sets to atrophy far more quickly than they do in the traditional war-fighting domains. This poses especially interesting challenges for the training and education of cyberspace operators.

For all of its difficulties, the US Air Force has a well-established grasp on the current cyberspace battleground. Yet, it must fully account for the nature of cyber dependency and the implications it holds for the expanding cyber battleground of the future.

Self-Induced Dependency

> *The F-35 Lightning II is one of the most complicated weapons systems ever developed, a sleek and stealthy fighter jet years in the making that is often called a flying computer because of its more than 8 million lines of code.*
>
> —Christian Davenport, *Washington Post*

While the space domain is the first to be wholly dependent upon cyber, it will not remain the only one. In the air domain, remotely piloted aircraft are an excellent example of a weapon system that is wholly cyber dependent.[14] Even the newest manned fighter aircraft, the F-35, has been described as a flying computer; furthermore, while the Army develops personal drones, smart exoskeletons, and computerized rifles, the Defense Advanced Research Projects Agency is developing pack-mule robots, and the Navy is creating its own autonomous drones, including both submarines and aircraft.[15]

While those efforts will certainly enhance war-fighting capabilities, increased cyber dependency also comes at a cost. The cost may be paid in increased risk to the missions that these technologies support or in deliberate security and active defense of the newly dependent systems.[16] In each example, the inherent risks introduced by cyber dependency are monumental. In the civilian world, hackers have already been able to take control of vehicles (most notably gaining full remote control of the latest Jeep models), smart guns, and hobby drones. They have even infiltrated the internal networks of commercial aircraft.[17] For the cyber squadron of the future, security and defense of local weapon systems—from land and air to space—must be a priority (fig. 3).

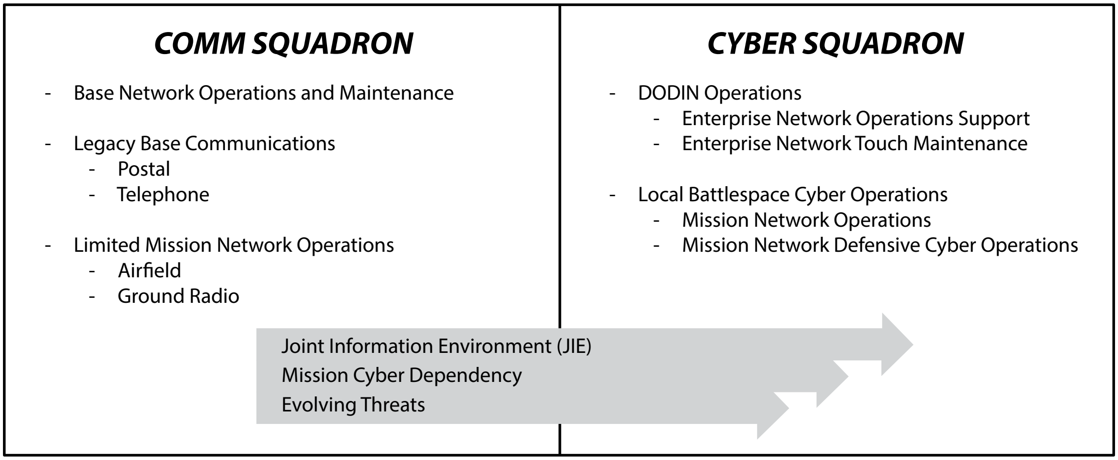


Figure 3. From communications to cyber. (Based in part on briefing, Lt Col David Canady, subject: Cyber Squadron of the Future, Headquarters US Air Force / A6CF, May 2014, http://www.safcioa6.af.mil/shared/media/document/AFD-140512-040.pdf.)

One particularly thorny challenge for those cyber operators will be the requirement to perform cyber operations on the live network of a weapon system, but this challenge can and must be overcome.[18] Choosing not to secure and defend is the riskiest choice of all. In cyberspace, the longer any vulnerability exists in an unmitigated form, the greater the odds that it will be weaponized and exploited by an adversary. By some measures the process, from discovery to weaponization and attack, takes hackers little more than one week to complete.[19]

Cybersecurity concerns have not yet stopped the Department of Defense from procuring weapons that are increasingly cyber dependent. In the civilian world, regular consumers also seem to not yet be dissuaded by security concerns.

Market-Driven Cyber Dependency

> *These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.*
>
> —Joint Publication 3-12 (R),
> *Cyberspace Operations*, 5 February 2013

Market forces in the civilian world are rapidly driving many categories of consumer products towards the "Internet of Things" (IoT). By 2020 it is estimated that there will be between 50 and 100 billion devices that are networked to each other across the world, creating an IoT.[20]

From refrigerators to coffeepots and thermostats, the commercial marketplace is growing increasingly flooded with Internet-aware devices of all types.[21] Arguably, the preponderance of devices in the marketplace in the near future will be Internet-aware, making it difficult for a discerning consumer such as the Department of Defense to find noncomputerized alternatives.[22] This will leave the military with difficult choices to make regarding the trade-off between accepting risk or accepting the costs associated with cybersecurity and defense of these newly networked refrigerators and coffeepots.

If we accept that in the future a much higher percentage of devices, infrastructure, and systems will have computer networking capabilities that are either a permanent part of military installations (such as supervisory control and data acquisition [SCADA]) or will regularly enter military installations (such as smart watches and self-driving cars), then those devices will become a de facto part of the cyber battlespace. It is the cyber squadron of the future that should be relied upon to secure and defend those devices. Efficiencies provided by organizational and structural changes such as the move to the joint information environment, as well as new technologies such as software-defined networking, may free up many of the resources required to allow the cyber squadron of the future to secure and defend the expanded cyber terrain; however, additional investment and reforms will also be needed to sustain these new requirements.[23]

Winning Tomorrow's Fight

Given the speedy movement towards greater cyber dependency throughout the military, it is critical that Air Force Space Command examine and consider the following recommendations for the cyber and space force-development systems.[24]

Leverage Big Data for Decision Making

Air Force Space Command should develop three standard tests and should implement them throughout the force-development process to assess both space and cyber Airmen. The first test should be for cyber proficiency and propensity only. This test would measure a recruit's or trainee's potential to comprehend cyber concepts and acquire cyber skills, regardless of formal cyber training.[25] The second and third tests would be knowledge based—one for knowledge applicable to cyberspace operations and the other applicable to space. Initially, it may be impossible to determine exactly what cyber proficiency looks like. This is acceptable and should not dissuade the command from undertaking this effort. As scores for all three tests are compiled, they must be associated with members and tracked alongside other metrics to determine how scores appear to correlate to a given individual's success, mediocrity, or failure. The process of data compilation and analysis should continually inform a cyclical reevaluation of the tests to ensure that they adequately assess ability and knowledge.

Pertinent data points that should be associated with test scores fall into three major categories: education, training, and experience. By combining proficiency and knowledge test scores with data points from these three categories, Air Force Space Command will gain powerful insight into how to prioritize education, training, and experience when it makes force-development decisions. By strategically retesting Airmen, the command can gain insight into how specific training events or educational milestones affect or do not affect scores.[26]

Mission-Specific Cyber Training

Air Force Space Command is close to having implemented the optimal framework for an initial, intermediate, and advanced training system for cyberspace operations. The current focus on mission-specific intermediate training as opposed to general intermediate training and on-the-job training is a great leap in the right direction.[27] Increased cyber dependencies will create the need for many additional mission-specific training courses such as SCADA and IoT defensive operations, as well as intermediate cyber defensive training that is specific to various Air Force land, space, and air mission systems.

For enlisted Airmen, the 1B initial training course should be split between a combined 3D and 1B initial training course and intermediate training courses that are specific to the mission requirements that 1B and 3D Airmen will encounter. The 3D career fields should not be left out of the operationalization of the communications career fields because they play important roles in the security and defense of the cyber battleground and will continue to do so. Efforts to divide training requirements between the 3D and 1B career fields should follow the National Institute of Standards and Technology's National Initiative for Cybersecurity Education Framework.[28] While training for enlisted 3D and 1B Airmen will diverge fairly quickly after the basics, there must be a set of core "operational cyber" fundamentals shared by the two career tracks.[29]

Specialized Training for Cyber-Dependent Operators

For those noncyber officers whose mission sets have high levels of cyber dependency, such as space operations personnel and remotely piloted aircraft pilots, opportunities should be made available for them to attend the intermediate and advanced cyber training that is applicable to their mission. Program acceptance for noncyber Airmen should be based in part on their cyber proficiency and knowledge test scores.

Just as there is an advantage provided by having weapons officers who are proficient across the spectrum of weapon systems, so would it be advantageous to have officers in cyber-dependent missions who are also proficient in cyber operations.[30] A program similar in many ways to the one offered by the USAF Weapons School but with a smaller footprint should be established to strategically place graduates within their cyber-dependent career fields.[31]

Work to Expand Industry Partnership Opportunities

Air Force Space Command should work with the Office of the Assistant Secretary of the Air Force for Acquisition (SAF/AQ) and the Air Force Institute of Technology (AFIT) to create a special pipeline for officer and enlisted Airmen in the space and cyber career fields to tour in the Education with Industry (EWI) program. If this cannot be accomplished, Air Force Space Command should consider establishing a similar program, focused on bringing cutting-edge innovation and specialized skills back to the military while expanding ties with industry partners.

Graduates of the EWI program not only help close the technology and skills gap between the military and the private sector but also help increase cooperation and strengthen ties between the two sectors at a critical time for space and cyberspace.[32] Air Force Space Command should focus on embedding officer and enlisted Airmen within corporations that are at the forefront of space and cyberspace technology and should press to expand outside the list of traditional cleared defense contractors.

Though the EWI program is not generally made available to enlisted Airmen, space and cyberspace require unique technical skills that can be developed and grown during an EWI tour. While an officer in the EWI program may develop unique leadership skills and pick up innovative ideas, correctly placed enlisted Airmen could bolster their coding or other technical skills that are specific to their mission and career field.

These efforts would be in line with Secretary of Defense Ashton Carter's initiative to increase innovation in the Department of Defense and strengthen military and industry ties.[33] In addition to coordination with SAF/AQ and AFIT on the EWI program, Air Force Space Command should seek to develop direct ties with Defense Innovation Unit X, the new Department of Defense cell in Silicon Valley.[34] Because Unit X will primarily develop and strengthen industry ties in the area of cyber operations, Air Force Space Command would benefit from coordinating with Unit X on force development of cyberspace operators.[35]

Encourage New Forms of Education and Training

The civilian market for Internet-based microdegrees, nanodegrees, and other forms of short-term, topic-specific training has greatly increased cost-effective education and training opportunities for Airmen to leverage.[36] Shorter than an associate degree but longer than a traditional training course, microdegrees and other new forms of Internet-based learning have proliferated in recent years. Air Force Space Command should actively embrace and explore this trend as a way to train and educate space and cyber Airmen. Partnerships with online learning companies such as Udacity, Coursera, edX, or other massive open online course (MOOC) providers may yield opportunities for Airmen to gain topical education and training customized to the needs of Air Force Space Command, with much lower entry costs and time barriers for students.[37]

Traditional education still has a very important role to play, but Air Force Space Command should take active steps to investigate how these education technologies are changing the civilian education market.[38] Microdegrees can provide Airmen with a far more agile, topical, and responsive form of education that also allows them to stay up to date in the rapidly advancing field of information technology. Beyond individualized education and training, partnerships between Air Force Space Command and MOOC companies could provide a relatively cost-efficient way to train space and cyber Airmen on the whole.[39]

Extensive Investment in the Cyber Training Corps

Of all the war-fighting domains, cyber's exponentially changing terrain makes "teaching cyber" a challenging task over time. Comparatively, very little changes year-to-year as pilots are trained in air operations or as space operators are trained in space operations, yet course material in the cyber domain may become outdated within months.[40]

Just as an individual operator's skills and knowledge will atrophy far more rapidly than in the other domains, so will material developed for training and education.[41] For every instructor assigned to a cyber instructional course, Air Force Space Command should consider assigning a second member whose responsibilities include rapid revision of course material based on changing circumstances in the cyber domain and tuning based on analysis of student feedback and performance.

While the instructor handles instruction, grading, and administration, a course developer would be tasked to ensure that course instruction remains timely and relevant. Whenever possible, course developers should be embedded with operational units and/or industry partners in the private sector for short bursts of time to retain cutting-edge knowledge and skills.[42] Like an information system with known vulnerabilities, cyber instructional courses cannot afford to remain static; instead, they must be treated like a constantly evolving system. For every cadre of instructors, there should be an equally large or greater cadre of course developers handling this function.

Conclusion

Of all the war-fighting domains, cyberspace is the most rapidly changing. These changes are driving Air Force missions and weapon systems towards greater cyberspace and space dependency. By understanding, anticipating, and posturing for greater degrees of cyber dependency throughout the force, Air Force Space Command will develop space and cyber Airmen who are ready to prevail in the cyber battleground of the future.

Air Force Space Command should consider the advantages of leveraging big data for decision making, continuing to develop mission-specific cyber training, making cyber training available to operators in cyber-dependent missions, strengthening ties with industry partners, encouraging new forms of education and training, and investing heavily in an expanded cyberspace training cadre. These investments, some small and some large, would yield sizable dividends when Air Force Space Command suddenly finds itself immersed in the cyber battleground of the future. It is possible to imagine, at some near-distant point in the future, an Air Force that is wholly dependent on space and cyberspace. It is equally possible to envision an Air Force whose cyber defense capabilities are far greater than the new threats that these space and cyber dependencies will pose. The time to begin overcoming the challenges of cyber dependency is now. ✪

Notes

1. Degrees of cyber dependency may be used to describe any military capability, technology, or strategy. Supremacy in the cyberspace domain is analogous to air supremacy and is defined by the author as the degree of cyber superiority over a portion or segment of cyberspace wherein the opposing cyber force is incapable of effective interference.

2. Market forces will drive the military to secure and defend a larger battlespace, but the Department of Defense itself will also deliberately expand the cyber battlespace in a much more consequential way.

3. Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, 5 February 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. JP 3-12 refers to this as the "[unique] relationship" between space and cyberspace. The author calls this "domain cyber dependency" because all operations in the space domain presently rely on cyberspace supremacy.

4. Ibid.; and JP 3-14, *Space Operations*, 29 May 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

5. JP 3-12 (R), *Cyberspace Operations*, defines cyberspace as "many different and often overlapping networks, as well as the nodes (any device or logical location with an internet protocol [IP] address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them" (I-2).

6. Ibid.

7. Ibid. With regard to space operations, the physical network layer of cyberspace includes the information systems with which space operators perform command and control operations and receive and analyze telemetry; the circuits connecting those information systems to the ground equipment; the ground equipment itself, which prepares and sends data to the space vehicle; and the space vehicles themselves. The logical network layer of cyberspace is embedded in each piece of the physical network. When space operators change configurations on or send commands to any part of the physical network layer, encrypt or decrypt transmissions, or perform data aggregation and analysis, they are operating within the logical network layer of cyberspace. To some degree, these actions may be considered cyberspace operations. The cyber-persona layer describes the space operators who rely on the physical and logical network layers to perform space operations. The cyber-persona layer also includes potential adversaries who may disrupt space operations through their own cyberspace operations.

8. Damon Poeter, "How Moore's Law Changed History (and Your Smartphone)," *PC*, 19 April 2015, http://www.pcmag.com/article2/0,2817,2482133,00.asp.

9. JP 3-12 (R), *Cyberspace Operations*; and Mark Pomerleau, "Army Cyber Chief Outlines Key Challenges, Goals," Defense Systems, 18 March 2015, http://defensesystems.com/Articles/2015/03/18/Army-cyber-Cardon-outlines-challenges-goals.aspx.

10. Max Boot, "The Paradox of Military Technology," *New Atlantis*, no. 14 (Fall 2006): 13–32.

11. Jose Pagliery, "Love, Not War: Pentagon Courts Silicon Valley," *CNN*, 23 April 2015, http://money.cnn.com/2015/04/23/technology/security/military-silicon-valley/.

12. Lt Col Gregory Conti and Col John "Buck" Surdu, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?," *IAnewsletter* 12, no. 1 (Spring 2009): 14–18; and Andrew Phillips, "The Asymmetric Nature of Cyber Warfare," US Naval Institute, 14 October 2012, http://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare.

13. JP 3-12 (R), *Cyberspace Operations*.

14. Katia Moskvitch, "Are Drones the Next Target for Hackers?," BBC, 6 February 2014, http://www.bbc.com/future/story/20140206-can-drones-be-hacked; and Aliya Sternstein, "How to Hack a Military Drone," DefenseOne, 29 April 2015, http://www.defenseone.com/technology/2015/04/how-hack-military-drone/111391/.

15. Christian Davenport, "Meet the Most Fascinating Part of the F-35: The $400,000 Helmet," *Washington Post*, 1 April 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/04/01/meet-the-most-fascinating-part-of-the-f-35-the-400000-helmet/; "Insects Inspire Military Mini Drones," *Fox News*,

18 September 2014, http://www.foxnews.com/tech/2014/09/18/insects-inspire-military-mini-drones/; Joyce P. Brayboy, "Army Researcher's Interest in Robots Leads to Innovative Device," US Army, 2 July 2015, http://www.army.mil/article/151527; Terri Moon Cronk, "Robot to Serve as Future Military's 'Pack Mule,' " US Department of Defense, 19 December 2012, http://archive.defense.gov/news/newsarticle.aspx?ID=118838; Brendan McGarry, "U.S. Military Begins Testing 'Smart' Rifles," DefenseTech, 15 January 2014, http://defensetech.org/2014/01/15/u-s-military-begins-testing-smart-rifles/; and Kris Osborn, "Navy to Deploy First Underwater Drones from Submarines," Military.com, 13 April 2015, http://www.military.com/daily-news/2015/04/13/navy-to-deploy-first-underwater-drones-from-submarines.html.

16. Cybersecurity is most commonly understood to be compliance related, such as the management of vulnerabilities and the implementation of protective measures. This contrasts with active defense, which is the implementation of defensive measures or maneuvers in anticipation of, during, or after a cyber incident or engagement with an adversary.

17. "The Pentagon Got Hacked While You Were at Def Con," *Wired*, 9 August 2015, http://www.wired.com/2015/08/security-news-week-pentagon-got-hacked-def-con/; 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/; Kim Zetter, "Is It Possible for Passengers to Hack Commercial Aircraft?," *Wired*, 26 May 2015, http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/; and Hallie Golden, "Security Experts Point to OPM's Biggest Cybersecurity Failure," NextGov, 21 July 2015, http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/. In each of these examples, the exploits were uncovered by security researchers, not professional "militarized" hackers. If a well-organized, advanced, persistent threat were to commit its resources to similar targets, the results would likely be far severer.

18. JP 3-12 (R), *Cyberspace Operations*. Traditionally, the bulk of defendable battlespace in the cyberspace domain has been communications infrastructure that provides support to the primary mission. One implication of greater cyber dependency will be that the defendable battlespace will expand to include the mission systems themselves. The challenge posed is that intuitively, friendly disruption to the mission would be more likely while defensively operating on a mission or weapon system than it would be while defending communications infrastructure.

19. Recorded Future Special Intelligence Desk, "Week to Weak: The Weaponization of Cyber Vulnerabilities," Ref ID: 2014-02 (Somerville, MA: Recorded Future, 4 December 2014), http://go.recordedfuture.com/week-to-weak-report. The "Week to Weak" report, published in late 2014, illustrates the rapid speed at which vulnerabilities are now weaponized and seen in the wild. Analysis by Recorded Future found that the median number of days for a vulnerability to be exploited is only 7.5. For reference, the report cites the National Institute of Standards and Technology (NIST) as publishing roughly 7,000 newly known vulnerabilities in 2014. This illustrates the incredible speed at which cybersecurity measures such as vulnerability management must occur to maintain risk at appropriate levels.

20. "Standards Are Making the Internet of Things Come Alive," IEEE Standards Association, 8 April 2013, http://standardsinsight.com/ieee_company_detail/standards_iot; and Dr. W. Charlton Adams Jr., "The Internet of Things and the Connected Person," *Wired*, December 2014, http://www.wired.com/insights/2014/12/iot-connected-person/.

21. Klint Finley, "Hacked Fridges Aren't the Internet of Things' Biggest Worry," *Wired*, 12 March 2015, http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/; Bill Wasik, "In the Programmable World, All Our Objects Will Act as One," *Wired*, 14 May 2013, http://www.wired.com/2013/05/internet-of-things-2/; and Dan Saffer, "The Wonderful Possibilities of Connecting Your Fridge to the Internet," *Wired*, 29 October 2014, http://www.wired.com/2014/10/is-your-refrigerator-running/.

22. If the public is not dissuaded by privacy and security concerns, consumer preference for smart devices from self-driving cars to networked refrigerators should provide supplying firms a competitive advantage. If this is the case, competitors to those "first-mover" firms may seek to adopt the same technology or develop their own, potentially commoditizing the technology itself and driving out non-adopting alternatives from the market.

23. Cade Metz, "Mavericks Invent Future Internet Where Cisco Is Meaningless," *Wired*, 16 April 2012, http://www.wired.com/2012/04/nicira/; and Klint Finley, "GE's New Cloud Must Be the Most Tempting Hacker Bait Ever," *Wired*, 5 August 15, http://www.wired.com/2015/08/ges-new-cloud-may-tempting-hacker-bait-ever/.

24. Since space operations are overwhelmingly reliant on cyberspace supremacy, several but not all of these recommendations are cyber-centric.

25. A cyber proficiency test would likely assess logic-based problem solving as well as abstract thinking, two skills required for success in cyberspace (and in space).

26. Critically, these tests should not be used to affect the career vectoring of individuals during the first several years of implementation. Over time, as the tests are refined and conclusions are able to be teased out of data points, they will become useful in making those decisions. Drawing conclusions too quickly and making vectoring decisions during the refinement process would skew the results and only lead to foregone conclusions rather than provide true insight.

27. Capt Kinder Blacke, "Intermediate Network Warfare Training Up and Running," Air Force Space Command, 3 March 2011, http://www.afspc.af.mil/news/story.asp?id=123245023; and SSgt Jarrod Chavana, "Airmen Train for 'New Wild, Wild West' in Cyber Domain," *Santa Maria Times*, 10 October 2014, http://santamariatimes.com/news/local/military/airmen-train-for-new-wild-wild-west-in-cyber-domain/article_1633ec02-eb22-54e5-ad04-f4bea53b776c.html.

28. "National Cybersecurity Workforce Framework," National Initiative for Cybersecurity Education, accessed 15 October 2015, http://csrc.nist.gov/nice/framework/.

29. In addition to being informed by the NIST standards, initial and intermediate training for enlisted Airmen should be informed by operational techniques used in the joint community, such as the plan, brief, execute, debrief (PBED) process.

30. J. R. Wilson, "Interview: Col. Robert 'Shark' Garland, Commandant, USAF Weapons School," Defense Media Network, 6 November 2011, http://www.defensemedianetwork.com/stories/interview-col-robert-%E2%80%9Cshark%E2%80%9D-garland-commandant-usaf-weapons-school/.

31. Entry into the program and placement following the program could be managed very similarly to the procedures of the USAF Weapons School, without the need to develop an entire training program that is separate from the traditional intermediate and advanced cyber courses that are specific to the graduate's mission.

32. Jim Garamone, "Winnefeld: DoD Must Strengthen Public, Private Ties," US Department of Defense, 14 May 2015, http://www.defense.gov/news/newsarticle.aspx?id=128810; and Kevin Gilmartin, "Education with Industry Program Offers Different Perspective," Air Force Print News, 14 March 2008, http://www.hanscom.af.mil/news/story_print.asp?id=123090306.

33. Cheryl Pellerin, "Carter Seeks Tech-Sector Partnerships for Innovation," US Department of Defense, 23 April 2015, http://www.defense.gov/news/newsarticle.aspx?id=128655.

34. Mark Pomerleau, "Carter Details DoD's Innovation Plans," Defense Systems, 6 May 2015, https://defensesystems.com/articles/2015/05/06/carter-dod-innovation-plans-congress.aspx; and Patrick Tucker, "Pentagon Sets Up a Silicon Valley Outpost," Defense One, 23 April 2015, http://www.defenseone.com/technology/2015/04/pentagon-sets-silicon-valley-outpost/110845/.

35. Pomerleau, "Carter Details DoD's Innovation Plans."

36. Stuart M. Butler, "How Google and Coursera May Upend the Traditional College Degree," Brookings Institution, 23 February 2015, http://www.brookings.edu/blogs/techtank/posts/2015/02/23-mooc-google-coursera-butler/.

37. Ibid.

38. In addition to partnering with the companies themselves, an examination of the underlying technology and methods may illustrate efficiencies that could be implemented in military-led training courses.

39. Jeffrey R. Young, "Will MOOCs Change the Way Professors Handle the Classroom?," *Chronicle of Higher Education*, 7 November 2013, http://chronicle.com/article/Will-MOOCs-Change-Campus/142869/.

40. Conti and Surdu, "Army, Navy, Air Force, and Cyber," 14–18.

41. Ibid.

42. Semiregularly, instructors and course developers should rotate between their respective functions to retain currency in each.

2nd Lt Chris Babcock, USAF

Lieutenant Babcock (BS, Indiana University) is the crew commander and deputy section chief for the 50th Space Communications Squadron's Air Force Satellite Control Network, Network Operations Security Center. He is a cyberspace operations officer with a special interest in network defense and intelligence integration.

Let us know what you think! Leave a comment!

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

Defending Our Satellites

The Need for Electronic Warfare Education and Training

Lt Col E. Lincoln Bonner, USAF

The US military enjoys tremendous advantages over any potential adversary because of its exploitation of space capabilities. It is of paramount importance that Air Force Space Command (AFSPC) position its Airmen to defend and protect America's space advantage in the contested space environment of the present and future. AFSPC can best develop space Airmen to win tomorrow's fight in this contested environment by significantly improving and expanding education and training in the use of electronic warfare to defend US satellites and improve their survivability.

The following discussion first describes why improving space system survivability is critical to US war fighting. It then explores and compares the role of electronic warfare in aircraft survivability to the space domain to demonstrate how prowess in electronic warfare is essential for successful defensive space control. The article next describes the current state of electronic warfare education and training for space operators. Finally, it explores suggestions for improving space leaders' readiness to win in electronic warfare in order to defend America's space advantage.

Space System Survivability and US War Fighting

The US military gains a disproportionate advantage over potential adversaries by exploiting space capabilities. Satellites provide an advantage similar to that of reconnaissance aircraft in World War I—(1) warning of enemy attack to help ensure that these attacks fail and (2) the enabling of precision strikes.[1] Additionally, satellites provide over-the-horizon communication at a combination of speed, volume, and mobility that terrestrial communications cannot match.

US military initiative—the ability to observe, orient, decide, and act more quickly and more effectively than an opponent—heavily depends upon space capabilities. US intelligence, surveillance, and reconnaissance satellites can observe far over the horizon, providing ample warning time to react to enemy moves and countermoves and help to ensure that adversary attacks fail—similar to the contributions of airborne reconnaissance in World War I. Space-based intelligence, surveillance, and reconnaissance extend that World War I airborne reconnaissance advantage, though, by providing not only time to react but also enough warning to seize the initiative and choose the time, place, and conditions of battle.

In addition to reconnaissance, satellites enable precision strikes. US advantages in massing and concentrating effective firepower from fewer units and strike platforms stem largely from the use of precision-guided munitions, which are, in turn, heavily dependent upon data provided by Global Positioning System (GPS) satellites. For example, in the 1991 Operation Desert Storm against Iraq to liberate Kuwait, 1,207 strike aircraft participated in the air campaign, approximately 4 percent of which were precision guided by laser—GPS-guided munitions were not yet available.[2] In Operation Iraqi Freedom in 2003, 772 strike aircraft participated in the air campaign—36 percent fewer than in 1991—and 68 percent of the bombs released were precision guided, principally by the GPS.[3] Newer weapons like the Small Diameter Bomb have a relatively small blast radius to limit collateral damage and become combat ineffective in many scenarios without precision guidance data from the GPS or an alternate source. US air, land, and naval forces heavily depend upon GPS information for navigating and conducting precision strikes. Even modern-day airborne reconnaissance, which provides advantages similar to those of satellite reconnaissance, heavily depends upon space capabilities.

Remotely piloted aircraft like the MQ-9 Reaper and RQ-4 Global Hawk have assumed a significant portion of the airborne reconnaissance workload. These remotely piloted aircraft leverage GPS data for navigation and guidance as well as employ secure satellite communications. These communications provide for command and control and mission-data relay to processing, exploitation, and dissemination on the ground half a world away.

No potential adversary can yet match US war-fighting advantages to seize the initiative and conduct precision strike; neither can such an enemy equal the scope and scale of US global reach. These war-fighting advantages stem from exploitation of space-based reconnaissance, precision navigation and timing, and communication. Hence, the first priority for Air Force space leaders in a contested environment is to conduct effective defensive space control operations and improve space system survivability to ensure the endurance of US war-fighting advantages flowing from exploitation of the ultimate high ground.

Electronic Warfare and Aircraft Survivability

As the Air Force quickly learned in the realm of air combat, survivability in a contested environment largely depends upon the capability to dominate in the realm of electronic warfare. Initially, prior to the invention of radar, the dominant strategy to improve bomber survivability was to use multiple engines to increase bombers' flight speed and altitude so they could not be threatened by antiaircraft guns or slower, lower-flying, single-engine fighters. However, the attrition rate that Luftwaffe Me-109 single-engine fighters inflicted on Allied bomber forces in World War II horribly demonstrated that speed and altitude alone did not provide sufficient protection.

Prior to World War II, radar did not exist; as a result, there was insufficient warning time for fighters to be launched and intercept attacking bombers before they could strike and escape. This situation changed with the development of radar, which provided the warning time and information (e.g., raid count, altitude, speed, and direction) that underpin integrated air defense. Bolstered by the warning provided by the Chain Home radar system and the speed and altitude provided by the Spitfire fighter and its Merlin engine, England's Fighter Command was able to win the fight for air superiority and blunt German bomber attacks to win the Battle of Britain.

The Allies learned the criticality of radar to effectively engaging penetrating aircraft during the Battle of Britain. As a result, they recognized that speed and altitude could not protect bombers from enemy fighters guided by radar. Ultimately, bomber survivability could be achieved only if the warning and information radar provided to enemy counterair capability could be sufficiently degraded or negated. As a result, Allied air forces initiated a concerted effort to develop electronic warfare capabilities. In 1940, immediately following the Battle of Britain, the Allies began a multiyear intelligence operation to learn everything they could about German air defense radar and communications in order to develop electronic warfare systems that could degrade or neutralize integrated German air defenses and increase Allied bomber survivability.[4] However, it would take two years for this intelligence operation to bear fruit.[5] In the meantime, US bomber strategy turned to formation tactics in the hopes of creating enough concentrated firepower from bomber self-protection guns to shield friendly aircraft from intercepting fighters. As the disastrous attack on Schweinfurt in 1943 showed, in which Allied bomber losses numbered 25 percent, either a new strategy was needed to protect Allied bombers or the Combined Bomber Offensive would fail.[6] Fortunately, the electronic warfare development effort delivered results just in time.

The Allies' new aircraft survivability strategy combined the use of electronic warfare capabilities, chaff, and airborne jammers with long-range fighter escorts to suppress German air defenses. In July 1943, Allied bombers first used chaff—thin strips of aluminum that create clutter on radar scopes.[7] Chaff degraded the performance of German ground control intercept radars used to vector Luftwaffe fighters onto attacking bombers.[8] Allied employment of airborne jammers like Airborne Cigar complemented the use of chaff. Airborne Cigar further degraded German air defenses by jamming the Lichtenstein radar aboard Luftwaffe night fighters so they could not effectively intercept Allied bombers attacking at night.[9] As a result of the electronic warfare advantage that systems like Window and Airborne Cigar bestowed upon the Allies, British bomber loss rates were cut by half compared to their average during the 1943 raids on Hamburg.[10]

The Air Force has never forgotten the importance of electronic warfare to aircraft survivability. As a result, it has developed stealth aircraft, modern jamming systems like the miniature air launched decoy jammer (MALD-J), and the high-speed antiradiation missile (HARM) to suppress and degrade enemy radar—the center of gravity of an air defense network. You cannot hit what you cannot see.

Unfortunately, the lesson of survivability and electronic warfare appears to have gone unnoticed within the Air Force's space operations community. While technology could have quickly negated the survivability that orbital altitude and velocity initially afforded, this military evolution was suspended. The two principal antagonists during the early days of space capability development—the United States and the Soviet Union—established the international convention that outer space was international territory over which sovereignty would not be asserted and unrestricted overflight of any territory would be permitted.[11] This Cold War convention preserved space as a sanctuary for over 60 years. But it also arrested development of the Air Force's space Airmen in a state analogous to that of pilots prior to World War I in which responding to system malfunctions for basic safe operations was the focus rather than surviving in the face of enemy attack. Understandably, without a credible counterspace threat over the last 60 years, improving space system survivability has not received much of Airmen's attention.

Unlike its status during the Cold War period, though, the convention of space as a sanctuary is rapidly disappearing. For example, China conducted successful antisatellite missile tests in 2007 and 2014.[12] Additionally, antisatellite electronic jammers capable of degrading the use of GPS satellites for precision navigation and strike and communications satellites are readily available.[13] More importantly, states have recognized the asymmetric advantage that US forces gain from space and are implementing military strategies designed to deprive the United States of this advantage. For example, Chinese military writings "emphasize the necessity of 'destroying, damaging, and interfering with the enemy's reconnaissance . . . and communications satellites.' "[14]

Fortunately, counterspace networks share characteristics similar to those of counterair networks that the Air Force can exploit to improve survivability of US space systems—namely, dependence on electronic surveillance and reconnaissance via radar to find, track, and engage US satellites. Like counterair capabilities, counterspace capabilities integrated into a network of sensors and shooters will likely be most effective. In the air domain, this network of sensors and shooters is known as an integrated air defense system (IADS), and the extension of this war-fighting concept to space is the logical next step for potential adversaries seeking to deny the US military the advantage from the high ground of space.

An IADS is composed of several components to find, track, and engage aircraft to complete the kill chain. First, there are early warning radars that find aircraft and provide course speed, direction, and altitude information about incoming aircraft. Data from multiple early warning radars are fused into rough tracks and passed on to tracking and engagement radars. These more precise tracking radars then perform focused searches with early warning radar information as the starting point to refine the speed, direction, and altitude information about incoming aircraft. When tracked aircraft enter the lethal envelope of shooters, these aircraft are engaged with antiaircraft missiles that are terminally guided by radar or electro-optical sensors, typically housed on board the missile. Only if all of these steps are achieved successfully can the target aircraft be destroyed. Note that for each aspect of the find, track, and engage elements, a successful counterair engagement depends upon effective electronic surveillance—either electro-optical or radar. The ability of Air Force aircraft to survive in the presence of an IADS largely depends upon the capability to conduct effective suppression of enemy air defenses (SEAD) operations via stealth, kinetic strike, and electronic jamming to blind or deceive the IADS's electronic sensors.

Since World War II, US SEAD capabilities have grown in sophistication from releasing strips of aluminum (chaff) into the air to today's MALD and MALD-J systems.[15] In addition to jamming, the US military has developed kinetic strike options to destroy and suppress, by threat of destruction, enemy counterair systems by combining the capability to electronically locate enemy threat radars with high-speed missile technology, resulting in the HARM and its companion HARM Targeting System.[16] In addition to SEAD jamming and strike operations, self-protection jamming is another element of the electronic warfare system of systems that improves US aircraft survivability. Air Force systems like the ALE-50 towed decoy and Large Aircraft Infrared Counter-Measure (LAIRCM) are designed to degrade the performance of terminal guidance radar and electro-optical sensors housed within missile seekers.[17] Aircraft survivability in a contested environment has depended on superiority in electronic warfare going back to World War II—so too will it be in the contested space environment that the United States now faces.

Like an IADS, the effectiveness of potential adversaries' counterspace networks will depend upon electronic surveillance by radar and electro-optical sensors to find, track, and engage adversary spacecraft. Multiple countries already field networks of sensors, Space Object Surveillance and Identification (SOSI) radars, and telescopes in an effort to keep, find, and track satellites and debris in Earth orbit. Russia, China, and the United States each possess a network of SOSI sensors capable of finding and tracking spacecraft. The way the Air Force is likely to protect US spacecraft is through the conduct of suppression of adversary counterspace capabilities (SACC), which "neutralizes or negates an adversary offensive counterspace system through deception, denial, disruption, degradation, and/or destruction."[18] Like SEAD, success in SACC to protect US satellites will likely depend on the Air Force's capability to conduct successful electronic warfare operations to jam and strike adversary counterspace network sensors (i.e., SOSI sensors). Today, SOSI sensors are generally large, immobile facilities, so tactical systems to electronically locate them—like the HARM Targeting System—are typically unnecessary, but SOSI sensors can be expected to evolve to become smaller and more mobile, just as IADS sensors have over time. As this evolution occurs, the conduct of successful electronic warfare operations to locate and jam mobile SOSI systems and their companion counterspace strike batteries in support of SACC will become simultaneously more important and more challenging.

However, suppression of enemy counterspace alone will be insufficient to adequately protect US satellites. Spacecraft survivability, like aircraft survivability, will depend upon a system-of-systems approach that incorporates suppression operations as well as self-protection electronic jamming and possibly stealth technology to defeat counterspace systems at the point of engagement. Decoy and countermeasure systems like the ALE-50 and LAIRCM will be needed to defeat an antisatellite missile's terminal guidance sensors and protect targeted spacecraft from being destroyed by counterspace batteries that continue to function despite suppression efforts. Furthermore, while stealth technology could theoretically improve spacecraft survivability exponentially, as it has for aircraft, basic satellite operations requirements for heat management and power generation using large solar arrays suggest that a stealth satellite is unlikely to emerge with today's technology.

In addition to the antisatellite missile threat, there are additional attack vectors against US satellites that manned aircraft are far less vulnerable to: cyber attack, kinetic strike on space system ground segments, and link jamming against both the command uplink and/or the data downlink. The fact that satellites are basically sophisticated robots/drones flying in space creates these additional vulnerabilities. Fortunately, there is a massive focus on cyber defense within AFSPC. AFSPC's Twenty-Fourth Air Force, the Air Force component to US Cyber Command, as well as the larger Air Force are in the midst of a massive recruiting, education, and training effort, the objective of which is to rapidly grow Airmen with the knowledge and expertise to defend Air Force assets from cyber attack. While Air Force space operators need to have knowledge of how cyber attacks could affect their systems, space operations will primarily find themselves in a supported role relative to cyber defense. Consequently, space operators do not need deep knowledge in cyber warfare at present, much as infantry does not need deep knowledge of air operations since the infantry most often finds itself in a supported role whereby it primarily needs to understand the effects that air operations can bring to bear. The same is true for space operators regarding cyber operations, and an introductory, familiarization-level of knowledge of cyber operations should suffice for space operators through broad courses like Undergraduate Space Training and Space 200/300. However, space operators require a significantly higher level of knowledge in electronic warfare because they will be directly engaged in it in order to protect their spacecraft.

Satellites are operated by personnel on the ground who send commands to the spacecraft via an electronic uplink. If this command uplink were to be successfully attacked electronically, a satellite would be rendered useless—if not immediately, then certainly over time. Moreover, because satellites' principal value is derived from the information they are able to acquire and communicate from their overhead vantage point and because that communication is via a wireless, electronic downlink to the ground, then effective electronic attack on that downlink immediately takes space systems out of the fight. For instance, jammers targeting the downlink from GPS satellites prevent users from receiving accurate and useful precision navigation and timing information from the spacecraft. However, if effective electronic support could be employed to geolocate and characterize enemy jammers, they could be destroyed, avoided, and negated via adaptive, real-time filtering or otherwise defeated by other electronic protection tactics like increasing transmitter power. Regardless, it is evident that skill in electronic warfare lies at the heart of successful defense against link jamming attacks on space systems.

Like aircraft survivability, spacecraft survivability will likely hinge on the ability to gain superiority in electronic warfare. To ensure space system survivability in a contested environment, space operators will have to holistically employ an electronic warfare system of systems comprised of electronic jammers and electronic countermeasures designed to degrade and defeat enemy SOSI systems and terminal guidance sensors of antisatellite weapons; electronic support equipment to geolocate and characterize enemy link jammers so they can be destroyed or otherwise neutralized; and electronic protection capabilities to defeat electronic attacks on friendly satellites. If the United States wants to protect its satellites in a contested space environment, it is paramount to achieve superiority in the corresponding electronic warfare battle. Yet, despite the centrality of electronic warfare to defensive space control operations, few Air Force space operators have any training in the fundamentals of electronic warfare, and those who do typically have only an introductory level of knowledge or a very specialized set of training centered on link jamming rather than breaking the kill chain of adversary counterspace capabilities, the center of gravity of which is radar.

Conclusion and Recommendations

Fortunately, this shortfall in electronic warfare education and training for space operators can be readily alleviated. Several potential courses of action exist that could address the deficiency of the Air Force's space operations cadre in electronic warfare skill. First, the introductory electronic warfare course currently taught at the Advanced Space Operations School could be expanded to more fully address electronic warfare in relation to radar and electro-optical/infrared sensors that form critical parts of potential adversaries' counterspace kill chains. Alternatively, this introductory electronic warfare course could be folded into Undergraduate Space Training to ensure that all space operators possess a basic level of electronic warfare knowledge from which to develop effective defensive space control capabilities, tactics, techniques, and procedures. Third, response to electronic attack should become a focus area of initial weapon system qualification training for space operators as well as a focus area of recurring training and exercises. Finally, and perhaps most importantly, AFSPC should consider developing a cadre of space electronic warfare officers (EWO) who attend the relevant portions of the Air Force's initial training for its rated combat systems officers and EWOs. A logical group to form this cadre would be the space weapons officers, and the most logical time to receive this training would be immediately prior to attending the Space Weapons Instructor Course. This space EWO cadre should be developed with the view that over the long term, space EWOs should make up the majority, if not the entirety, of the space operations career field.

Space operator education and training historically has been rooted in conducting routine spacecraft flight operations and executing emergency procedures in response to satellite malfunctions. In the contested space environment the Air Force now faces, planning and executing electronic warfare operations absolutely must become a space operations core competency on par with traditional flight safety tasks. If the Air Force's space leaders and operators are not prepared to fight and win in electronic warfare, the tremendous war-fighting advantages that the US military enjoys from space will be at grave risk. ✪

Notes

1. Lee Kennett, *The First Air War: 1914–1918* (New York: Free Press, 1991), 220.

2. Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington, DC: Office of the Secretary of the Air Force, 1993), 199; and Carl Conetta, Project on Defense Alternatives Briefing Memo no. 30, subject: Catastrophic Interdiction: Air Power and the Collapse of the Iraqi Field Army in the 2003 War, 26 September 2003, 2, http://www.comw.org/pda/fulltext/0309bm30.pdf.

3. Lt Gen T. Michael Moseley, *Operation IRAQI FREEDOM—By the Numbers* (Shaw AFB, SC: USCENTAF, 30 April 2003), 6, 11, http://www.afhso.af.mil/shared/media/document/AFD-130613-025.pdf.

4. Alfred Price, *Instruments of Darkness: The History of Electronic Warfare*, new expanded and updated ed. (London: Macdonald and Jane's, 1977), 77.

5. Ibid., 81–86, 93–95.

6. Cited in Maj Greg A. Grabow, "Schweinfurt Raids and the Pause in Daylight Strategic Bombing" (master's thesis, US Army Command and General Staff College, 2008), 56.

7. Price, *Instruments of Darkness*, 163.

8. Ibid., 164.

9. Randall T. Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command* (Toronto: University of Toronto Press, 2009), 155.

10. Ibid., 139; and Price, *Instruments of Darkness*, 151–60.

11. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (signed at Washington, London, Moscow, 27 January 1967), Art. II, US Department of State, accessed 14 October 2015, http://www.state.gov/t/isn/5181.htm.

12. Colin Clark, "Chinese ASAT Test Was 'Successful': Lt. Gen. Raymond," *BreakingDefense*, 14 April 2015, http://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/; and Leonard David, "China's Anti-satellite Test: Worrisome Debris Cloud Circles Earth," Space.com, 2 February 2007, http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.

13. Cited in Maj Brian Garino and Maj Jane Gibson, "Space System Threats," in AU-18, *Space Primer*, prepared by Air Command and Staff College Space Research Electives Seminars (Maxwell AFB, AL: Air University Press, 2009), 276, http://aupress.maxwell.af.mil/digital/pdf/book/AU-18.pdf; and cited in Maj Dewitt Morgan III, "Space Power: A Critical Strength . . . and a Critical Vulnerability of the US Military," research report (Newport, RI: Naval War College, 10 May 2007), 11.

14. 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), 14–15, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

15. "Miniature Air Launched Decoy (MALD)," Raytheon, accessed 21 July 2015, http://www.raytheon.com/capabilities/products/mald/.

16. "High Speed Anti-radiation Missile Targeting System," US Air Force, 18 October 2007, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104602/high-speed-anti-radiation-missile-targeting-system.aspx.

17. "B-1B Lancer," US Air Force, 29 September 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104500/b-1b-lancer.aspx; and Capt Lauri Turpin, "Large Aircraft Infrared Countermeasures— LAIRCM," Pope Field, 2 May 2009, http://www.pope.afrc.af.mil/news/story.asp?id=123147362.

18. Curtis E. LeMay Center for Doctrine Development and Education, "Defensive Space Control," in "Annex 3-14, Space Operations," 19 June 2012, [4], https://www.doctrine.af.mil/download.jsp?filename=3-14-D34-SPACE-OPS-DSC.pdf.

Lt Col E. Lincoln Bonner, USAF

Lieutenant Colonel Bonner is commander of a space operations squadron at Aerospace Defense Facility–Colorado. He has also served as an airpower strategist at Headquarters Air Force and has held assignments as a space operator performing space-based missile warning and as a flight test engineer. He is a graduate of the Massachusetts Institute of Technology, the US Air Force Test Pilot School, Air Command and Staff College, and the School of Advanced Air and Space Studies—the Air Force's school for strategy. He holds a bachelor's and master's degree in aerospace engineering and is currently an Air University candidate for a doctorate of philosophy in military strategy.

Let us know what you think! Leave a comment!

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

Developing Tomorrow's Space War Fighter

The Argument for Contracting Out Satellite Operations

Maj Sean C. Temple, USAF

> *So when any environment comes under threat, what we have to do is we have to figure out how to fight through that threat and continue to provide operational capability, and that's the fundamental first priority of our command today.*
>
> —Gen John E. Hyten
> 2015 National Space Symposium

To date, space has been a fairly unchallenged environment to work in. The threat, however, is growing. As General Hyten stated, the priority of Air Force Space Command (AFSPC) is to continue to provide operational capability, even in a threatened environment. As the chance of a war in space intensifies, developing AFSPC personnel who are equipped to "win tomorrow's fight" will be increasingly necessary. Tomorrow's space war fighter will need to possess a broad range of skills to deal with potential threats to our space systems. As we move forward, our focus needs to move from operating satellites in an uncontested setting to ensuring that satellite effects are available even in a congested, contested, and competitive space environment.[1] *To develop space war fighters who are educated, experienced, and prepared to win tomorrow's fight, AFSPC should contract out day-to-day satellite command and control and shift the space operator's focus to defending our nation's space assets.*

War in Space

> *War in space would destroy the intrinsic trust and cooperation necessary to maintain these systems, and combat itself in space would produce debris that would destroy the satellites, seriously ending the possibility of using space for peaceful purposes.*
>
> —Helen Caldicott and Craig Eisendrath
> *War in Heaven: The Arms Race in Outer Space*

The United States has made it clear in policy that it has no wish to fight a war in space. According to the 2011 *National Security Space Strategy*, "We seek a secure space environment in which responsible nations have access to space and the benefits of space operations without need to exercise their inherent right of self-defense."[2] The launch of an antisatellite weapon by China in 2007, however, highlighted that there is a need for countries to be able to defend themselves.[3] It also highlighted the devastating effects that a war in space could produce. This single event created more than 3,000 pieces of debris in low Earth orbit that will take an estimated 100 years to dissipate.[4] Each piece of debris, travelling at speeds of more than 17,000 miles per hour, has the potential to physically destroy a satellite on impact.[5] Imagine several of these antisatellites being used simultaneously in different orbits; the effects to the space environment would be catastrophic, both militarily and commercially.

Additionally, there are many nonkinetic threats that can be used to interfere with space capabilities. While nonkinetic effects are usually reversible (i.e., causing no permanent damage to the satellite), they have the ability to take our space systems out of the fight in a conflict. Jammers, laser dazzling, spoofing, and cyber attack are but a few of the methods that can prevent a satellite from delivering operational capability. This is the type of environment that tomorrow's war fighter needs to be prepared to fight in and through.

Defending space systems is not a simple task. As a 2008 Council on Foreign Relations special report states, "Satellites' predictable orbits make them vulnerable to a variety of offensive counterspace technologies that are growing more sophisticated and capable over time. In space, offense has a major advantage over defense."[6] The United States arguably has the most to lose in a war in space, which puts it in the difficult position of having to defend our space systems. As adversary offensive counterspace technologies continue to evolve and become increasingly effective, it is imperative that we educate our space war fighters on their capabilities and potential ways to counter them.

Developing Tomorrow's Space War Fighter

> *We will improve the ability of U.S. military and intelligence agencies to operate in a denied or degraded space environment through focused education, training, and exercises and through new doctrine and tactics, techniques, and procedures.*
>
> —2011 *National Security Space Strategy*

To be ready for the challenges of tomorrow, space war fighters must have a better understanding of the art and science of war in space and must have the systems to support them. Now is the time to develop doctrine and train space professionals for tomorrow's conflict. This education needs to occur early and often in the careers of our space professionals. Now is the time to start developing systems with advanced defensive capability. We should begin preparing tomorrow's space cadre by focusing education in areas that will make them better space war fighters instead of just better space operators.

The Space War Fighter Needs to Have a Solid Understanding of Threats That Are Out There, Both Kinetic and Nonkinetic

Anything that can degrade, disrupt, deny, or destroy our operational space capability should be known and understood by the space war fighter. Space war fighters need to have the appropriate clearance level and access to classified information to stay current on threats. This includes space war fighters who develop requirements and acquire space systems.

The Space War Fighter Needs to Be Educated on Ways to Counter the Enemy Threat

It is not enough to know the threat; space war fighters need to be well versed on defensive tactics. They should have a technical understanding of defensive counterspace operations and how to implement them. As they work with specific weapons systems, they should learn which defensive tactics can be applied to their weapons system and which ones can't because of operational or technical limitations. War fighters should have potential threats to their system at the forefront of their minds, constantly thinking about new ways to counter them or operate through them.

The Space War Fighter Needs to Have a Solid Understanding of Our Space Systems and Their Capabilities

All space professionals should know, in general, what space systems are out there and what mission they perform. As personnel work with specific weapons systems, they should learn the specific capabilities provided by the system and why it is vital to the war-fighting effort. They should develop tactics, techniques, and procedures to ensure that the capability is available in a denied or degraded space environment, even if the capability no longer comes from space. War fighters should practice counterspace capabilities on their system so they are ready when called upon.

The Space War Fighter Needs to Have a Solid Understanding of the Space Environment

From orbital mechanics to the electromagnetic spectrum, understanding how space works and how it is different than the terrestrial environment is key to developing war fighters who can defend our systems in space. According to Simon Worden, "It is more important that all space professionals be versed in orbital dynamics mathematics than being able to recite the elements of total quality management."[7] While a technical degree may not be necessary for today's space operator, it will become increasingly important that we recruit technically minded individuals who can understand the complexities of space.

The Space War Fighter Needs to Have a Solid Understanding of Space Policy and Direction

War fighters need to understand what our country defines as acceptable behavior in space. War fighters need to understand the impact that counterspace actions could have on the larger picture. For instance, maneuvering several Global Positioning System (GPS) satellites to avoid a questionable space object could affect GPS accuracies that civilians depend on. Along with an understanding of policy, space war fighters need to have a clear chain of command and control. They need to be empowered to take action to defend our satellites within well-defined boundaries.

The Space War Fighter Needs to Have the Experience and Knowledge to Develop Quality Space Systems

As space professionals progress in their careers, they will likely be involved in developing the next generation of space systems. The experience they gain as space war fighters will aid them in developing good requirements. Such development must take into account the potential vulnerabilities of the system and attempt to minimize those vulnerabilities using the space war fighter's knowledge of defensive counterspace options. Space war fighters must also be intimately involved in the acquisition of more robust, capable, and survivable space systems. The space war fighter cadre should include acquisition personnel who will spend their careers acquiring for space.

The Space War Fighter Needs to Be Integrated

Defending space will be a team effort that will involve contributions of the intelligence community, commercial partners, and allied countries to the common defense. Tomorrow's war fighter needs to understand the risks and benefits of partnering with other organizations and utilize them to the maximum extent practicable.

The Space War Fighter Needs to Focus on Space as a Contested Environment

Space war fighters must focus on counterspace operations to ensure that our nation's space assets are available when needed. They need to be prepared to help defend our allies and commercial assets from potential threats. Simulations and exercises need to be done frequently and with realism. Space war fighters need to have the resources available to accurately simulate possible threats and to test and validate tactics, techniques, and procedures.

Contracting Out Satellite Operations

> *We will build a more diverse and balanced workforce among military, civilian, and contractor components. These professionals must be educated, experienced, and trained in the best practices of their field—whether it is planning, programming, acquisition, manufacturing, operations, or analysis.*
>
> —2011 *National Security Space Strategy*

Developing tomorrow's space war fighter will take time, training, and a refocus toward space as a war-fighting domain. Where does one find the time to do this when all of his or her energy is spent training, certifying, evaluating, and operating satellites? One answer is to contract out day-to-day satellite operations and remove the myriad of requirements that satellite operations bring with them. Having military personnel perform satellite operations is both inefficient and unnecessary.

Because AFSPC falls under the United States Air Force, it is natural that one would expect space operators to "fly" satellites in the same way that a pilot flies a plane. The actual process of maintaining a satellite on orbit is much different. A satellite is repositioned, reconfigured, and updated by sending commands through a data link from the ground to the satellite. Every command sent to a satellite needs to be carefully developed, thoroughly reviewed, and appropriately tested to ensure that there are no adverse effects on the satellite. A bad command sent at the wrong time could cause a catastrophic loss of a multi-billion-dollar system. To develop and/or modify these commands, many satellite programs depend on contractor expertise. Often, the contractor that built the satellite is the only one with the knowledge and technical ability to create commands. Once the satellite is built, these commands are then passed to the military operator, who uploads them to the satellite at the appropriate time.

Having Military Personnel Operate Satellites Is Inefficient

Military space operators must go through months of generalized training on how to operate a satellite, how to use command and control software, how to run checklists, and so forth. Once this training is finished, the military operator gets more specialized training on his or her specific systems. All of this training takes time, facilities, and a cadre of experienced instructors. Additionally, because of the sensitive nature of the job (commands are sent to very expensive satellites), the operators must be constantly evaluated on their proficiency, certified, and medically cleared for operations. Even with all of this training, most operators have far less knowledge of how the system works than their support contractor, who has been doing the job for years. We spend a lot of time and money developing technical orders and checklists to make operations more manageable for military operators and to reduce the chance of an error. Finally, after our military personnel are fully qualified and have some experience operating their satellite, we move them to a different job. Whether it's moving to a back shop of the squadron (such as the scheduling section), to an evaluator/instructor position, or to a new satellite system entirely, operators are rarely in place long enough to take advantage of all the training they have received.

A primary cause of the inefficiencies in our current system is the constant turnover of military personnel. By having contractors take over operations, we can eliminate much of this turnover. Contractors would still have to go through a rigorous initial training process prior to taking over satellite operations; however, they would have to do this training only one time and only for the system they operate. Because turnover would be much reduced, contract operators wouldn't require an army of instructors/evaluators that changes every few months. A few highly trained contractor personnel could train newcomers and ensure the proficiency of existing operators. The 24/7 engineering support currently provided to military operations personnel could also be much reduced. A contract operator with continuity and detailed technical understanding of the system should rarely need to rely on on-call support.

Further efficiencies can be gained by adding interoperability and automation as well as by streamlining processes for our Air Force's satellite command and control systems.[8] According to a 2013 Government Accountability Office (GAO) report, "While commercial companies use computer programs to perform routine tasks, the Air Force typically uses human operators. Increasing automation for routine control functions could reduce Air Force personnel costs, and the potential for human errors."[9] The contractor should have sufficient incentive to develop systems and/or processes, with government oversight and approval, that optimize satellite commanding. One operator can do the job of many if the processes are mostly automated. In fact, some commercial companies have gotten to the point where they can control up to 15 satellites with just one operator at a time.[10]

Having Military Personnel Operate Satellites Is Unnecessary

On the one hand, many of our Air Force pilots are required to operate their aircraft where the threat of losing their lives is quite possible. Other military operators are in control of weaponry that can have lethal and devastating effects. Space operators, on the other hand, are under no direct threat. Most of our satellite operations are performed from within US borders. Additionally, while the operational effects from space are critical to the military and civilian population alike, there are no direct lethal effects delivered from satellites. Ultimately, there is no military necessity for satellite operators to be military personnel. Commercial satellite operators provide very similar command and control services for commercial satellites every day, and, returning to the first point, they do so far more efficiently. Again, the 2013 GAO report summarizes the situation well: "While commercial satellites and Air Force satellites can greatly differ in their missions, and to some extent may differ in their need for information security, basic satellite control operations functions of most of these satellites are generally the same, allowing trusted practices from the commercial sector to be applicable to many Air Force satellite programs."[11]

Transitioning to Contracted Operations Is Not without Its Risks

Contract operators should be mainly focused on performing day-to-day operations and meeting the requirements of their contract while military personnel should be focused on overseeing the contractor and developing defensive tactics to keep their satellite available. If both are to do their jobs well, a high degree of integration must exist between the military and the contractor. The space war fighter must work with the contractor to define what the satellite's defensive triggers are, what defensive options can be executed, and under what constraints. The military needs to be able to integrate defensive counterspace into the command and control processes of the contractor so that options can be implemented quickly in a crisis. All systems will require competent government oversight and approval to ensure that systems are being operated in the best interests of the government.

Summary

Tomorrow's space war fighter needs to be educated, experienced, and prepared to win tomorrow's fight in space. Performing daily satellite command and control operations does not prepare our forces for that fight. To start the transition from space operators to space war fighters, we should take the following steps:

1. Start transitioning to contractor satellite operations where feasible.
2. Transition space operators to a contractor oversight role, and shift their focus to defensive counterspace operations.
3. Reinvigorate space education to focus on the skills that tomorrow's space war fighter will need (see "Developing Tomorrow's Space War Fighter," above).
4. Enhance training/simulation/exercises to develop space war fighters' thinking and to test space-war-fighting capabilities.
5. Utilize the development of space war fighters' expertise to define and acquire the next generation of defensible space systems.

In these fiscally and manpower-constrained times, finding more efficient ways to operate is critical. It already takes an army of on-site and factory engineers to do the analysis and develop the commands that our military space operators rely on. In fact, many of our systems could not be operated without contractor expertise. Removing the military as the middleman in satellite operations is one area where we can generate huge gains in efficiency. By contracting out satellite operations, we can free up time for our military personnel to focus on learning about the threats to our space systems and planning for their defense. ✪

Notes

1. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy: Unclassified Summary* (Washington, DC: Department of Defense and Office of the Director of National Intelligence, January 2011), 1, http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.
2. Ibid., 4.
3. Bruce W. MacDonald, *China, Space Weapons, and U.S. Security*, Council Special Report no. 38 (New York: Council on Foreign Relations, September 2008), 5, http://i.cfr.org/content/publications/attachments/China_Space_CSR38.pdf.
4. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy*, 2; and MacDonald, *China, Space Weapons, and U.S. Security*, 6.
5. MacDonald, *China, Space Weapons, and U.S. Security*, 5.
6. Ibid., 32.
7. Simon P. Worden, "Future Strategy and Professional Development: A Roadmap," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes and Peter L. Hays (Fort Lesley J. McNair, Washington, DC: Institute for National Strategic Studies, National Defense University, 2011), [580], http://www.dtic.mil/dtic/tr/fulltext/u2/a546585.pdf.
8. US Government Accountability Office, *Satellite Control: Long-Term Planning and Adoption of Commercial Practices Could Improve DOD's Operations* (Washington, DC: US Government Accountability Office, April 2013), 19, http://www.gao.gov/assets/660/654011.pdf.

9. Ibid., 20.
10. Ibid., 18–19.
11. Ibid., 19.

Maj Sean C. Temple, USAF

A graduate of the US Air Force Academy and Auburn University–Montgomery, Major Temple is the chief of space control and space situational awareness programs at Headquarters Air Force Space Command. Career highlights include 4th Space Operations Squadron engineering flight commander, flight commander / instructor at the Air and Space Basic Course, and multiple program management positions at the Space and Missiles Systems Center.

Let us know what you think! Leave a comment!

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

Reconsidering the American Way of War: US Military Practice from the Revolution to Afghanistan by Antulio J. Echevarria II. Georgetown University Press (http://press.georgetown.edu/), 3240 Prospect Street, NW, Suite 250, Washington, DC 20007, 2014, 219 pages, $49.95 (hardcover), ISBN 978-1-62616-139-9; $29.95 (softcover), ISBN 978-1-62616-067-5.

In his latest work, Dr. Antulio Echevarria, a leading Clausewitz scholar, applies some of the Prussian's theories to the controversial historical subject the "American Way of War." As any student of military history knows, several notable writers over the past few decades have tried to pigeonhole how and why America fights. Some claim that we use massive firepower or overwhelming numbers—or that we even rely on irregular warfare to fight our enemies. All of these theories have large holes in them, and Echevarria uses Clausewitz to show that the only common thread of American conflict is politics. Readers should keep in mind that "politics" does not necessarily refer to how our leaders are shown on cable news but how they choose to exert their ideas and power.

Reconsidering the American Way of War consists of three parts. The first examines the current body of knowledge regarding an American way of war and various scholarly ideas, including the myth of strategic culture; it also analyzes military art. The second part, which makes up the bulk of the work, is a brief synopsis of every conflict in which the United States has been involved, from the colonial era to the war on terror. This section in itself is worthwhile because Echevarria covers over 200 years of warfare in fewer than 100 pages without missing a conflict and examines the how/why of America's involvement. Finally, he briefly ties the conflicts together by concluding that the United States conducted every conflict based on the political ramifications of the time. Sometimes overwhelming force was required and used, sometimes America sought wars of attrition, and sometimes a minimal footprint became the political choice. If the work has a fault, it is that Echevarria does not elaborate on this point. To readers who have studied Clausewitz and understand his maxim that war is an extension of policy, the conclusion makes sense, and Echevarria's historical synopsis reinforces that point. However, someone unfamiliar with the Prussian may not as easily connect the dots.

Despite this shortcoming, *Reconsidering the American Way of War* is brief, to the point, and—most importantly—readable. Echevarria takes some complex ideas and simplifies them so a layperson can use this study as an introduction to US military history. Nonscholars may choose to skip the discussions on strategic culture and military art since the text can be a little tedious and is not essential to understand either the work or the author's conclusions. The book is a must for military historians but would also be appropriate for all military members who wish to learn about their heritage and how their country chooses to employ the force that they provide.

(Academic integrity note: Dr. Echevarria was the adviser for my master's degree in military history capstone work.)

Capt Ian S. Bertram, USAF
Kirtland AFB, New Mexico

Predator: The Secret Origins of the Drone Revolution by Richard Whittle. Henry Holt and Co. (http://us.macmillan.com/henryholt), 175 Fifth Avenue, New York, New York 10010, 2014, 368 pages, $30.00 (hardcover), ISBN 978-0-8050-9964-5; 384 pages, $18.00 (trade paperback), ISBN 978-1-2500-7479-9.

Richard Whittle's new book *Predator* is worth reading for both skeptics of remotely piloted aircraft (RPA) and advocates of this technology. *Predator* traces the RPA's journey from experimental technology demonstrations in the 1970s to the modern battlefields in the war on terror. The operational successes and failures he describes say as much about the organizational dynamics in government as the technological genius of the system's designers.

Told from the point of view of its participants, *Predator* describes the technological innovations that made RPA operations such a vital aspect of American airpower today. Starting with the chief engineer and visionary, Abe Karem, the book describes how a few dedicated pioneers overcame a myriad of technological and organizational challenges. Many of the solutions they developed were imperfect, and the system today is burdened by the legacy of several earlier technological shortcuts, particularly in human-machine interface. Nevertheless, it soon became clear that "Predator's biggest problem is political" (p. 118). Whittle shows how a few relentless innovators, facing staunch institutional resistance, overcame obstacles to meet a compelling mission need. Unfortunately, Whittle ends the story in 2003, before many of the political battles over RPAs had fully evolved, but his focus clearly remains on the story of innovation and determination that brought Predator to the battlefield.

Beyond the history of innovation it describes, this book vividly depicts the way organizational processes contorted to accommodate this new technology. From the failure to strike Osama bin Laden before 9/11 and the failed attack on Mullah Mohammed Omar in 2001 to the attack on Mohammed Atef in 2002, Whittle cuts through self-interested accounts from various participants in these events. He highlights the increasing dangers of centralized execution on the modern battlefield with examples of strategic leaders micromanaging events via real-time video. By describing the various combinations of hand wringing and conflicting guidance, Whittle also details how the lack of clear authorities bred complacency in some individuals and a tendency to overcentralize authority in others.

It might be tempting to dismiss the command failures detailed in this book as isolated events or assume that any interagency effort requires this type of contorted supervisory structure. While worldwide networking of the Predator's video feed gives strategic leaders visibility of the battlefield from an unprecedented distance, the temptation and the danger of myopia are nothing new. One does not need the wisdom of Napoleon to recognize that strategic leaders can control the fine details of a battle only by abandoning their broader perspective. The leaders in this story failed to establish appropriate lines of authority and responsibility—essential to effective delegation. Whittle's narrative provides a valuable addition to the historical examples of the principle of war known as unity of command. In this case, senior leaders failed to adapt to this new technology—a failure that should inform the ongoing debate about the proper command structure for RPAs.

The proliferation of RPA technology in the last two decades has far exceeded the expectations of even its most zealous advocates when the US Air Force assumed control of the mission in 1995. *Predator* offers valuable lessons for anyone who claims or aspires to be a part of the decision-making process in the application of military power. This hard-hitting story of innovation shows how technology brings out the best and worst in the American government and its military.

Lt Col Cameron S. Pringle, USAF
US Naval War College

The Spirit of Attack: Fighter Pilot Stories by Bruce Gordon. AuthorHouse LLC (http://www.authorhouse.com), 1663 Liberty Drive, Bloomington, Indiana 47403, 2014, 116 pages, $34.99 (softcover), ISBN 978-1-49184-603-2.

In *The Spirit of Attack*, author Bruce Gordon, a former US Air Force major with 4,249 total hours of flying, takes the reader into the cockpit with him during gripping night-bombing runs over South Vietnam, tense scrambles to meet Soviet bombers penetrating American airspace during the Cold War, and many more exciting missions. This entertaining book collects more than 40 fighter pilot stories written by Gordon and a few fellow pilots who detail their aerial adventures from World War II through the Cold War. Also included are more than 90 photos that illustrate many of the aircraft they flew and fought against.

Gordon has a superb storytelling style, making the reader feel as if he or she is sitting next to him as he vividly recalls his vast collection of Air Force memories. The stories can be a bit disjointed and sometimes appear to lack a clear narrative, but they do follow a gradual progression through Gordon's early life and career, from experiencing the Pearl Harbor attack on Hawaii as a child, to basic pilot and jet training, Cold War assignments in Alaska and Michigan, and combat missions over Vietnam. Since all of the stories are only a few paragraphs long, they hold the reader's interest and allow for experiencing a wide variety of accounts in one sitting. Near the end of the book are a few stories from fellow pilots, including notable contributions from Philip Payne detailing his aerial observation of a nuclear detonation in the Nevada desert and Ray James describing a visual reconnaissance mission over the Ho Chi Minh Trail in Vietnam.

The title of the book comes from the former 317th Fighter Interceptor Squadron motto, adopted in turn from a quotation by Adolf Galland, the Luftwaffe's General of Fighters during World War II: "Only the spirit of attack borne in a brave heart will bring success to any fighter aircraft, no matter how highly developed the aircraft may be" (p. 15). Many of Gordon's stories refer to this "spirit of attack," a fighter pilot's innate, aggressive desire to seek out and destroy the enemy. Gordon's fighter pilot bravado shines through when he discusses the spirit of attack; nevertheless, such confidence is not excessively displayed and is quite understandable (and perhaps necessary) given the deadly and dangerous business of being a fighter pilot.

The Spirit of Attack will appeal to readers interested in hearing firsthand what it was like to fly training and combat missions in Vietnam and at the height of the Cold War. The personal nature of these stories offers a unique individual perspective to complement the more typical operational- and strategic-level histories of the Vietnam and Cold Wars. In that sense, herein lies the real strength of the book. As the Vietnam and Cold War era passes further into history (this year marks 40 years since the fall of South Vietnam), *The Spirit of Attack* preserves the proud heritage of these fighter pilots and is a welcome read for any military aviation enthusiast.

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

Every Citizen a Soldier: The Campaign for Universal Military Training after World War II by William A. Taylor. Texas A&M University Press (http://www.tamupress.com), John H. Lindsey Building, Lewis Street, 4354 TAMU, College Station, Texas 77843-4354, 2014, 232 pages, $39.95 (hardcover), ISBN 978-1-62349-146-8.

As a thorough military history, William Taylor's *Every Citizen a Soldier* offers something for everyone. His portrayal of the quest for universal military training (UMT) goes beyond the rationales of the senior Army leaders who proposed it by examining the social, political, and even religious factors that combine to shape national military policy in the United States. At the conclusion of the Second World War, the idea of UMT—the mandatory year-long training of every 18-year-old male not physically disqualified—swept the nation. *Every Citizen a Soldier* proceeds chronologically and thematically through the jungle of military manpower debates in the early twentieth century to illuminate this striking concept. The author introduces the initial proposals for UMT that emerged after the First World War and traces their progress up to 1943, when US Army leaders embraced them in earnest (p. 26). Taylor demonstrates how UMT became central to War Department plans for the postwar era and argues that this singular focus ultimately brought about the failure of the policy altogether (p. 32).

Army leaders fought hard for the establishment of UMT, drafting press pieces, enlisting the support of civilian organizations, and even recruiting sympathetic chaplains to persuade religious authorities, but as their message spread, so did concern about and opposition toward the plan. Negative responses forced proponents into an increasingly reactionary narrative, and they began to slowly lose control of their message. Taylor leaves none of these facets unexplored and even dedicates an entire chapter to the "Fort Knox Experiment" designed by the Army to showcase the attainability of UMT through small, highly successful units of trainees known as "Umties" (p. 112).

Beginning in 1945, the Truman administration restructured the UMT proposal with heavy emphasis on education, health care, and vocational development; consequently, it began to lose the purely military function that Army leaders had envisioned. However, according to Taylor, the greatest hurdle to UMT's legislative success was the sense of urgency the War Department had manifested in the minds of citizens, a phenomenon the author terms the "paradox of preparedness" (p. 171). In the political climate of 1948, citizens and legislators saw an immediate security problem that UMT could not solve and opted instead for Selective Service as a short-term fix. With this task completed, the urgency fell away, and UMT would never regain the momentum necessary to become a reality (p. 171).

Every Citizen a Soldier is a lively telling of an unexplored moment in US history. Its narrative is interesting and accessible to a broad audience. It has particular value for readers involved in the age-old challenge of military manpower. UMT stands in stark contrast to the All Volunteer Force of today, and *Every Citizen a Soldier* reveals surprisingly relevant concerns expressed by postwar leaders about the issues that a less "democratic" fighting force might face (p. 29).

The timeline in appendix B proves helpful for any reader struggling to track the order of major events, and the notes demonstrate a solid research foundation on which Taylor built his study. US military historiography often falls victim to rehashing the same tired debates, but Taylor's work tackles a fresh subject in a way that makes it remarkably applicable for current discussions of military policy.

Amanda B. Biles
Minot, North Dakota

NASA's First A: Aeronautics from 1958 to 2008 by Robert G. Ferguson. National Aeronautics and Space Administration (http://www.nasa.gov), 300 East Street Southwest, Washington, DC 20546, 2013, 293 pages, ISBN 978-1-62683-009-7. Available free from http://www.nasa.gov/sites/default/files/files/NASAsFirstA-508-ebook.pdf.

"The Other NASA" best summarizes Robert Ferguson's most recent addition to the National Aeronautics and Space Administration's (NASA) Historic Program Office's history series. In *NASA's First A: Aeronautics from 1958 to 2008*, Ferguson brings to light the often forgotten and seldom known history of NASA research and the resulting impact it had on the development of airpower, military strategy, space capability, technology, and US economic growth. Ferguson reveals NASA's rich history of research, spanning multiple laboratories and test sites, which led to technological advances in aeronautics such as military rocketry programs, the X-15 space plane, spacecraft capable of landing after Earth reentry, and the supersonic transport. Finally, he explores the most turbulent of times when US political and economic factors, unnecessary competition, and lack of market discipline threatened the future of aeronautics research toward the turn of the millennium in the 1990s.

Ferguson explains in detail how, unlike space research, aeronautics research initiatives delivered to the US taxpayer practical and largely accepted solutions to economic, military, and commercial challenges. One of the most utilized—and least known of commercial advances—is the winglets on the tips of US commercial airliners and newer military cargo jets, a component designed to increase efficiency and reduce drag at subsonic speeds. Another dually beneficial advance propelled by aeronautics research is the subsonic airfoil—a design perfected by NASA researchers for highly efficient, low-drag, high-subsonic wings. The aforementioned designs are still employed by air and space engineers during development of military airlift and commercial passenger aircraft. Ferguson's work captures and preserves NASA's aeronautics research accomplishments for future aviation and space scholars, historians, and researchers.

In the final chapters, Ferguson provides a comprehensive narrative covering the most volatile, uncertain, complex, and ambiguous time in the history of NASA's aeronautics research. At the turn of the century, the federal government experienced tremendous budget cuts. Even NASA, with a preponderance of federal funding during the Clinton administration, was struggling to support its air and space research initiatives. Ferguson highlights how poorly monitored performance and unregulated program growth, as well as fraud, waste, and abuse, created distrust in federally funded research and development. Given these events and the preparation for a Mars mission driven by the Bush administration, NASA leaders redirected focus and scarce funds away from aeronautics research and toward space exploration.

At only 234 pages of text, *NASA's First A* is an easy-to-read, well-written historical compilation of NASA's aeronautics research milestones—as well as struggles—suited best for space buffs, scholars, historians, and researchers in the space industry. The average Air Force, NASA, or commercial industry space practitioner will discover little of practical value in the text, and without an interest in history or research, such individuals might find it difficult to navigate the detailed presentation of NASA's historical developments.

Maj Jason M. Newcomer, DBA, USAF
Air Force Flight Standards Agency
Oklahoma City, Oklahoma

Shadow Wars: Chasing Conflict in an Era of Peace by David Axe. Potomac Books (https://www.nebraskapress.unl.edu/pages/PotomacBooks.aspx), 1111 Lincoln Mall, Lincoln, Nebraska 68588-0630, 2013, 256 pages, $29.95 (hardcover), ISBN 978-1-61234-570-3.

Shadow Wars examines the events leading to twenty-first-century warfare and the nature of that conflict by intertwining the history of drones, military contractors, special operations, peacekeeping operations, and embedded journalists with the fighting in Iraq, Afghanistan, Somalia, Chad, Mali, the Democratic Republic of the Congo, the Central African Republic, the Philippines, and others. The shortness of the book (only about 200 pages), combined with an ambitious spread of stories, makes for a fast-paced narrative that seeks to profoundly challenge "readers' conceptions of war and peace in the twenty-first century" (inside jacket).

Axe's main thesis is that wars are less likely to be fought between conventional forces and increasingly involve the United States' use of security contractors, media manipulation, public apathy, and drones to attain strategic goals in so-called shadow wars. As a result, war is less prominent, involves fewer casualties, and is easier for the public to dismiss. Overall, the author seeks to remind the public to pay attention to these conflicts as he draws on personal experiences as a journalist to take the reader through various battlefields. In between visits to the front lines, Axe includes an abbreviated history of drones and security contractors, including Blackwater, to describe the United States' growing preference to wage war from the shadows.

The strongest narrative in *Shadow Wars* that supports this thesis concerns the counterterror and counterpiracy battles waged in Somalia since the "Black Hawk Down" incident of 1993. Axe uses Somalia to describe how the incident created an aversion for deploying US forces and led the United States to call upon security contractors, drones, special operations forces, and the armies of Ethiopia, Kenya, and the African Union to fight proxy battles in Somalia. The story of how America supported several African armies is available to readers who know to look for it, and the author rightly brings the entire narrative into the limelight while adding context.

Throughout the book, Axe uses the conflict in Somalia as a springboard to offer some sharp insights into and criticisms of modern warfare, some of which are not related to operations in Africa. In one of his most passionate asides, Axe recalls the experience of embedded journalists during Operation Iraqi Freedom, claiming that military commanders arbitrarily evicted and thus prevented them from covering the Iraq conflict in a deliberate attempt to "preserve the shadows" (p. 87). This recollection serves as a transition to the story of the stealthy RQ-170 Sentinel, a drone that the US Air Force kept secret for years until a photo of it operating at Kandahar was leaked in 2009 (p. 88). These somewhat disjointed anecdotes support Axe's overall thesis of the growing tendency of conducting wars away from the public's attention.

Another refreshing aspect of *Shadow Wars* is the author's willingness to confront the conventional wisdom that drone strikes are counterproductive because they inspire more terrorists than they remove from the battlefield. Axe disputes the idea that terrorists have used US drone strikes in Yemen as an effective recruiting tool (p. 175). In doing so, he draws upon many well-documented references in the notes, offering the reader a number of sources useful in further exploring the book's various conflicts and stories.

Unfortunately, Axe gets carried away by his ambitions to tie so many narratives and conflicts together. Furthermore, several of his asides are only loosely connected to the main thesis, seemingly included only because they represent the author's personal testimony (e.g., the description of how the MQ-9 Reaper uses synthetic aperture radar) (p. 112). He also drifts into personal speculation that could hinder an uninformed reader's efforts to understand which conclusions are well supported and which ones remain in the shadows. For example, although the military may have restricted the access of embedded journalists in Iraq and tightly controlled information related to drone capabilities over the past 20 years, it seems unlikely that both of these efforts were part of a coordinated effort to enable a worldwide campaign of shadow wars. Casting a wide net of subjects and anecdotes ultimately forces Axe to leave some stories incomplete and some ideas only cursorily examined.

Shadow Wars would have better served its thesis by more narrowly focusing on US involvement in Somalia, easily the strongest of several narratives competing for attention. Axe still would have had the opportunity to delve into background material but without the distracting anecdotes about the very public wars in Iraq or the development of the RQ-170 Sentinel. The author himself acknowledges that drone's irrelevance to the shadow wars involving enemies who lack the very radars that a stealthy drone so effectively avoids (p. 89).

Such a narrower perspective naturally would have led to an examination of the most prominent unanswered question of *Shadow Wars*: "So what?" Axe seems to imply that the general public should be more concerned about the use of contractors, drones, and foreign armies to realize US objectives, but one of his principal points is that this form of warfare is far less destructive than a total war and thus a better option for the United States to pursue its interests (p. 190). This implication is unfortunate since his open-ended conclusion calls into question the validity of the author's previous questions about the military's handling of journalists and the use of military contractors, drones, and proxy armies. The reader can assume that Axe believes that journalists should have more freedom to report on the US military but is left with ambiguous conclusions concerning ethical use of the other components of shadow wars.

Despite these and other flaws, including a shortsighted look at special operations and security contracting, *Shadow Wars* does present enough fresh insight mixed into an ambitious narrative that will engage a well-informed reader. Individuals who wish to become well versed in one of the subjects covered by Axe's book will find that they are frustrated by the competing narratives and would be better off reading more complete books, such as P. W. Singer's excellent studies of security contractors or drones, which are referenced throughout *Shadow Wars*. However, readers who are informed about the various components of Axe's shadow wars will appreciate his attempt to weave these stories together and may find just enough unique insight to make this book worth the quick read.

Capt Nicholas A. Reinhold, USAF
Langley AFB, Virginia

Wiki at War: Conflict in a Socially Networked World by James Jay Carafano. Texas A&M University Press (http://www.tamupress.com/catalog/CategoryInfo.aspx?cid=152), John H. Lindsey Building, Lewis Street, 4354 TAMU, College Station, Texas 77843-4354, 2011, 336 pages, $39.95 (hardcover), ISBN 978-1-60344-586-3; $24.95 (softcover), ISBN 978-1-60344-656-3.

In *Wiki at War*, James Jay Carafano presents a thoroughly researched synopsis of the national security implications of social networks and the connectivity afforded by Web 2.0. Dr. Carafano, the vice president of Foreign and Defense Policy Studies at the Heritage Foundation, is an accomplished historian and national security expert with several published works. In this book, his expertise is readily apparent as he distills complex subject matter into understandable concepts and seamlessly weaves together historical examples and recent events in support of his central thesis.

The author argues that "engaging in the war online is not optional" (p. 22), defending this position by drawing on a survey of social networks and their effect on our world. The book's seven chapters are informally organized into three nearly equal parts. Part 1 presents a history of social networks and the technological advances that contributed to the emergence of Web 2.0. Carafano maintains that speech was the first social network, that each human being is a node in the network, and that transmission of ideas through speech is the connection between nodes. This "technology" facilitated the formation of communities, enabled coordinated action in battle, and led to the development of other forms of social networks. As communities grew, so did the need for more capable social networks. Writing eliminated the distance limitations of speech and facilitated the storage of information. Machine writing expedited the writing process and facilitated mass communication. The telegraph and, later, the telephone provided near-real-time communication over long distances. Finally, the emergence of broadcast and mass media accelerated the delivery of messages over great distances to numerous recipients. Social networks today still depend upon these basic characteristics.

Although such networks evolved over thousands of years, Carafano notes that the evolution of computing technology occurred relatively quickly. He details the development of the Electronic Numerical Integrator and Computer ENIAC in 1942. Originally designed by John Mauchly to calculate gunnery tables, ENIAC emerged as the world's first programmable computer. The subsequent introduction of memory, high-level programming languages, and silicon processors fueled the computer revolution and led to its modern-day counterparts. Similarly, in an attempt to make an efficient research network, the Advanced Research Projects Agency developed the technology and protocols that enable the Internet. Over time, the Internet matured, and interactive applications that permit "user created content" (p. 84) began to emerge. This new, more interactive version of the Internet is often referred to as Web 2.0.

Part 2, dedicated to present-day cyberspace, examines the malicious actors operating in cyberspace, addresses government shortcomings in managing cyberspace activities, and declares that individuals have the potential to "act as agents of influence" in cyberspace (p.167). The author's coverage of various archetypes of threats in cyberspace is comprehensive and well written. Although he pays less attention to nation-state actors, his emphasis on cyber criminals and activists offers a balanced view representative of reality. The downside is that Dr. Carafano seems to have a bias which leads him to conclude that the number of people affiliated with China's "Red Hacker Alliance" equates to cyberspace superiority and that other advanced nations, including the United States and Russia, are inferior in this area. Some aspects of his findings may be true, but readers are not afforded the opportunity to arrive at their own conclusion.

Carafano's treatment of governments' ability to adapt and operate in Web 2.0 is equally biased. He argues that government shortcomings have "less to do with the state of technology . . . than they do with their courage and competence to act" (p. 160), pointing out numerous failures by the US government, from deploying e-government to recognizing the importance of human capital. Although these claims are factually accurate, the author tends to overemphasize their effects, a commonplace trend among cyberspace writers. This section closes with a discussion of the importance of individuals in Web 2.0, observing that "the national security implication of individuals online is too big a subject for free states not to pay attention to" (p. 193).

Part 3 presents a road map for governments to become competitive in cyberspace and discusses key technological areas in which future innovations may change the cyber landscape. The author presents a compelling "to-do list" for governments that includes being deliberate and systematic, finding ways for hierarchical and networked processes to complement each other, and developing cyber-savvy leaders to face the challenges of the future, using examples from earlier sections of the book to fortify these arguments. Finally, he examines areas in which innovations could change the landscape of cyberspace, including quantum computing, storing inordinate amounts of data, and developing applications that scan environmental factors and predict users' information needs. Even though these theories seem far-fetched today, their potential for becoming reality adds credence to the author's argument that "thinking about the future is a vital part of holding the cyber heights" (p. 263).

In *Wiki at War*, Dr. Carafano realizes his objective of surveying cyberspace and addressing the current issues with which governments must deal. Parts 1 and 3 are exceptional, providing thoroughly researched and well-written discussion. Part 2, unfortunately, falls short because Carafano's biases result in inaccuracies and overstatements regarding the impacts of his arguments.

This book is best suited for senior leaders or policy makers interested in a broad survey of cyberspace. However, individuals more familiar with the subject will likely find its wide-ranging approach inadequate. Furthermore, readers directly involved in cyberspace operations may discover that *Wiki at War* suffers from overemphasized claims and the type of sensationalism that has become commonplace in the cyber genre.

Maj William R. Giles, USAF
Lackland AFB, Texas

A Low-Visibility Force Multiplier: Assessing China's Cruise Missile Ambitions by Dennis M. Gormley, Andrew S. Erickson, and Jingdong Yuan. National Defense University Press (http://ndupress.ndu.edu), 260 Fifth Avenue, Building 64, Fort Lesley J. McNair, Washington, DC 20319-5066, April 2014, 165 pages. Available free from http://ndupress.ndu.edu/Portals/68/Documents/Books/force-multiplier.pdf.

Since the fall of the Soviet Union, the US military has searched for a military near-peer competitor that will justify its continued purchase of high-end military equipment and training for large force-on-force conventional warfare. For many people, that competitor is China, which possesses the fastest growing economy in the world, makes increasingly large expenditures on military equipment, and seeks to assert itself as a regional hegemon. Unsurprisingly, then, the US military is keeping a close eye on development of the Chinese military and its selection of investments in conventional force capability and foreign imports. *A Low-Visibility Force Multiplier* is a thorough, albeit unclassified, review and assessment of one key portion of the Chinese military's advancement—specifically, its investment in cruise missiles.

This book is not for the amateur or casual reader. Despite its brevity, the study contains monotonous lists and descriptions of Chinese production companies, antiship and land-attack cruise missiles, and launch platforms. Furthermore, it contains a detailed examination of the confusion that exists about these missiles and companies, based on the secrecy that surrounds them and the muddle over their names and capabilities. For military professionals who want to expand their knowledge of the Chinese military threat or learn the complete lexicon of military cruise missiles and platforms developed or imported by China, *A Low-Visibility Force Multiplier* satisfies that requirement.

The book builds the case that China is investing in its cruise missile program as a key component of an antiaccess/area denial capability against the United States. The Chinese military sees cruise missiles as a cheap and capable asymmetric military capability that gives it a significant military advantage in regional wars, especially a military campaign against Taiwan that would include US military intervention. For the Chinese military, cruise missiles are not only inexpensive and compact but also require only limited support (p. xvii). Ground-launched platforms can be highly mobile, thus enhancing their prelaunch survivability.

Their potential for "supersonic speed, small radar signature, and very low altitude flight profile" will prove stressful for even the most modern air defense systems (p. xvii). Additionally, the ability of the Chinese military to conduct salvo launches from multiple axes, possibly combined with launches of conventional ballistic missiles, gives it reason to believe that these weapons can overwhelm any US defense. Similarly, China is keenly aware of the US reliance on naval vessels to project power into any future conflict. To deter such an onslaught, it has aggressively pursued development of advanced antiship cruise missiles (ASCM) and has imported Russian supersonic ASCMs. These weapons enable the Chinese military to pose a formidable challenge to US surface vessels by overwhelming their defenses. The authors do acknowledge that the Chinese cruise missile capability is still in development and has not yet reached its full potential: "Shortcomings remain in intelligence support, command and control, [delivery] platform stealth and survivability, and postattack damage assessment" (p. xx). Nevertheless, such antiship and land-attack cruise missiles would give China a significant asymmetric defense against US intervention in any future conventional conflict in the region.

For readers seriously interested in learning about the evolving prowess of the Chinese military, this short book will give them the unclassified information they desire. The real value of *A Low-Visibility Force Multiplier*, though, is its elucidation of the Chinese cruise missile threat and its examination of the hurdles involving technology, development, training, doctrine, and employment that still prevent China from fully realizing the benefits of its cruise missile capability.

Lt Col John S. Meiter, USAF
Headquarters North American Aerospace Defense Command
Peterson AFB, Colorado

Let us know what you think! Leave a comment!

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