ASPJ
Air & Space Power Journal

November–December 2014
Volume 28, No. 6
AFRP 10-1

Senior Leader Perspective

Feature

Departments

The *Air and Space Power Journal* (ISSN 1554-2505), Air Force Recurring Publication 10-1, published electronically bimonthly, is the professional journal of the United States Air Force. It is designed to serve as an open forum for the presentation and stimulation of innovative thinking on military doctrine, strategy, force structure, readiness, and other matters of national defense. The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

http://www.af.mil

http://www.aetc.randolph.af.mil

http://www.au.af.mil

Air and Space Power Journal
155 N. Twining Street
Maxwell AFB AL 36112-6026

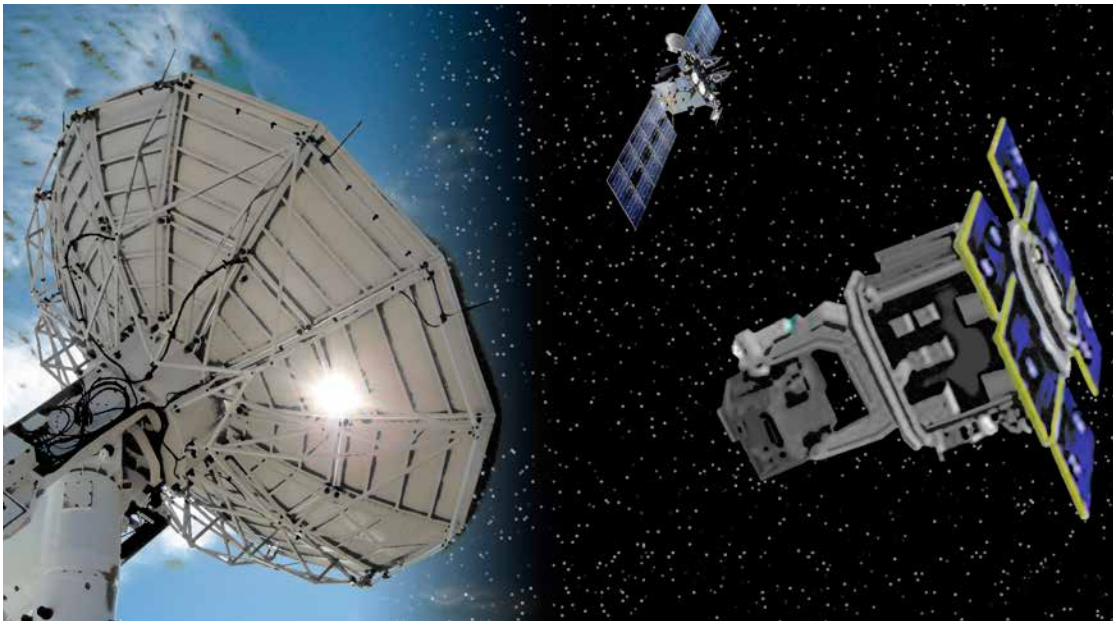
e-mail: aspj@us.af.mil

Visit *Air and Space Power Journal* online at http://www.au.af.mil/au/afri/aspj/.

Space Situational Awareness

Difficult, Expensive—and Necessary

Dr. Gene H. McCall
John H. Darrah*



In 1990 Operation Desert Storm, which marked the first widespread use of precision-guided munitions and low-observable aircraft, introduced a new set of military technologies and capabilities. Perhaps, though, the most valuable lesson learned from that operation

*The authors thank Gen William Shelton for his thoughtful and insightful comments.

was that space assets could significantly improve military effectiveness through enhanced target identification, better damage assessment, and more efficient communications.

Since Desert Storm, the United States has spent much effort and many dollars to refine space capabilities. In particular, the Global Positioning System (GPS) became fully operational for both military and civil users to enable navigation and weapon accuracy never attained in the past. Surveillance capabilities such as the Space-Based Infrared System emerged, reconnaissance assets became more proficient, and worldwide communication bandwidths increased dramatically. Weather satellites upgraded our prediction capabilities and shortened disaster-warning times. Many of these programs benefited the civil community; primarily, though, they measurably helped the expertise of the US military. Although the Air Force deployed the major developments, both the land and sea forces profited greatly as well.

As part of the development and fielding processes, we cultivated sophisticated methods for monitoring the health, position, and operational status of space vehicles. However, the evolution and installation of sensors to warn of and identify attacks on them were somewhat neglected. Even though some people believed that such sensors were important, the programs, in general, proceeded as though their distance from the surface of the earth and their speed conveyed upon them a charmed existence.

But we should not think, for even one moment, that the increasing reliance of US military forces on space assets has gone unnoticed by potential adversaries, both military and economic. Nations both large and small have begun to develop space and antispace capabilities that fall into two broad categories: (1) assets located in space that can enhance national military capabilities or contribute to the nation's economic development, and (2) technologies and devices that can defeat or destroy American space assets. The first category includes surveillance instruments created by various nations, space-based navigation systems developed by Russia and China, and weather- and earth-sensing devices produced by countries such as India and Japan. Such assets

contribute to *foreign mission enhancement* (FME). In the second category, we have seen a significant amount of work on antisatellite devices by Russia and China. Innovations in high-power laser and microwave technology, which could be used against American space assets, continue in many countries. These devices and technologies are *US mission-defeat* assets. As yet, we have seen no direct-attack weapons based in space, such as warhead-carrying missiles that could target an object on the earth's surface, but we should not completely discount the possibility of these weapons emerging in the future. As early as 1962, the Soviet Union began work on a device called the Fractional Orbital Bombardment System (FOBS). Although the Soviets did not design FOBS to place a nuclear weapon permanently in orbit, its launcher and guidance system could do just that. The project appears to have been abandoned because of accuracy shortfalls, not deployment difficulties. Development of improved reentry precision, occasioned by the need to provide services for the International Space Station, may enable the deployment of such weapons in the future. In terms of a category, we identify these devices as *direct-attack* space assets. A third category—*space debris*—has received much publicity but, as yet, has had only a minor impact on space operations. We will expand this area a bit by defining a set of dangerous objects as *passive threats*. Certainly, debris falls into this category, but it also includes items like out-of-control satellites and rockets.

The Needs of Space Situational Awareness

Although the term is a rather clumsy grammatical construct, *space situational awareness* (SSA) is a necessity for any nation that seriously bases its military and economic well-being even partly on space capabilities. SSA is the enabling of a description of the location and operation of US space assets as well as the location and function of the assets of other nations, particularly those that are, or could become, our enemies. SSA also identifies the capabilities needed for protecting US assets and for destroying or disabling those of the enemy. Frequently, a mission

defeat can be just as useful as destruction while not violating treaties or providing grounds for retaliation.

We should emphasize, though, that SSA is primarily the result of inference. Technology, associated terrestrial intelligence, and prior experience can all be important contributors to the understanding of an enemy's intentions and status in space, but SSA is not an exact science.

Tracking Foreign Mission Enhancement

SSA is sometimes defined as knowledge of the position and orbit of every object in space. As demonstrated below, however, if SSA is to be a useful military concept, it must become much more than that. SSA seeks to determine the position, function, and current status of every object in space, but such a goal may exceed US capabilities. Therefore, the first attempt at SSA should involve identifying those objects associated with FME and determining their owner, capabilities, and status.

Tracking Position and Determining Function

Perhaps the most costly part of SSA is the tracking and position monitoring of space objects. We must stress, though, that tracking only supports SA. The main output of an SSA effort is determination of the capabilities of a space object and the intentions of its owner.

The primary method for tracking all objects in space entails the use of radar, which has not yet provided accurate location of and orbital information about all space objects. Even if perfect radar information were available, however, the method offers no data about the function of detected satellites. One usually infers function by tracking a satellite from launch to final orbit and associating that information with data from other intelligence sources. Apparently, possible adversary nations have not attempted to deploy radar-defeating technologies such as stealth, but given the emphasis that, say, Russia and China have placed on the development of such technology for aircraft, we should expect the appearance of these technologies in space in the

future. The increasing use of shorter-wavelength radar systems by the United States makes that possibility even more likely. Therefore, America would do well to develop radar-independent tracking methods, such as lasers and coherent infrared sensors. We can improve the tracking accuracy of US satellites by replacing radar with onboard GPS sensors and including the GPS position as part of the usual downloaded information about health and status.

No tracking method can supply complete information about the function of a satellite, even if we use the inference method mentioned above. Additional data can be obtained from images of a satellite, which can show antennas and sensors associated with known devices and functions. US military laboratories have pursued optical imaging methods for decades and should continue to do so, developing techniques to yield images having a spatial resolution of one centimeter or better. Infrared imaging can provide additional information, but, again, inference is necessary. We can most likely obtain direct information about the structure and function of a satellite of interest by placing a sensor satellite in close proximity. The latter can take surface photographs of the target vehicle, monitor attitude and orbit changes, and observe its emissions, which may include radio frequency power; optical energy from far infrared to x-rays; and neutrons, protons, electrons, and other atomic and subatomic particles. In general, atmospheric attenuation prevents the observation of particle emissions from the ground unless they are very intense. One could even imagine placing two satellites on opposite sides of the target vehicle, one of them emitting x-rays or neutral or charged particles that could penetrate the structure of the vehicle and the other imaging those x-rays to form a photograph of the target's interior. We could utilize microwave imaging as well, taking care to prevent damage to the target satellite.

Provocative? Perhaps. But there appears to be no territorial limiting distance associated with space objects. We can identify them as valuable property, though, and make a case for compensating the owner for any damage done by a sensor satellite. Such an expenditure would

be a small price to pay for detailed information about an adversary's intentions in space. Furthermore, for example, if the satellite contained a weapon of mass destruction (e.g., a nuclear device), we could employ active methods to destroy it. For chemical or biological weapons, the sensor satellite could obtain a swab from the surface of the target, analyze it on board, or return to Earth—as was the procedure with early film canisters. Expensive? Yes, but giving our enemies the upper hand in space would prove even more costly.

Communication Monitoring

Communication capabilities and operations are important factors in SSA. Even minimal information about a satellite should include a report on its communication history. Basic questions to answer are as follows: Does the satellite emit energy that appears to come from a communication system? How often does it emit such energy? With whom does it appear to communicate? What or where is the source? Does the satellite appear to receive as well as transmit? Does satellite status change following a communication session? Can the nature or details of the communication be determined? Other questions may be appropriate as well, but communication status remains a valuable source of information about the purpose and function of a satellite. Much of this data can be obtained from ground or airborne sensors, but the latter cannot compete in either detail or accuracy with satellites deployed in the same or a nearby orbit in close proximity to the vehicle under study.

Geosynchronous Orbit

The geosynchronous or geostationary orbit that rings the earth above the equator at a radius of 42,157 kilometers (km) or an altitude of 35,786 km (22,236 miles) provides a special opportunity for FME. Satellites in this orbit remain above the same point on the earth at all times. Their orbital period equals that of the earth's sidereal period—23 hours, 56 minutes, and 4 seconds. We know, for example, that the orbit con-

tains at least four satellites of the Chinese BeiDou-2 satellite navigation system. It is also home to many communication and observation satellites used by a number of nations. The geosynchronous orbit includes approximately 600 satellites, not all of them operational or functional. Some have exhausted the fuel required to maintain the orbit, and others have failed systems. Still, because many possibilities for military applications inimical to the interests of the United States remain, the satellites deserve careful and frequent observation.

Recently, Gen William Shelton, then commander of US Air Force Space Command, announced the Geosynchronous Satellite Space Awareness Program (GSSAP), designed to place in geosynchronous orbit a sensor satellite capable of approaching a target satellite and observing its operations. Certainly this is a step in the proper direction to improve US military forces' knowledge about FME. Eventually, such sensors should track all foreign satellites, but the geostationary orbit is a logical first step, given that the GSSAP will have access to nearly 600 satellites while many low Earth orbits (LEO) and even Molniya orbits contain only one or a few satellites. Thus, GSSAP satellites will have nearly 600 times more intelligence-gathering capability than a single-orbit LEO or medium-altitude satellite. Assuredly, the Air Force and its contractors well understand that the GSSAP vehicles must possess unprecedented accuracy in terms of propulsion and positioning. A collision will result in significant political and financial problems; moreover, it could produce debris capable of contaminating a large portion of the geosynchronous orbit. Certainly, maneuvering operations will generate very tense times at the satellite control center at Schriever AFB, Colorado. The more sparsely populated orbits will demand new technologies and methods—a problem discussed to some extent below.

Low Earth Orbit and Companion Satellites

LEO presents special difficulties for the task of maintaining effective SSA. Important assets such as reconnaissance, Earth-observing, and mobile communication satellites occupy these orbits. Highly elliptical

orbits, such as Molniya orbits, tend to have perigees in this range as well. Thus, altitudes between approximately 150 and 2,000 km can contain important assets that should be a part of an SSA program. Unfortunately, these orbits tend to be very sparsely populated. The United States should develop a fleet of vehicles identified as *companion satellites* designed to monitor the actions of satellites of interest that can contribute significantly to an adversary's war plans. The companions should occupy the same orbit as the satellite of interest in close proximity to observe the actions and functions of the target. It may be possible to design a generic companion satellite that will function as a monitor for a large class of foreign assets, or we may need to field a special satellite for each foreign asset. In either case, costs of construction, launch, and operation will be significant factors in deciding whether to deploy such devices. Perhaps we can reduce the required number of companion satellites by launching them into orbits that intersect those of target satellites at a point appropriate for observation. Further, we may realize some cost reductions by making the companions reusable so that they can be returned to the earth, serviced, and inserted into a new orbit.

Passive Threats

Passive threats primarily consist of objects such as debris or uncontrolled satellites or rockets. Almost always, the important factor for SSA is location. Since orbital parameters can be derived from location measurements, it is possible to determine which objects could prove dangerous to US space assets and generate warnings at proper times to stimulate defensive actions.

Another set of passive threats, sometimes not included in SSA estimates, are those from high-energy particles and photons. These particles may be generated by natural events such as solar storms or caused by events like nuclear explosions in the atmosphere or in space. In either case, detection by space assets would most effectively determine the characteristics and possible dangers of such threats.

Facilities

All of the tasks mentioned above call for a significant amount of equipment and numbers of personnel to enable their functions. One item not emphasized but necessary for an effective SSA is a facility for controlling assets and sensors, displaying and analyzing sensor information, and giving the proper people a place to freely discuss the information at hand. This information center should also have access to current intelligence that can be related to actions in space associated with the world geopolitical situation.

The authors believe that this important part of an SSA system too often has been neglected by those who plan for and appropriate such facilities. This situation must be rectified if the United States wishes to maintain an effective presence in space. Obviously, the planning and construction of these facilities should closely involve people who analyze and use the SSA information. An addition to SSA sensors, the new space fence on Kwajalein Island offers a significant improvement in the ability to locate both active and passive threats. Too often, however, the US military tends to view a new, improved capability as a reason for ending its support and upgrade of facilities. We sometimes indoctrinate our people, particularly those responsible for building new installations, into believing that the new capability is a suitable end for developments in the field.

Nothing could be more counterproductive. Seldom is a new system the absolute best that we can do, even using current technology. We must constantly and routinely reevaluate all facilities as we observe the emergence of new technologies and changes in the world's political situation that may indicate a need for new and better capabilities. Even if immediate changes are not possible, such evaluations can serve as guides for research and development.

Space Situational Awareness as a Career Field

Given the variety and number of topics described above, it should be clear that expertise in SSA comes neither quickly nor easily. Individuals with less than a decade of experience in the art will probably find themselves ineffective at describing space conditions important to the defense of the United States in a way that is understandable and useful to combatant commanders. (The word *art* indicates that SSA is not an exact science.) The keys to effective performance are education and experience. Education in space technology, though necessary, is not sufficient. A good understanding of geopolitics may be just as important as an understanding of foreign satellite technology. A set of checklists is unlikely to provide much useful SSA although they may contribute to the total knowledge of those responsible for constructing a valuable SSA.

As mentioned above, SSA is as much a matter of inference as of data gathering. Probably, no one will be perfect at it, and few will be better than acceptable. Very likely, those who have an aptitude for the art will be readily identifiable. They should be encouraged by appropriate recognition and promotion, and their assignment to the subject for an entire Air Force career is appropriate—a procedure usually identified as a career field. Surely, it is at least as important as, say, personnel management as far as the security of the nation is concerned.

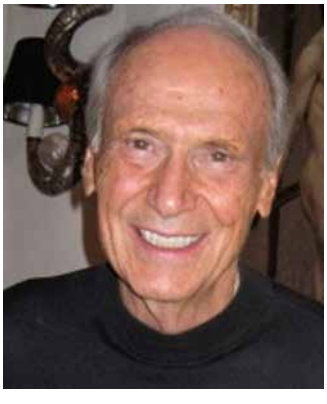
Conclusion

It should be clear that although location and orbital information are essential parts of SSA, its ultimate goal is to define the function and status of space objects as well as the intentions of their owners. Radar and optical observations are significant, but they are not likely to provide a complete picture that enhances the defense of the United States. SSA is a varied, complex, and substantial activity that can boost the military capabilities of American forces. The US military should pursue it actively with the assignment of enough forces and budget allocations to make it effective. SSA, perhaps, is a good example of the

observation attributed to Thomas Jefferson, among others, that "eternal vigilance is the price we pay for liberty." ✪

Dr. Gene H. McCall

Dr. McCall (BEE, Georgia Institute of Technology; MEE, New York University; PhD, Princeton University) has served as chief scientist, Air Force Space Command; laboratory fellow, Los Alamos National Laboratory; and chairman, USAF Scientific Advisory Board. He helped found the Inertial Fusion Program at Los Alamos and was a consultant to the Department of Energy for inertial fusion issues. In 1995 Dr. McCall directed the *New World Vistas* study requested by the secretary and chief of staff of the Air Force, widely regarded by the defense community as a guide for the development of twenty-first-century weapons for the Air Force. He has received the Department of Energy's E. O. Lawrence Award for contributions to national security, the Air Force Association's Theodore von Karman Award for technical achievement, the Department of Defense Distinguished Public Service Award, and the Secretary of the Air Force Exceptional Service Award with oak leaf cluster.



John H. Darrah

Mr. Darrah (BA, MS, University of Nevada) is an adjunct staff member at the Institute for Defense Analysis in D.C. where he supports the commander, US Northern Command; commander, Air Force Space Command; assistant secretary of defense (OSD/C3I); and other DOD and government offices and agencies. In 1999 Mr. Darrah retired as AFSPC's chief scientist, the senior civilian for the command, and served in similar positions for NORAD, Aerospace Defense Command, and US Space Command. He is nationally recognized in the many missions and systems of NORAD and AFSPC and is also known internationally for his work to make survivable US strategic forces and their command and control. Mr. Darrah has advised government agencies on nuclear weapons, their effects, and alternative systems designs and served as an advisor on Strategic Arms Limitation Talks. He was also the senior scientist at the Air Force Weapons Laboratory.

Let us know what you think! Leave a comment!

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

Space Separatism

Degree of Differentiation

Capt Luke R. Stover, USAF
Dr. Alan Johnson, Lieutenant Colonel, USAF, Retired

Space activities are critical to the Nation's technological advancement, scientific discovery, security, and economic growth.

—National Space Transportation Policy
21 November 2013

The importance of space is clearly articulated in the introduction of last year's US *National Space Transportation Policy*.[1] However, the far-reaching benefits of space activity on society are diffi-

cult to comprehend, much less quantify. Also challenging to understand is the interaction between various governmental and nongovernmental agencies that provide for space activities. One of those organizations—a major stakeholder in and provider of space activities—is the Department of Defense (DOD).

Space is so important that the DOD recognizes it as one of five domains in which US forces operate (the other four are land, sea, air, and information).[2] In 2001 Secretary of Defense Donald Rumsfeld designated the Department of the Air Force (DAF) the "Executive Agent for Space for the DOD."[3] Given the national importance of space activities, the formation of a separate space force has been a topic of persistent discussion in academic and doctrinal circles ever since the United States first entered the space age. Proponents of a separate force argue that because space is an inherently unique domain, forces operating there should be organized, trained, equipped, and funded separately—as are air, land, and sea forces.[4] Opponents highlight the interconnectedness of space activities in the other domains as primary justification for maintaining the status quo.[5]

Recognizing the complexity of the issue, for purposes of this article, we assume that the proponents are justified and that space is a unique domain, meriting organizational status as such. If we believe that space activities should be organized as a distinct and separate force, then the question becomes one of degree. How separate should a DOD space organization be? This article examines five proposed models presented in the literature regarding creation of a separate organization to manage space for the DOD (fig. 1). We examine them from four distinct perspectives: financial efficiency, operational effectiveness, logistics considerations, and policy considerations. Collectively, these perspectives allow for a robust comparison of the potential implications associated with each of the five proposed models.

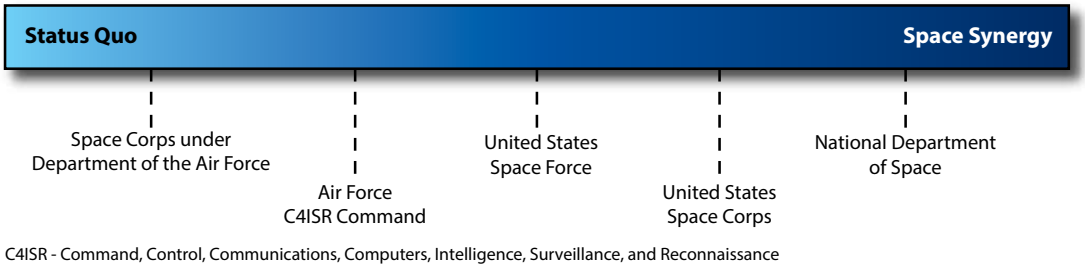


Figure 1. Spectrum of space separatism

Status Quo

Starting at the left end of the spectrum, we begin by briefly addressing the current model for space activities within the DOD. Although the DAF may be the DOD's executive agent for space, the Department of the Navy (DON) and the Department of the Army (DA) play a supporting role in effecting DOD space activities, broadly defined in enclosure 6 of DOD Directive (DODD) 5100.01, *Functions of the Department of Defense and Its Major Components.*[6] These functional activities are summarized in table 1. Collectively, the military departments provide space forces to US Strategic Command (USSTRATCOM) in support of national security objectives. This synopsis clearly delineates the supporting role of the DA and DON versus the operational role of the DAF in DOD space activities. Less apparent are the financial, operational, logistical, and policy implications of this current structure.

Table 1. Space functions of military departments

Space Operations		
Functions of the Army	*Functions of the Navy*	*Functions of the Air Force*
"Provide *support for space operations* to enhance joint campaigns, in coordination with the other Military Services, Combatant Commands, and USG [US government] departments and agencies" (emphasis added).	"Provide *support for joint space operations* to enhance naval operations, in coordination with the other Military Services, Combatant Commands, and USG departments and agencies" (emphasis added).	"Conduct *offensive and defensive operations* to gain and maintain space superiority to enable the conduct of operations by U.S. and allied land, sea, air, space, and cyberspace forces." "Conduct *space operations* to enhance joint campaigns, in coordination with the other Military Services, Combatant Commands, and USG departments and agencies" (emphasis added). "Conduct global integrated command and control for air and *space operations*" (emphasis added).

Source: DODD 5100.01, *Functions of the Department of Defense and Its Major Components*, 21 December 2010, 30–31, 34, http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf.

For fiscal year (FY) 2014, the DOD requested a total of $11.8 billion in support of space activities.[7] Of this total, approximately $10.1 billion (86 percent) originated from the DAF.[8] This amount is in line with historical levels wherein the DAF accounts for 85 percent of space-related DOD budget activity per FY.[9] The division of budget resources among military departments is synchronous with the operational capability that they provide the DOD.

The DAF makes available bases, facilities, and space systems to carry out space operations in support of US combatant commanders and other government agencies. Air Force Space Command conducts operations including space lift and satellite launch for the DOD and other government agencies, as well as surveillance, missile warning, nuclear detection, position, navigation, timing, weather activities, and communications.[10]

The DA channels space support through Army Space Command, which assists the Defense Satellite Communications System in providing

worldwide communications capability. Through a network of ground terminals and receivers, the DA collects and receives space, air, and ground intelligence. Finally, Army Space Command performs space surveillance operations from Kwajalein Atoll in the Marshall Islands.[11]

The DON performs space support under the purview of Naval Space Command, responsible for operating surveillance and warning space systems, tracking spacecraft telemetry, and performing on-orbit engineering. However, the command's primary mission is to provide space support to operational naval units around the world.[12]

The logistical implications of the current model for space activities are best understood through the lens of the seven principles of logistics defined in Joint Publication 4-0, *Joint Logistics*. These principles, summarized in table 2, serve as a backdrop for later discussion of logistic considerations within the five proposed models.

Table 2. Seven principles of logistics

Principle	*Definition*
Responsiveness	"Providing the right support when and where it is needed . . . characterized by the reliability of support and the speed of response to the needs of the joint force."
Simplicity	"Clarity of tasks, standardized and interoperable procedures, and clearly defined command relationships."
Flexibility	"The ability to improvise and adapt logistic structures and procedures to changing situations, missions, and operational requirements."
Economy	"The minimum amount of resources required to bring about or create a specific outcome . . . achieved when support is provided using the fewest resources within acceptable levels of risk."
Attainability	"The assurance that the essential supplies and services available to execute operations will achieve mission success."
Sustainability	"The ability to maintain the necessary level and duration of logistics support to achieve military objectives."
Survivability	"The capacity of an organization to prevail in spite of adverse impacts or potential threats."

Source: Joint Publication 4-0, *Joint Logistics*, 16 October 2013, I-9–I-10, http://www.dtic.mil/doctrine/new_pubs/jp4_0.pdf.

All three military departments currently operate under overarching policy contained in DODD 3100.10, *Space Policy*, which stipulates that the secretaries of the military departments shall develop departmental-level policies and programs in support of national security objectives; internally integrate space capabilities into every aspect of the departments' strategy, doctrine, training, and operations; and organize, train, and equip for space operations. DODD 3100.10 also directs the Joint Staff, combatant commanders, defense agencies and field activities, and other DOD components to carry out space-related duties in support of national security objectives.[13] This policy amplifies guidance from two all-encompassing national policies regarding space—the *National Space Policy* and the *National Space Transportation Policy*.[14]

Overarching space policy does not guarantee either operational efficiency or effectiveness of DOD space activities. For example, Lt Gen Michael Hamel, USAF, retired, asserts that "today military space includes numerous stovepiped systems operated by different communities, services, and agencies that use different concepts and approaches for operating and employing these capabilities in peace, crisis, and war."[15]

Viewed collectively, the financial efficiency, operational effectiveness, logistics considerations, and policy implications of the status quo raise questions about the utility of the current US model for space operations. An $11.8 billion DOD budget request in FY 2014 for space operations during a fiscally constrained environment, the current lack of interdepartmental coordination regarding space policy and operations, and the expansive logistics footprint necessary to sustain these various departments support the concept of a separate, dedicated space-organization model.

Critics of the status quo argue that the current narrow focus on individual, department-specific missions and the absence of interdepartmental coordination have resulted in a degraded US space capability. Arati Prabhakar, director of the Defense Advanced Research Projects Agency, suggests that the current US space environment is analogous to ducks on a lake in winter: "These ducks would cluster at twilight,

and they'd sit in the lake, and they would stop moving, and the lake would start icing up around them. Eventually, they would just freeze in place on this lake. . . . Tragically, that's what it feels like to me when I think about where we are in terms of our ability to react and do what we need to do quickly [and] cost effectively in space for national security purposes."[16]

Given this apparent atrophy of US space operations, perhaps a shift in organizational construct is the catalyst needed to strengthen the effectiveness and efficiency of the status quo. An examination of the five proposed constructs along the spectrum of space separatism begins with the creation of a Space Corps under the purview of the DAF.

Space Corps under the Department of the Air Force

In 2001 Congress directed the formation of a Commission to Assess United States National Security Space Management and Organization. One of the items studied by the commission was the establishment of a separate Space Corps within the DAF. According to the commission's report, "Existing Air Force space forces, facilities, units and personnel, and military space missions could be transferred to a Corps. A Space Corps could have authority for acquisition and operation of space systems, perhaps to include both DOD and Intelligence Community systems, while leveraging existing Air Force logistics and support functions."[17] The report also examined the financial efficiency of such a model.

From a financial efficiency perspective, little change from the status quo is expected under this proposal. The same $10.1 billion currently budgeted for space activities within the US Air Force would come under the control of a Space Corps that would still have to compete for DAF resources.[18] Furthermore, Air Force support agencies would still need to sustain Space Corps forces. In short, a financial net-sum gain of zero is expected under the proposed model. Conversely, under this model, positive change is expected with regard to operational effectiveness.

Just as the Air Force found its operational niche in the basis of the Army Air Corps, so could a space force refine its operational efficacy under a separate corps. According to the commission, a Space Corps could develop forces, doctrine and concepts of operation for space systems.[19] The commission envisioned the evolution of a Space Corps into a full-fledged Space Force or Space Department as forces, doctrine, and concepts of operations mature. This concentration on space activities would be aided through reliance upon existing logistics and support functions from within the Air Force.

The logistics considerations of a separate Space Corps would remain virtually unchanged from the status quo. The only logistics principle that might be positively influenced under this model is *simplicity*. Allowing the Air Force to manage its logistics functions should enable a Space Corps to focus on its core mission of space capabilities in accordance with DOD space policy.

Air Force Policy Directive (AFPD) 13-6, *Space Policy*, states that "the Air Force will recruit, sustain, and retain a workforce of highly skilled military and civilian space professionals proficient in operations, technical expertise, policy, strategy, acquisitions, contracting, managerial oversight and leadership."[20] Further, "the Air Force will provide space capabilities and forces, integrating them into Air Force plans, operations, and training while contributing to and enabling joint and combined forces."[21] A functional corps, dedicated to the development of space professionals, missions, and applications, is certainly in line with this strategic vision. The next proposed model on the spectrum of space separatism incorporates additional functional activities via the creation of an Air Force Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Command.

Air Force C4ISR Command

The opening section of this article highlighted that space is a unique domain. However, some individuals have contended that viewing

space from a domain-focused perspective is shortsighted.[22] Instead, critics maintain that space should be viewed as an effects-based medium. The effects produced by space activities are largely encompassed within C4ISR operations. Therefore, some have proposed that the Air Force could create a C4ISR Command to concentrate C4ISR functional operations, including space activities, under a coordinated, effects-based model.[23] Lt Gen John Koziol, USAF, retired, former commander of the Air Force ISR Agency, remarked that the result of such a model should be "an all-source, full-spectrum ISR mission-capable organization."[24] This model also effectively incorporates the fifth DOD domain (information) into Air Force operations. By including a broad range of functional activities under a single command, this model has potentially far-reaching financial implications.

In addition to the $10.1 billion Air Force space budget for FY 2014, $14.2 billion of the service's C4ISR-related budget resource would be reallocated to Air Force C4ISR Command under the proposed model.[25] Future budget-request reductions under the proposed model are not guaranteed, but the synergy created through the coalescence of these functional activities will probably yield more efficient operations and therefore reduce the baseline budget of $24.3 billion under the status quo for FY 2014. The $24.3 billion figure represents 21 percent of the Air Force's $114.1 billion baseline budget request for FY 2014.[26] Just as 21 percent is a substantial portion of the service's budget, so are the implications regarding operational effectiveness under the proposed model of considerable significance.

Under an Air Force C4ISR model, the commander could concentrate on the interrelationship of C4, ISR, and space activities to deliver effects for the DOD and other governmental agencies in support of national interests.[27] Dr. Edward Tomme notes that a C4ISR Command

> would become a much more effective organization for supporting USSTRATCOM's Joint Functional Component Command for ISR. It would work hand in glove with other intelligence organizations such as the National Geospatial-Intelligence Agency [NGA] and the National Security

> Agency [NSA] to satisfy combatant command and national operational and intelligence requirements.[28]

The interconnectedness of the proposed command would also likely streamline the logistics support requirements of the model.

The integration of C4, ISR, and space systems could improve the interoperability of those systems. As new space systems are designed to incorporate and exploit C4 and ISR capabilities, these *simplified* systems should be more *responsive* to the needs of the intelligence community and provide *flexible* options to combatant commanders in an *economical* manner with little duplication of intraservice effort.

This proposed model supports guidance in AFPD 13-6 for the Air Force to "integrate space surveillance, intelligence, and other information from commercial, civil, international partners, and national security sources to develop timely and accurate SSA [space situational awareness]."[29] Before space activities can be integrated outside the DOD, they must first be integrated internally. The next step on the spectrum of space separatism attempts to do just that.

United States Space Force

Creation of a separate US Space Force is perhaps the most obvious and commonly cited model for space organizational reform within the DOD. Proponents of such a model attempt to mesh the uniqueness of space with the current DOD organizational structure. They assert that just as the US Army exists because land is a unique domain, so we should have a US Space Force to operate in the distinct realm of space. The advancement of technological capabilities peculiar to space, the need for acquisition reform of space systems, a call for organizational reform across the DOD, and constrained DOD and Air Force budgets are also commonly cited as reasons why the US Space Force model makes sense.[30] The final argument is perhaps the timeliest, given the current fiscal realities of the US government.

The DOD budgeted $11.8 billion for space activities in the current FY. Under the proposed model, these budget resources should flow to the US Space Force. Additionally, establishment of a separate US Space Force would force the DOD to budget additional resources to provide staff positions and support activities germane to operating a military service. As an estimate of the number of resources these activities consume, the Air Force budgeted $6.5 billion in FY 2014 for DAF administration and servicewide administration and support activities.[31] If we add this notional amount, the estimated budget request for a US Space Force is, at minimum, $18.3 billion. Is this budget level justified by an associated increase in operational effectiveness?

At the heart of this question lies a secondary question—what is the role of space in DOD operations? Proponents of a US Space Force hold that space activities are now viewed primarily from the perspective of mission support to other operational activities.[32] Conversely, advocates of space separatism call for space activities to perform full-spectrum operations. Their premise is that a US Space Force would be free to conduct offensive, defensive, stability, and civil-support operations from the space domain.[33] This additional operational capability may indeed justify the added expense of creating a separate US Space Force. Also justifiable are the logistical considerations associated with such a force.

Consolidation of all DOD space functions under a unified force would make it more *responsive* to support the needs of customers, both internal and external to the DOD. A clearly defined US Space Force command would *simplify* logistics support while simultaneously enhancing the *flexibility* of that support. Having complete control over logistics activities, a US Space Force would enhance the *attainability* of immediate logistical support and the *sustainability* of a prolonged effort. From a long-term perspective, a US Space Force meshes well with DOD and national space policy.

DODD 3100.10 observes that space activities "will balance protecting and defending U.S. space capabilities . . . with maintaining capabilities

to deter and, if necessary, defeat efforts to interfere with or attack U.S. or allied capabilities."[34] A US Space Force would certainly be well situated to effect this strategic guidance, as would the next model on the spectrum of space separatism.

United States Space Corps

The placement of this model along the spectrum raises two obvious questions. First, how is this model different from a Space Corps under the DAF? Second, why is this model to the right of the US Space Force model on the spectrum?

Regarding the former question, this US Space Corps model is part of a more expansive one proposed by Kenneth Keskel, who envisions a functionally aligned, unified DOD structure in which the "teeth" of the services are delineated from the "tail." The term "teeth" refers to the core war-fighting competencies of the services. Keskel argues that these functions should be realigned among smaller, more flexible corps (Air Corps, Navy Corps, Army Corps, Space Corps, etc.). The "tail" refers to support forces that sustain the services' teeth. Keskel suggests that these functions should be consolidated under a joint support force.[35] Answering the first question should answer the second—a US Space Corps model calls for reform across the DOD, not just within the space community. Accordingly, the financial efficiency implications of this model are noteworthy.

Reforming the entire DOD implies potential economies across the department's entire baseline budget ($516 billion for FY 2014).[36] However, to accommodate comparison with other models, we excluded budget areas not associated with or in support of space activities. In total, this model considers $11.8 billion for space activities and an additional $48 billion for administrative and servicewide support functions.[37] Altogether, nearly $60 billion in budgetary resources are under consideration for this model, and its potential influence on operational effectiveness is expansive.

Keskel postulates three operational benefits of implementing the proposed model. First, the corps would be able to focus exclusively on its core competencies. Second, functional duplication among services would be greatly reduced. Finally, interoperability between forces and operating systems would be significantly enhanced. In total, his model supports emerging missions, addresses current fiscal constraints, and improves "jointness" to fulfill objectives in accordance with national security guidance.[38]

Under the US Space Corps model, logistics functions would largely be considered support activities and would therefore be consolidated under a joint-support force structure. Such consolidation would likely improve the *economy* of space logistics functions. Simultaneously, the focused nature of a US Space Corps should enhance the *responsiveness*, *simplicity*, and *flexibility* of logistics support. A decoupled logistics "tail" would probably adversely affect the attainability and sustainability of logistics support for space activities. Conversely, such degrees of separation might improve the *survivability* of space logistics activities. Keskel's model is a major departure from the status quo financially, operationally, and logistically. Does this model synchronize with current space policy?

DODD 3100.10 directs that the "DOD will develop and integrate into an operational space force structure all appropriate space-related defense capabilities required to support national security objectives."[39] The US Space Corps model could realize this consolidation of space activities under a defensewide, operationally engaged Space Corps. For the final model on the spectrum of space separatism, we open the aperture even further by examining the coordination of space activities across all US government agencies.

National Department of Space

As stated in the opening paragraph of this article, the DOD is not the only, or even the primary, player in the US space community. Numerous government and nongovernment agencies play an important role in

the interconnected domain of space. Lt Col Kristine Shaffer asserts that "given the depth and breadth of space, there exists a clear opportunity and the absolute need to establish one organization and one responsible leader to provide the national and global requirements, needs and capabilities, all day, every day."[40] She proposes the creation of a National Department of Space (NDS) as a model towards this end.[41]

A review of DODD 3100.10 identifies current US government agencies that contribute to or are end users of US space activities, including the Defense Intelligence Agency (DIA), National Reconnaissance Office (NRO), National Aeronautics and Space Administration (NASA), NGA, and NSA.[42] Shaffer's model unites all of these agencies under an overarching NDS.[43] Merging the operations of six government agencies is certainly a drastic proposal, but the financial efficiency implications are remarkable.

The DOD's budget request for space activities in FY 2014 was $11.8 billion. Additionally, although budget request data for the DIA, NGA, NRO, and NSA are classified, the total budget request for the National Intelligence Program, which encompasses all of these agencies, was $52.2 billion for FY 2014.[44] Finally, NASA's budget for FY 2014 was $17.8 billion.[45] In total, budget resources under consideration by this model amount to approximately $82 billion. Perhaps more significant than this figure are the model's implications regarding operational effectiveness.

Shaffer believes that the drastic change proposed under an NDS model "is required to elevate the importance of space within the nation, to enable the nation to better prioritize space-related activities, to promote greater coordination on space-related activities and to reduce redundant systems and capabilities while promoting interoperability with space- and non-space national and international communities."[46] Essentially, this model recognizes the criticality of space in conducting modern warfare. The United States' preeminence in space remains largely unquestioned. However, the effects of this position can be fully realized only under an organizational model that enables the seamless coordination

of all agencies that provide space activities. The NDS model may prove to be just that. Such interagency coordination is also likely to have beneficial effects on logistics considerations of US space activities.

The model would likely improve the *responsiveness, simplicity, flexibility, economy, attainability, sustainability*, and *survivability* of current space logistics support. By vertically integrating both suppliers and customers of space activities, the NDS could readily move beyond a logistics focus to adopt a supply chain perspective that integrates key processes from end user through original suppliers to foster a true enterprise focus.[47] Such a perspective is congruent with the *National Space Policy*.

According to that policy, the director of national intelligence shall "integrate all-source intelligence of foreign space capabilities and intentions with space surveillance information to produce enhanced intelligence products that support SSA."[48] Further, the secretary of defense and the director of national intelligence are charged to "maintain and integrate space surveillance, intelligence, and other information to develop accurate and timely SSA. SSA information shall be used to support national and homeland security, civil space agencies, particularly human space flight activities, and commercial and foreign space operations."[49] Both of these statements underscore the importance of interagency coordination to optimize existing and future space capabilities.

Summary

This article has examined five distinct models for space separatism from four perspectives. The following figures and tables summarize the implications of each perspective for each model along the spectrum of space separatism.

Figure 2 depicts the financial efficiency implications of the proposed models. The budget resources identified in this figure represent an opportunity for future budget reductions. A larger budget-resource figure indicates a greater opportunity to reduce budget requests for space activities in future FYs.

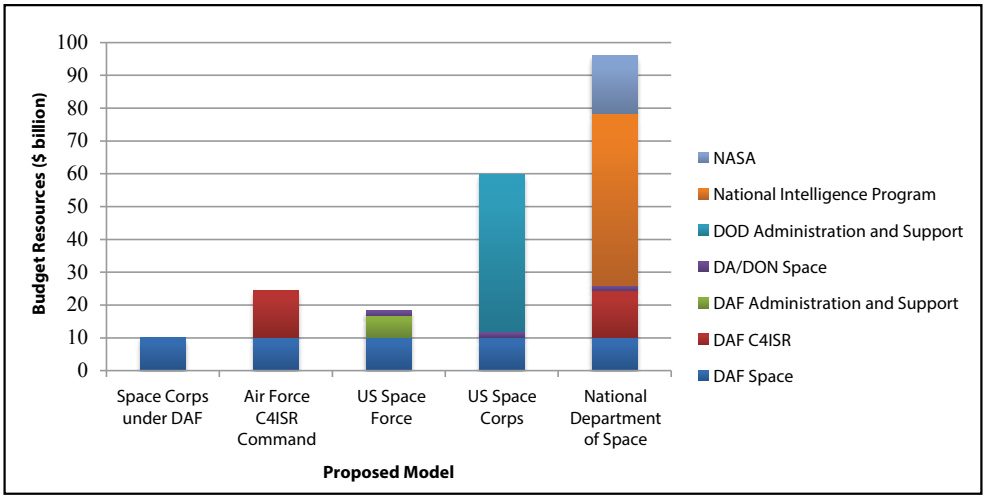


Figure 2. Summary of financial efficiency implications

Table 3 encapsulates the operational effectiveness implications of the proposed models. Although operational effectiveness is more difficult to quantify than financial efficiency, analyzing the former by model reveals general trends across the spectrum of space separatism.

Table 3. Summary of operational effectiveness implications

Proposed Model	*Operational Effectiveness Implications*
Space Corps under DAF	Develop forces, doctrine, and concepts of operation for space systems
Air Force C4ISR Command	Deliver effects-based space, C4, and ISR activities for the DOD and other governmental agencies in support of national interests
US Space Force	Enable force to conduct offensive, defensive, stability, and civil-support operations from the space domain
US Space Corps	Focus exclusively on core competencies, reduce functional duplication among services, and enhance interoperability among forces and operating systems
National Department of Space	Elevate the importance of space, enable the nation to better prioritize space-related activities, promote greater coordination on space-related activities, and reduce redundant systems and capabilities while promoting interoperability with space and nonspace national and international communities

Table 4 addresses the logistics implications of the proposed models through the lens of the seven principles of logistics. Given the breadth and depth of logistics support required to operate and sustain space activities, these principles are not all encompassing. Instead, they serve as a strategic lens through which to view and understand the adequacy of the proposed models from a logistics perspective.

Table 4. Summary of logistics implications

	Space Corps under DAF	Air Force C4ISR Command	US Space Force	US Space Corps	National Department of Space
Responsiveness		✓	✓	✓	✓
Simplicity	✓	✓	✓	✓	✓
Flexibility		✓	✓	✓	✓
Economy		✓		✓	✓
Attainability			✓		✓
Sustainability			✓		✓
Survivability				✓	✓

Table 5 recaps the policy implications of the proposed models. These synthesized results highlight applicability of the proposed models to current national and DOD space policy.

Table 5. Summary of policy implications

Proposed Model	*Policy Implications*
Space Corps under DAF	"The Air Force will recruit, sustain, and retain a workforce of highly skilled military and civilian space professionals proficient in operations, technical expertise, policy, strategy, acquisitions, contracting, managerial oversight and leadership." "The Air Force will provide space capabilities and forces, integrating them into Air Force plans, operations, and training while contributing to and enabling joint and combined forces."—AFPD 13-6, *Space Policy*
Air Force C4ISR Command	"Integrate space surveillance, intelligence, and other information from commercial, civil, international partners, and national security sources to develop timely and accurate SSA."—AFPD 13-6

Table 5. Summary of policy implications (Continued)

Proposed Model	*Policy Implications*
US Space Force	"Space activities will balance protecting and defending U.S. space capabilities . . . with maintaining capabilities to deter and, if necessary, defeat efforts to interfere with or attack U.S. capabilities." —DODD 3100.10, *Space Policy*
US Space Corps	"DOD will develop and integrate into an operational space force structure all appropriate space-related defense capabilities required to support national security objectives."—DODD 3100.10
National Department of Space	"Integrate all-source intelligence of foreign space capabilities and intentions with space surveillance information to produce enhanced intelligence products that support SSA." "Maintain and integrate space surveillance, intelligence, and other information to develop accurate and timely SSA. SSA information shall be used to support national and homeland security, civil space agencies, particularly human space flight activities, and commercial and foreign space operations."—*National Space Policy*

Conclusion

This article has examined the financial efficiency, operational effectiveness, logistics considerations, and policy implications of five models by which the DOD could structure future space operations. Of the models examined, the National Department of Space best addresses each of the four assessed areas. This reasonable conclusion is easily recognizable from the results in the summary section. As the scope of an organization grows, so does the potential of that organization to effect positive change at a macro scale. Reforming space operations within the Air Force, though a worthy effort, may have a limited impact on space operations of other governmental and nongovernmental agencies. Conversely, a cabinet-level department dedicated to the integrated operation of US space activities could consolidate all involved parties while synchronizing their efforts.

However, one should note that these models were presented along a spectrum. They are not isolated solutions but representative of a myriad

of possible space-force organizational models. This approach seeks to highlight the fact that the discussion regarding creation of a separate space force should be multidimensional. A model that optimizes financial efficiency at the expense of operational effectiveness may be a shortsighted solution. Similarly, a model that is logistically favorable but not synchronous with space policy is not a desirable plan. If the DOD moves towards a separate force dedicated to space activities, then it must take a holistic approach. The far-right side of the spectrum of space separatism is labeled "Space Synergy," an idea that captures the desirable interconnectedness of space agencies to provide synchronous space-based effects.

In closing its report, the 2001 Commission to Assess United States National Security Space Management and Organization concluded that "our growing dependence on space, our vulnerabilities in space and the burgeoning opportunities from space are simply not reflected in the present institutional arrangements."[50] The DOD must embrace this call to action as it examines the structure of tomorrow's space force. ✪

Notes

1. Office of the President of the United States of America, *National Space Transportation Policy* (Washington, DC: White House, 21 November 2013), http://www.whitehouse.gov/sites/default/files/microsites/ostp/national_space_transportation_policy_11212013.pdf.

2. Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington, DC: US Government Printing Office, June 2000), 26, http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf.

3. 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: Executive Summary* (Washington, DC: The Commission, 11 January 2001), 30–35, http://fas.org/spp/military/commission/executive_summary.pdf.

4. Lt Col Mark E. Harter, "Ten Propositions Regarding Space Power: The Dawn of a Space Force," *Air and Space Power Journal* 20, no. 2 (Summer 2006): 64–78, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/sum06/sum06.pdf.

5. Maj Alec M. Robinson, "Distinguishing Space Power from Air Power: Implications for the Space Force Debate" (Maxwell AFB, AL: Air Command and Staff College, April 1998), 47–49.

6. DODD 5100.01, *Functions of the Department of Defense and Its Major Components*, 21 December 2010, 25–35, http://www.dtic.mil/whs/directives/corres/pdf/510001p.pdf.

7. Office of the Under Secretary of Defense (Comptroller), *Defense Budget Materials—FY2014*, http://comptroller.defense.gov/budgetmaterials/Budget2014.aspx. See FY14_Green_Book.pdf.

8. Office of the Secretary of the Air Force, Deputy Assistant Secretary for Budget (SAF/FMB), *United States Air Force Fiscal Year 2014 Budget Overview* (Washington, DC: SAF/FMB, April 2013), 40, http://www.saffm.hq.af.mil/shared/media/document/AFD-130410-051.pdf.

9. Lt Col Kristine M. Shaffer, "National Department of Space" (Fort Leavenworth, KS: School of Advanced Military Studies, US Army Command and General Staff College, 25 March 2008), 22–25.

10. Ibid., 51.

11. Ibid.

12. Ibid.

13. DODD 3100.10, *Space Policy*, 18 October 2012, 8–11, http://www.dtic.mil/whs/directives/corres/pdf/310010p.pdf.

14. Office of the President of the United States of America, *National Space Policy of the United States of America* (Washington, DC: White House, 28 June 2010), http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf; and Office of the President of the United States of America, *National Space Transportation Policy*.

15. Lt Gen Michael Hamel, "Building Space Power for the Nation: Air Force Achievements, Challenges, and Opportunities," *Air and Space Power Journal* 20, no. 2 (Summer 2006): 58.

16. Cheryl Pellerin, "DARPA Programs Create New Future for Space, Director Says," American Forces Press Service, 13 January 2014, http://www.defense.gov/news/newsarticle.aspx?id=121474.

17. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission*, 26.

18. Ibid., 28.

19. Ibid., 18.

20. AFPD 13-6, *Space Policy*, 13 August 2013, 2, http://static.e-publishing.af.mil/production/1/saf_sp/publication/afpd13-6/afpd13-6.pdf.

21. Ibid.

22. Dr. Edward B. Tomme, "Emphasizing Effect over Domain: Merging Three Organizations to Enhance the Efficacy of Our Nation's Intelligence Production," *Air and Space Power Journal* 23, no. 1 (Spring 2009): 83–92, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj09/spr09/spr09.pdf.

23. Ibid., 90.

24. John A. Tirpak, "The Big Squeeze," *Air Force Magazine* 90, no. 10 (October 2007): 32.

25. Office of the Secretary of the Air Force (Financial Management and Comptroller), *United States Air Force Fiscal Year 2014 Budget Overview*, 40.

26. Ibid.

27. Tomme, "Emphasizing Effect over Domain," 90.

28. Ibid.

29. AFPD 13-6, *Space Policy*, 5.

30. Maj Norman W. Barber, Maj Richard J. Douglass, and Maj John D. DuMond, "Why Space Should Be a Separate Service" (Norfolk, VA: Joint Forces Staff College, 6 September 2002); MAJ William S. Moncrief, "Building a United States Space Force," *Army Space Journal*, Winter/Spring 2010, 34–38; COL Kurt S. Story, "A Separate Space Force: An Old Debate with Renewed Relevance" (Carlisle Barracks, PA: US Army War College, 9 April 2002); and Taylor Dinerman, "United States Space Force: Sooner Rather Than Later," *Space Review*, 27 February 2006, http://www.thespacereview.com/article/565/1.

31. Office of the Under Secretary of Defense (Comptroller), *Defense Budget Materials—FY2014*. See FY14_Green_Book.pdf.

32. Story, "Separate Space Force," 2–5.

33. Moncrief, "Building a United States Space Force," 34–38.

34. DODD 3100.10, *Space Policy*, 3.

35. Lt Col Kenneth Keskel, "Doing Things That Can't Be Done: Creating a New Defense Establishment," research report (Maxwell AFB, AL: Air War College, April 2002), 35–55.

36. Office of the Under Secretary of Defense (Comptroller), *Defense Budget Materials—FY2014*.

37. Ibid.

38. Keskel, "Doing Things That Can't Be Done," 35–55.

39. DODD 3100.10, *Space Policy*, 3.

40. Shaffer, "National Department of Space," 38.

41. Ibid.

42. DODD 3100.10, *Space Policy*, 8–11.

43. Shaffer, "National Department of Space," 28–37.

44. "DNI Releases Updated Budget Figure for FY 2014 Appropriations Requested for the National Intelligence Program," press release, Office of the Director of National Intelligence, 27 June 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/888-dni-releases-updated-budget-figure-for-fy-2014-appropriations-requested-for-the-national-intelligence-program.

45. National Aeronautics and Space Administration, *FY 2014 President's Budget Request Summary*, 1, http://www.nasa.gov/pdf/740512main_FY2014%20CJ%20for%20Online.pdf.

46. Shaffer, "National Department of Space," 50.

47. Donald J. Bowersox, David J. Closs, and M. Bixby Cooper, *Supply Chain Logistics Management* (Boston: McGraw-Hill, 2002), 2–5.

48. Office of the President of the United States of America, *National Space Policy*, 14.

49. Ibid., 13–14.

50. Commission to Assess United States National Security Space Management and Organization, *Report of the Commission, 9*.

Capt Luke R. Stover, USAF

Captain Stover (BS, Montana State University; MS, Air Force Institute of Technology) is the resources flight commander, 576th Flight Test Squadron (FLTS), Vandenberg AFB, California. The 576 FLTS is the only dedicated ICBM test and evaluation squadron in the country, reporting directly to Air Force Global Strike Command / Operations. He leads 22 Airmen in support of a $350 million force-development evaluation program. A career maintenance officer, Captain Stover has held a variety of flight- and squadron-level aircraft and munitions maintenance positions. He is a distinguished graduate of the Air Force Reserve Officer Training Corps and the Air Force Advanced Maintenance and Munitions Officer School.

Dr. Alan Johnson, Lieutenant Colonel, USAF, Retired

Dr. Johnson (BS, Montana State University; MS, Air Force Institute of Technology; PhD, Virginia Tech) is an associate professor of logistics management at the Air Force Institute of Technology. His research interests include all aspects of military logistics but emphasize reliability and maintainability as well as their effects on the life-cycle management of weapon systems and issues related to strategic-airlift mobility.

Policy for US Cybersecurity

Lt Col August G. Roesener, PhD, USAF
Maj Carl Bottolfson, USAF
CDR Gerry Fernandez, USN

Since creation of the first interconnected computer network in 1969 as an Advanced Research Projects Agency endeavor, cyberspace has expanded to affect many, if not most, aspects of Americans' lives. Unfortunately, accessibility to and expansion of the Internet often proceeded without proper consideration for the security of the information contained or transmitted therein. The lack of necessary security and the anonymity afforded by the Internet led to equally rapid growth (if not more so) of the nefarious exploitation of this man-made domain. Regrettably, it is unlikely that "the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."[1] However, this prospect should not limit attempts by the United States to defend its cyberspace infrastructure, "whether the threat comes from terrorists, cybercriminals, or states and their proxies."[2] Consequently, America must develop offensive and defensive cyber capabilities. Additionally, clearly defined policies require development and implementation to ensure cohesion across the whole of government. With respect to cyber domain attacks on US civilian systems attributable to a nation-state, the Department of Homeland Security (DHS) should have responsibility for responding (in the form of consequence management); US Northern Command (USNORTHCOM), for domestic attack assessment; and US Cyber Command (USCYBERCOM), for defense and any counterstrike response (in

coordination with applicable combatant commands and US national agencies). This article describes the cyberspace environment and its threats; explains the current authorities, roles, and responsibilities of these and other agencies; and details how these authorities, roles, and responsibilities need modification to best protect US national security interests.

The Environment

Cyberspace is "the globally-interconnected digital information and communications infrastructure."[3] From smartphones with navigation systems, to online banking, to global communications, cyberspace is an essential portion of most Americans' lives. The US Department of Defense (DOD) recently decided to "treat cyberspace as an operational domain."[4] Because of the ease and relatively low cost of conducting operations in cyberspace (compared to the physical domains of air, land, sea, and space) as well as the anonymity afforded by this virtual domain, cyber threats and attacks are more prevalent and arguably just as dangerous as those in the physical domains. In fact, the 2010 *National Security Strategy* noted that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[5] This statement is particularly troubling because "foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day."[6] Although not readily apparent, these attacks could affect the lives of average American citizens. Indeed, these types of cyber threats and attacks "go well beyond military targets and affect all aspects of [US] society. . . . Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption."[7] The potential negative impact on US national interests as well as the lives and assets of US citizens calls for government preparation and protection in the virtual domain equal to those in the physical domains.

Authorities, Roles, and Responsibilities

The following explains the current authorities, roles, and responsibilities for securing and defending cyberspace, examining those of the private sector and then their relationship to US government agencies—specifically, the Department of Commerce (DOC); DHS; Department of Justice (DOJ); Department of Energy (DOE); and DOD, including US Strategic Command (USSTRATCOM), USCYBERCOM, USNORTHCOM, and the National Security Agency (NSA). Here, *private sector* refers to any non-US government entity—an individual, a small company, or a large corporation. Because data and information with potential national security and vital economic interests reside on private-sector networks, they are targets for cyber intrusions in the form of nation-state and corporate espionage, identity theft, economic terrorism, and so forth. In light of the privacy issues inherent in the US government's protection and defense of cyberspace, few requirements are placed on the private sector for reporting cyber intrusions or attacks. In Presidential Policy Directive 21, the Obama administration designated the DOC, in collaboration with the DHS and other relevant federal departments and agencies, as the lead agency to "engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems."[8] The goal of this effort includes collaboration to enhance protection and security but involving only *engagement* activities. The DOC has no authority either to demand or enforce cybersecurity standards in these institutions.

Other key private-sector actors, such as the defense industrial base (DIB), have access to or oversee aspects of national interest and therefore receive more cybersecurity emphasis. The DIB includes "the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel."[9] In a memorandum to DOD leadership, the deputy secretary of defense noted that "cyber threats to DIB unclassified information systems represent an unacceptable risk of compromising DOD information and pose an imminent threat to US

national security and economic interest."[10] Consequently, the DOD implemented a cybersecurity and information assurance program in which "DOD provides classified and unclassified cyber threat information and information assurance best practices to DIB companies."[11] The DIB agencies then have a responsibility to "report cyber incidents that may involve DOD information for analysis, development of coordinated mitigation strategies, and, when needed, cyber intrusion damage assessments of compromised DOD information."[12] Unfortunately, the fact that this "responsibility" is not a requirement but voluntary reduces the probability that the DIB actor will self-report because, once labeled a security concern, it could lose government contracts, thereby decreasing revenue.

In addition to the DIB, the US government retains a vested interest in protecting agencies that control portions of the United States' critical infrastructure and key resources (CIKR), the former including "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters."[13] US key resources are "publicly or privately controlled resources essential to the minimal operations of the economy and government."[14] To enhance cybersecurity and awareness, CIKR owners and operators are *encouraged* to remain "integrated both physically and virtually into the [DHS's National Cybersecurity and Communications Integration Center (NCCIC)] during steady-state operations and . . . fully and appropriately integrated into cyber incident response capabilities."[15] Again, because this is the private sector, any participation is purely voluntary. Additionally, President Obama released an Executive Order on Improving Critical Infrastructure Cybersecurity which noted that "in order to maximize the utility of the cyber threat information sharing with the private sector, the Secretary [of Homeland Security] shall expand the use of programs that bring private sector subject matter experts into Federal service on a temporary basis."[16] Thus, these experts can "provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators

in reducing and mitigating cyber risks."[17] Because neither partnerships nor strong relationships exist between the private sector and the US government in this context, the data and information on their networks are vulnerable to cyber attacks in the form of intrusion or exploitation. This vulnerability poses a great threat to US national security.

In Homeland Security Presidential Directive 7, President George W. Bush designated the DHS as the lead agency for protection of critical infrastructure, specifying that the secretary of homeland security will "maintain an organization to serve as a focal point for the security of cyberspace."[18] These roles and responsibilities receive additional detail and refinement in that "through CS&C [cybersecurity and communications], the Secretary of Homeland Security is responsible for providing crisis management and coordination in response to Significant Cyber Incidents."[19] Furthermore, as the lead agency of the NCCIC, the DHS will

> coordinate with all partners, including law enforcement agencies, leading the national effort to investigate and prosecute cybercrime; the IC [intelligence community] regarding threats, intelligence, and attribution; DOD elements regarding intelligence and information sharing, military operations to defend the homeland; State and Local governments; and the private sector to ensure common operational situational awareness is being leveraged by all response organizations as they execute their individual authorities and missions.[20]

With Presidential Policy Directive 21, the Obama administration slightly modified these roles by stating that the DHS retains responsibility to "coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure."[21] It is important to note that although the DHS is charged with cybersecurity, its primary concern is the area of crisis-management response and coordination with other agencies. In fact, the "DHS currently has very limited statutory responsibility for the protection of federal information systems."[22] The National Institute for Standards and Technology (NIST), a nonregulatory federal agency within the DOC, has established a cybersecurity framework to help "critical infrastructure owners and operators reduce risks in industries such as power generation, transportation

and telecommunications."[23] Thus, one US department sets the standards for critical infrastructure cybersecurity, and another is tasked with protecting these assets in the cyber domain. Moreover, according to Mark Weatherford, DHS undersecretary of cybersecurity for the National Protection and Program Directorate, "There's a lack of true cyber security talent. I mean the real ninja kind of guys and gals that you can build your security program around. . . . I don't think it's overstating to say this is a national emergency."[24] The lack of proper authorities and capabilities prevents the DHS from adequately fulfilling its defined responsibilities.

In Homeland Security Presidential Directive 7, President Bush tasked the DOJ, including the Federal Bureau of Investigation (FBI), to "reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources."[25] Although these roles do not specifically mention cyberspace, those of the attorney general were subsequently refined to include offering "guidance on legal issues that require resolution during efforts to respond to, and recover from, a cyber incident; manag[ing] any resulting criminal and/or domestic foreign intelligence investigations; and shar[ing] information from those investigations as permitted by law."[26] The FBI was assigned the responsibility of serving as "the lead agency operating domestically to protect and defend the United States against terrorist and foreign intelligence threats, including those that have a cyber nexus."[27] Presidential Policy Directive 21 modified these roles so that the FBI "conducts domestic collection, analysis, and dissemination of cyber threat information."[28] Additionally, the FBI operates the National Cyber Investigative Joint Task Force—the "focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations, . . . making the Internet safer by pursuing the terrorists, spies, and criminals who seek to exploit [US] systems."[29] Some roles include cyberspace concerns, but the responsibility of the DOJ resides mainly with the prevention of terrorist activities in cyberspace as well

as investigating and prosecuting those who perpetrate these types of activities.

Cybersecurity is a paramount concern for the DOE because "a resilient electric grid is . . . arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services."[30] According to the NIST, cybersecurity "must be included in all phases of the [electric] system development life cycle, from design phase through implementation, maintenance, and disposition/sunset."[31] The DOE supports cybersecurity for the electric grid by "facilitating public-private partnerships to accelerate cybersecurity efforts for the 21st century; funding research and development of advanced technology to create a secure and resilient electricity infrastructure; [and] supporting the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities."[32] Thus, the DOC (through the NIST) sets the standards for cybersecurity of critical infrastructure; the DHS protects critical infrastructure in the cyber domain; and the DOE owns a large portion of the US government's critical infrastructure. This arrangement inevitably produces inefficiencies with cybersecurity for these assets.

As the principal agency responsible for homeland defense, the DOD maintains key roles and responsibilities in cyberspace. It relies heavily on cyberspace; in fact, the "DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[33] Consequently, the department is very dependent upon its networks for "command and control of . . . [its] forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field."[34] The virtual domain, then, is not only a key domain for conducting operations but also a key *enabling* domain for the conduct of operations within the physical domains. As such, the DOD has responsibility for the security and protection of its own cyberspace infrastructure. If necessary, though, it can take "action to deter or defend against cyber attacks that pose an

imminent threat to national security."[35] Regarding this responsibility, as well as the accompanying roles of the DHS, "in extraordinary circumstances, the President, as Commander in Chief, or Congress may authorize military actions to counter threats to the United States. Therefore, DOD may conduct missions as the lead in defending the United States. In such circumstances, DHS, via the NCCIC, works though its processes and with its partners to support DOD missions."[36] By doing so, the DOD assures the security of its networks and cyberspace infrastructure and, when authorized by the president or Congress, conducts activities in cyberspace to defend the United States and its national interests.

Within the DOD, the secretary of defense tasked "cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments."[37] USCYBERCOM, currently a subunified command under USSTRATCOM, "plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[38] Clearly, for the DOD, USSTRATCOM has the responsibilities for operating in cyberspace, but the majority of the department's cyberspace capabilities reside with the subordinate command, USCYBERCOM.

Another DOD combatant command with a stake in cyberspace defense and security, USNORTHCOM plans, organizes, and executes homeland defense missions. Specifically, it "defends America's homeland—protecting our people, national power, and freedom of action."[39] With respect to cyberspace, USNORTHCOM does not have a specifically defined mission; however, no specific domain is associated with homeland defense. Therefore, the currently defined roles appear to require that the command defend the homeland in the cyberspace domain along with the physical domains.

The director of the NSA, an agency also involved in cyberspace, is dual-hatted (i.e., simultaneously serves in both positions) as the commander of USCYBERCOM. The NSA "leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decisive advantage for the Nation and our allies under all circumstances."[40] Although its director is in the DOD, the NSA's roles and responsibilities go beyond one department, supplying "products and services to the Department of Defense, the Intelligence Community, government agencies, industry partners, and select allies and coalition partners."[41] Cognizance of the NSA's information gives the USCYBERCOM commander better understanding of the cyberspace environment.

Recommendations

Any detailing of the cyberspace environment and the roles, responsibilities, and authorities of the private sector and US government agencies therein naturally raises two questions. Are the agencies charged with certain roles and responsibilities capable of performing those tasks? Are the authorities given to the responsible agencies adequate to allow them to secure and defend cyberspace as required? We contend that the answer to both of these questions is no. According to the 2011 *Cyberspace Policy Review* produced by the Office of the President of the United States, the US government "is not organized to address . . . [the cyberspace] problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way."[42] If the United States is to adequately "defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies," then government agencies' roles, responsibilities, and authorities within cyberspace need alteration.[43]

The first major change involves the DIB as well as CIKR owners and operators within the private sector. The companies and corporations that comprise the DIB and support the DOD must incorporate cybersecurity measures that satisfy DOD standards. This effort will undoubtedly encounter resistance; many will claim that it involves an invasion of privacy or that "big brother" is watching them. Additionally, the alteration of security standards and protocols entails inherent costs (in terms of dollars, time, resources, etc.). The best method to prevent these concerns calls for requiring this level of cybersecurity as part of awarding any new DOD contracts and the upgrade of any existing ones. Additionally, all new or updated contracts must include reporting of any cyberspace intrusions, attacks, or breaches. To facilitate this reporting, DIB companies and corporations must adhere to the cybersecurity standards established by the NIST and connect (either virtually or through direct representation) to the NCCIC, which then shares relevant information with the appropriate agencies (National Cyber Investigative Joint Task Force, USCYBERCOM, USNORTHCOM, etc.).

Current laws preclude the US government from levying a similar contractual requirement on CIKR owners and operators. Nevertheless, the NIST established a cybersecurity framework "for understanding, managing, and expressing cybersecurity risk."[44] Most of the services and products provided by CIKR owners and operators are essential for US citizens but not contractually funded by the US government; therefore, the latter cannot demand contractual arrangements similar to those with DIB companies and corporations. An appropriate method for making sure that many CIKR owners and operators adhere to the same conditions placed on the DIB and the standards established by the NIST involves inclusion of contractual wording in any US government–provided insurance, subsidies, grants, and so forth, that they receive. To qualify for government-provided funds, CIKR owners and operators must institute a prerequisite level of cybersecurity as well as a guarantee of reporting any cyberspace intrusions, attacks, or breaches to the NCCIC. An additional measure to persuade them to voluntarily participate involves providing them (at no cost) with the DOD-approved

cybersecurity and information assurance software and training with the stipulation that any intrusions, attacks, or breaches call for notification to the NCCIC. Unfortunately, no panacea exists for cybersecurity within the private sector. By modifying some requirements, though, the US government improves security within the DIB, as well as the CIKR owners and operators, and enhances the requirement for reporting cybersecurity incidents.

With respect to the US government agencies, the president and/or secretary of defense impose desired demands or restrictions. The first major step in improving US cybersecurity and defense is to activate USCYBERCOM as a fully functional combatant command instead of a subunified command under USSTRATCOM. Although no specific activation date currently exists, preparation began several years ago. Current cyber threats and attacks necessitate completion of this action as quickly as possible. As the agency with the best understanding of cyber threats, USCYBERCOM should be redesignated as the principal agency for developing and implementing cybersecurity measures across all US government agencies (by authority of *US Code* Title 40) and the previously discussed DIB and CIKR owners/operators (by authority of *US Code* Titles 10 and 32, respectively). Unfortunately, this step will require a simultaneous reduction in the DHS's responsibilities, explained below. USCYBERCOM must also work with the services to develop capabilities and training for the personnel who detect and respond to attacks in the cyber domain (if the president or secretary of defense should authorize the response). Indeed, USCYBERCOM is already anticipating a massive manning influx of more than 900 personnel between 2014 and 2016; active service members are scheduled to fill 80 percent of these slots, and the rest by civilians.[45] Further, USCYBERCOM "activated the headquarters for its Cyber National Mission Force . . . [to] react to a cyber attack on the nation."[46] Unfortunately, establishing a new combatant command that concentrates mainly on a specific domain generates other challenges. For example, the austere fiscal environment imposes tightening of the military services' purse strings,

making the expenditure of funds on a largely underestimated and ill-defined problem difficult to justify.

The role of the NSA in cybersecurity also needs modification. Its capability for determining the indications and warnings of an impending or ongoing attack—as well as attributing attacks to individual actors, groups, or nation-states—needs more utilization by the US government in cybersecurity. The NSA must have connectivity into the NCCIC to facilitate the sharing of intelligence and information across the cyber domain. Additionally, since the agency's director is also the USCYBERCOM commander, the two entities can codevelop the previously mentioned cybersecurity standards and measures, thereby enabling a better product. Unfortunately, this dual-hatting of a single commander with both *US Code* Title 10 and Title 50 authorities remains a tenuous proposition for many members of Congress. Rectification of this contentious issue is essential if a unified combatant command should come into existence.

Although USNORTHCOM is the combatant command specifically charged with homeland defense, a partnership between it and USCYBERCOM for defense in the cyber domain must be codified. A similar partnership exists between USNORTHCOM and USSTRATCOM in the space domain. USCYBERCOM retains the capabilities and should have the authorities for cybersecurity and defense, but it cannot determine if a cyber attack is a precursor to or a portion of a larger attack. To remedy this deficiency, USNORTHCOM requires full integration into the NCCIC to guarantee availability of a detailed description of the homeland defense environment across all domains—air, land, maritime, space (with USSTRATCOM), and cyberspace. The understanding of threats in all domains enables the USNORTHCOM commander to give the president and/or the secretary of defense an assessment of current or expected attacks against the homeland.

The DHS's role also demands redefinition. Although currently the lead agency for cybersecurity, the department cannot perform this role. Even though the DHS should retain responsibility for securing critical infrastructure in the physical domain, the president should

redefine its cybersecurity role to include coordination of cybersecurity intelligence and the consequence-management portion for effects after a cyber attack that results in physical damage. For the crisis-management response, the DHS's Federal Emergency Management Agency remains the lead organization. The DHS's NCCIC should continue to function in its current capacity; however, USCYBERCOM must have co-ownership or co-oversight of this center. Because USCYBERCOM maintains more cybersecurity and cyber defense capabilities, its additional involvement enhances the NCCIC's capabilities. Furthermore, dual oversight by the DHS (by authority of *US Code* Title 6) and the DOD (by authority of *US Code* Title 10) prevents reliance on a single agency for cybersecurity. Finally, USCYBERCOM's increased engagement in the NCCIC improves the DOD's situational awareness within the cyberspace domain.

The DOJ should keep its focus on cyber terrorism and implement only minor alterations to its roles and responsibilities. The FBI should continue as the lead agency that operates domestically to protect and defend the US cyber domain against terrorist attacks as well as maintain the National Cyber Investigative Joint Task Force. USCYBERCOM, however, must have responsibility for defending against cyber threats emanating from a state-sponsored foreign intelligence agency. Attacks and intrusions from these actors require proper analysis to determine if they are part of a larger attack on the US homeland. Note that none of these proposed changes affects or reduces the investigative authorities and roles of the FBI, which should remain the lead federal agency for conducting law-enforcement activities.

Conclusion

The future of US cybersecurity, cyber defense, and cyber response is not clear. However, policies that currently define authorities, roles, and responsibilities do not adequately address the ever-increasing threat in the cyberspace domain. With some dramatic changes within the authorities and responsibilities, the US government could drastically

improve its ability to protect US citizens from cyber threats. Specifically, the companies and corporations that comprise the DIB and support the DOD must incorporate cybersecurity measures that satisfy DOD standards. USCYBERCOM should be designated a functional combatant command, share control and oversight of the NCCIC with the DHS, and be tasked with responsibilities in the cybersecurity, cyber defense, and cyber-response realms by authority of *US Code* Title 10 and 32. USNORTHCOM requires integration with USCYBERCOM through the NCCIC; as a combatant command charged with homeland defense, USNORTHCOM must examine a broader range of threats (across the physical and virtual domains) to determine if a cyber attack is part of an overall larger attack by a nation-state. The DHS should retain responsibility for securing critical infrastructure in the physical domain. The DHS's cybersecurity role should be reduced to include only the consequence-management portion (by the Federal Emergency Management Agency) for effects after a cyber attack that results in physical damage. Incorporation of these recommendations will enhance the mitigation of these types of challenges and concerns. ✪

Notes

1. Office of the President of the United States, *Cyberspace Policy Review* (Washington, DC: White House, 2011), i, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
2. Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), 12, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
3. Office of the President of the United States, *Cyberspace Policy Review*, iii.
4. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, July 2011), 5, http://www.defense.gov/news/d20110714cyber.pdf.
5. Office of the President of the United States, *National Security Strategy* (Washington, DC: White House, May 2010), 27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
6. Department of Defense, *Strategy for Operating in Cyberspace*, 3.
7. Ibid., 4.

8. Office of the Press Secretary, "Presidential Policy Directive/PPD-21" (Washington, DC: Office of the Press Secretary, White House, 12 February 2013), 5, https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

9. Department of Defense, *Strategy for Operating in Cyberspace,* 8.

10. Office of the Deputy Secretary of Defense of the United States, to Department of Defense Leadership, memorandum, subject: Defense Industrial Base Cyber Security, October 2012, par. 1.

11. Ibid., par. 3.

12. Ibid.

13. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, DC: Department of Homeland Security, 2009), 109, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

14. Ibid., 110.

15. Department of Homeland Security, *National Cyber Incident Response Plan*, interim version (Washington, DC: Department of Homeland Security, September 2010), 7–8, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

16. Office of the Press Secretary, *Executive Order—Improving Critical Infrastructure Cybersecurity* (Washington, DC: White House, 12 February 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

17. Ibid.

18. Office of the President of the United States, "Homeland Security Presidential Directive-7" (Washington, DC: White House, December 2003), par. 16, https://www.dhs.gov/homeland-security-presidential-directive-7.

19. Department of Homeland Security, *National Cyber Incident Response Plan*, 5.

20. Ibid., 24n43.

21. Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 3.

22. Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, CRS Report for Congress R42114 (Washington, DC: Congressional Research Service, 20 June 2013), 9, http://www.fas.org/sgp/crs/natsec/R42114.pdf.

23. "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments," National Institute of Standards and Technology, 22 October 2013, http://www.nist.gov/itl/cybersecurity-102213.cfm.

24. Amber Corrin, "DHS Feels Growing Pains in Cybersecurity Role," FCW, 17 October 2012, http://fcw.com/articles/2012/10/17/dhs-cybersecurity.aspx.

25. Office of the President of the United States, "Homeland Security Presidential Directive-7," par. 22 (a).

26. Department of Homeland Security, *National Cyber Incident Response Plan*, 6.

27. Ibid.

28. Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 4.

29. "National Cyber Investigative Joint Task Force," Federal Bureau of Investigation, accessed 9 March 2013, http://www.fbi.gov/about-us/investigate/cyber/ncijtf. See also Office of the Press Secretary, "Presidential Policy Directive/PPD-21," 4.

30. "Cybersecurity," Department of Energy, accessed 6 March 2014, http://energy.gov/oe/services/cybersecurity.

31. National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements* (Washington,

DC: National Institute of Standards and Technology, August 2010), 1, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

32. "Cybersecurity," Department of Energy.

33. Department of Defense, *Strategy for Operating in Cyberspace*, 1.

34. Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2010), 37, http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf.

35. Department of Homeland Security, *National Cyber Incident Response Plan*, C-2.

36. Ibid., 10.

37. Department of Defense, *Strategy for Operating in Cyberspace*, 5.

38. "US Cyber Command Factsheet," US Strategic Command, accessed 5 September 2014, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

39. "About USNORTHCOM," US Northern Command, accessed 5 September 2014, http://www.northcom.mil/aboutUSNORTHCOM.aspx.

40. "About NSA," National Security Agency, accessed 13 February 2013, https://www.nsa.gov/about/mission/index.shtml.

41. Ibid.

42. Office of the President of the United States, *Cyberspace Policy Review*, i.

43. Office of the President of the United States, *International Strategy for Cyberspace*, 12.

44. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0 (Washington, DC: National Institute of Standards and Technology, 12 February 2014), 7, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

45. Andrew Tilghman, "Cyber Command to Hire Thousands of Troops, Civilians," *DefenseNews*, 12 February 2013, http://www.defensenews.com/article/20130212/C4ISR01?302120026/Cyber-Command-Hire-Thousands-Troops-Civilians.

46. Cheryl Pellerin, "Cybercom Activates National Mission Force Headquarters," US Department of Defense, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

Lt Col August G. Roesener, PhD, USAF

Lieutenant Colonel Roesener (USAFA; MS, University of Florida; PhD, University of Texas; MMOAS [Master of Military Operational Art and Science], Air University) currently serves as the chief analyst for Headquarters Air Mobility Command, Scott AFB, Illinois. He previously performed campaign plan assessments as a joint air analyst at the North American Aerospace Defense Command, US Northern Command, Peterson AFB, Colorado

Maj Carl Bottolfson, USAF

Major Bottolfson (BA, University of Wisconsin; MA, Trident University International) serves as chief of policy in the Department of Defense Executive Agent for Space staff. He received his commission through ROTC at the University of Wisconsin in 2000. Prior to his current assignment, Major Bottolfson served as chief of space policy at US Strategic Command and chief of space situational awareness operations at the Joint Space Operations Center, Vandenberg AFB, California.

CDR Gerry Fernandez, USN

Commander Fernandez (BS, San Diego State University; MS, Naval Postgraduate School) serves as section head for service-level management and communication and information systems requirements at Headquarters North Atlantic Treaty Organization, Supreme Allied Commander Transformation. He received his commission through ROTC at San Diego State University in 1992. Commander Fernandez previously served on the staff of the commander, Joint Task Force Horn of Africa, in Djibouti, Africa.

Let us know what you think! Leave a comment!

The Search for Space Doctrine's War-Fighting Icon

Dr. Dale L. Hayden

The reason for the US Air Force's existence is rather straightforward—nothing more or less than to protect and defend the nation. It does so by holding adversaries at risk, unhampered by the tyranny of distance and time. How it goes about accomplishing this task is complex and occurs across all domains. The Air Force, as do the other services, looks to doctrine to provide a foundation and guidance regarding how to operate within each separate domain and collectively in the joint environment. Those who operate on the land, at sea, and in the air have lead theorists to whom they point as seminal to their doctrine development. Carl von Clausewitz, Alfred Thayer Mahan, and Giulio Douhet serve as foundational figures in the path toward war-fighting doctrine. For decades space professionals have asked, "Who is our foundational theorist?" or "Where is the space Mahan?" Who is space's doctrinal icon, and if one does not exist, why not?

Doctrine that revolutionized warfare involved forces which independently shaped the battlefield. Clausewitz, Mahan, and Douhet observed the world around them and chronicled what they saw as the keys to victory. What separated these men from others was their ability to see beyond existing convention or the current state of technological development. They could envision future potential by which armies, navies, and air forces should best deploy forces to defeat their enemies.

Independently of other services, each man reflected upon how victory could be achieved within and through a specific domain.

Land and sea doctrine evolved over centuries. War-fighting air doctrine came about less than 30 years after the first powered flight. In each case, observation was the key element to developing effective theories and strategies that would lead to war-fighting doctrine. Given America's more than 50 years of experience in space, some people might expect war-fighting space doctrine to have fully matured. This article explores why this is not the case.

For example, joint doctrine defines *space superiority* as "the degree of dominance in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from space-based threats."[1] One significant problem exists, though. Unlike its ability to establish air superiority, the US military has limited means to create space superiority in a contested environment.[2]

A Historical Milieu

For the uninitiated, Mahan was a US naval officer who in the late nineteenth century proposed theories of naval warfare. His theories provided a foundation for maritime doctrine that resulted in the United States becoming a global naval power in the twentieth century. If a space Mahan does not exist today, then the logical next question must be, why not? Maybe the time is not yet right to expect mature war-fighting space doctrine, and that is why the domain has not yet produced its icon. Then, one would logically ask, when might be the right time? To answer that question requires looking at the purpose of doctrine and why each service must describe what it does on the battlefield.

In the latter half of the twentieth century, space began to play an ever-increasing role in protecting and defending the nation. The services and the joint community developed doctrine to reflect how the

space domain is used to support the joint effort and the combatant commander's needs.

The Department of Defense defines doctrine as "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."[3] Thus, space doctrine is a necessity in conducting the joint fight. However, a less formal view could describe military doctrine. In its simplest terms, doctrine prescribes how military forces execute combat through campaigns, operations, and battles. If we use this definition, the question about war-fighting space doctrine might require a different answer.

We can best obtain an understanding of why this is not yet the time for mature war-fighting space doctrine by conducting a brief review of how current doctrine developed on land, at sea, and in the air. Before joint doctrine existed, each service followed certain guidelines—either codified or not—that directed their actions. The Roman phalanx, Genghis Khan's cavalry, and Horatio Nelson "crossing the T" gave their militaries a distinct advantage over their adversaries. These approaches loosely governed how armies and navies executed combat on a tactical and regional scale. Each in its own way contributed to 1,000 years of Roman rule in Europe, a Mongol Empire stretching across Central Asia and China, and the sun never setting on the British Empire.

From the early days of human civilization, a nation's greatness was determined by the might of its army. During the Renaissance, naval power began to emerge as a significant determinant of power. Exploration and trade, as demonstrated by the city-state of Venice, began to show how ships at sea could create a nation's wealth and power. The American experience was no different. As the colonies attempted to break free of Mother England, the fledgling nation looked to the Continental Army to win its independence. Gen George Washington borrowed tactics and strategy from Europe, relying heavily upon the training and guidance of Frenchman Gilbert du Motier, Marquis de Lafayette—better known today simply as Lafayette. Up until the Ameri-

can Civil War, European doctrine continued to promulgate through the US Army. Young officers at the US Military Academy were educated first as engineers—a necessity demanded by civilizing a continent—and next as soldiers steeped in studies of the Napoleonic wars and the theories of Gen Antoine-Henri Jomini. Prior to the Civil War, the translated writings of Jomini were the only works on military strategy taught at West Point.[4]

When Pres. Abraham Lincoln called upon the US Army during the Civil War, it took years for a semblance of American doctrine to arise. Both Union and Confederate commanders attempted to execute the war in European fashion with traditional battle lines and frontal engagement. This all changed with Gen Ulysses S. Grant, who employed what might be described as attrition warfare—leveraging the greater manpower and industrial might of the North against a less populated, more agrarian South. Essentially, Grant set out to exhaust the Confederacy and destroy its ability to conduct military operations, earning him the nickname "Butcher Grant."[5] The number of casualties in a conflict became secondary to the overall success of the battle. Whereas Union generals like George McClellan at Antietam and George Meade at Gettysburg failed to press the advantage in order to allow their troops to rest, Grant continued to engage the Army of Northern Virginia until Gen Robert E. Lee surrendered at Appomattox.[6] In his book *The American Way of War*, Russell Weigley described Grant's approach as "a strategy of annihilation."[7]

As the US Army moved toward modern warfare in the years between the Civil War and World War I—the United States' nineteenth-century interwar period—it again turned to Europe, only this time to rising power Germany for its command structure and basic military guidelines. One German whom the US Army would eventually embrace—more so after the Vietnam conflict—was Clausewitz, a Prussian general who chronicled warfare during the Napoleonic era in his work *On War*. Clausewitz wrote of a thoughtful and philosophical approach to warfare, which he saw as something that could be studied and ana-

lyzed systematically, focusing on offense rather than defense, as had Jomini. Rather than viewing war as an event of chaotic disorder to overcome, he recognized that it involved economies and technologies—not just people on a field of battle.[8]

During the latter half of the nineteenth century, the US Navy had its own strategist and proponent of naval doctrine—Mahan. Called "the most important American strategist of the nineteenth century," Mahan observed the political and military environment of his time and concluded that great nations must possess great navies.[9] During a period of technological change and global expansion for the United States, Mahan's book *The Influence of Sea Power upon History, 1660–1783* transformed not only the US Navy but also the navies of France, Germany, Britain, and Japan.[10] Mahan emphasized mass at the strategic point of attack, detailing an approach to counter the global British threat while portending the naval battles of World War I and beyond.

The late nineteenth century also witnessed advanced technological innovation on and off the battlefield. Armies acquired artillery that could range for miles; navies moved from wooden sailing ships to steel-hulled warships; and for the first time, with the Wright brothers' accomplishment at Kitty Hawk in 1903, the United States recognized the potential for powered flight. Entering World War I, European militaries possessed mature doctrine that directed the actions of their land and sea forces. The air component, however, required seasoning as it transformed from aerial observation platforms to aircraft that played an integral part in determining the outcome on the battlefield. Douhet, one of the earliest airpower theorists, was an Italian general who observed World War I warfare and looked beyond the fragile flying machines constructed of wire, wood, and canvas to their potential for shaping future wars. His goal in future conflict called for avoiding the stalemate of trench warfare and shortening the struggle through airpower, thus reducing the carnage that destroyed an entire generation of men in Britain, France, and Germany. In his treatise *The Command of the Air*, Douhet detailed gaining control in the air and attacking vital

centers as central to the conduct of any air operation.[11] More than 70 years later, his thoughts remain essential to airpower theory and doctrine.

During the interwar years, the Air Corps Tactical School at Maxwell Field, Alabama, began teaching air doctrine. Heavily influenced by the observation and thoughts of Brig Gen William "Billy" Mitchell and Douhet, a select group of former faculty members would go on to develop the airpower concepts employed in World War II.[12] Their work started the evolution of airpower tactics and strategies that would aid in transforming an isolated America during the 1930s into a global economic and military superpower.

From their concepts of daylight precision bombing employed during World War II to attacks on the centers of gravity during Operation Desert Storm, airpower doctrine continued to evolve. Men like Mitchell and Col John Warden advocated airpower's role in winning conflicts and protecting America's sovereignty. Mitchell's experience in World War I and Warden's on the Korean peninsula and during the Vietnam conflict shaped their views of airpower. Through observation, both men formulated concepts that would later shape air warfare in the twentieth century. In particular, Warden's first book, *The Air Campaign: Planning for Combat*, challenged prevailing AirLand Battle doctrine which held that airpower is subservient to the land battle and reemphasized the strategic nature of airpower.[13]

A brief look into the past helps demonstrate that observation of the battlefield has been a key element in the development and evolution of doctrine on land, at sea, and in the air. Historically, doctrine was developed so that soldiers on the battlefield who could not see their comrades might have a degree of certainty about how units on their right and left flanks would behave and respond in battle (i.e., so that they know what the guys to the right or left of them are doing). Consequently, in the days of linear warfare, troops had confidence that their flanks were protected and that they need not be concerned about the enemy attack from the rear. Today, warfare is considerably more complex, and doctrine has evolved to reflect the new environment. This

evolution in warfare took time. Indeed, one question that we must address asks whether space has been involved in warfare long enough to observe best practices.

Since the first successful US space launch in 1958 with Explorer, the United States has aggressively engaged in space exploration and exploitation. After more than 50 years, space has become both an integral part of everyday American life and critical to the twenty-first-century American way of war. Capabilities demonstrated by precision-guided munitions over the past two decades only hint at what space can bring to the battlefield. Even with our dependence upon space and the integration of its assets into the combat mission of all services, those assets alone cannot—yet—independently shape the battlefield, as can armies, navies, and air-breathing airpower. Without the ability to do so—like armies, navies, and air forces—it is impossible for a "space Mahan" to emerge.

The Present Dilemma

The fact that space assets cannot independently alter the course of combat does not mean that the force should not think about, or even write about, space doctrine. If Douhet and Mitchell had not pondered air combat during World War I, then coherent air doctrine would not have emerged during the interwar years. Moreover, as US military doctrine has evolved, each service looks to the printed page to guide how it integrates and operates in the joint environment. For that purpose alone, space doctrine as written today finds relevance. Space professionals cannot afford to play catch-up or wait for the day when the battlefield is shaped from the heavens. Waiting could have disastrous effects, costing US lives and placing national sovereignty at risk. One more short departure into our history can help explain this urgency.

History is littered with examples of technological development outpacing doctrine. More often than not, the result has been needless loss of life. Centuries of warfare supplied the template. For armies in con-

tact, battle lines were separated by the approximate distance of the firing range of the standard firearm of the day. Troops would rush en masse across the open fields to ensure concentration of the greatest amount of firepower on the enemy's position, attempting to cover the distance before the opponent could reload. Despite the advancement from using the smooth-bore musket to placing helical grooves in a gun barrel (rifling), tactics remained essentially the same. From the American Revolution to the American Civil War, range and accuracy increased sixfold, from 100 yards to greater than 600 yards. Attempting to cover the increased distance, men found themselves deep within killing fields between lines. On a single day during the Battle of Cold Harbor, 90 percent of the more than 6,000 casualties occurred because of small-arms fire.[14]

Technology continued to advance over the next 50 years, further outpacing doctrine. World War I found the static battle lines employed for generations now in trenches, but artillery that could effectively range for miles as well as machine guns and barbed wire deterred advancing troops. Out of the horror of battle came airpower doctrine as an attempt to overcome centuries of ground doctrine that had led to stalemate and the death of hundreds of thousands.

In one modern-day example—cyberspace—we appear to be playing catch-up insofar as doctrine lags technology. The argument rages about using cyberspace for offense, while as a domain, cyberspace has already demonstrated that actions there can independently affect the battlefield, where nonkinetic actions can have kinetic effects. More specifically, in 2010 a software virus reportedly ruined almost one-fifth of Iran's nuclear centrifuges.[15] As a service, we still struggle with what is in cyberspace and what is not, from systems to career fields. But we must postpone the question "Where is the cyberspace Mahan?" for another day.

Today, US doctrine has reached the point where modern warfare is seldom executed solely by one service. The American military in the twenty-first century can be described in many ways, but none is more

telling than the word *joint*. Although combat may at times seem isolated to a single service, in reality each one must rely upon the other to ensure that the adversary is deterred or defeated, as necessity dictates. This precept is as true with space as it is in any other domain. One interesting observation: land, sea, and air doctrine as envisioned by Clausewitz, Mahan, and Douhet, respectively, developed somewhat independently, but war-fighting space doctrine may not have that opportunity. It will be very interesting to see how it evolves under this construct of "jointness."

What's Next?

The next logical progression in relation to combat would be either warfare in the space domain or, more likely, assets in space independently influencing earthbound combat, be it in the air, at sea, or on the ground. Space is long past being weaponized or used to support military operations. Corona, launched in the early 1960s as the United States' first "spy satellite," provided information to our war planners on the state of the Soviet military arsenal. The Global Positioning System first offered navigation and timing to the US military for use in combat. Thus, both of these satellites weaponized space decades ago—and these are just two limited examples.

Since the 1950s, space professionals have talked about raining down death and destruction from above or launching kinetic projectiles from Earth's orbit onto ground targets.[16] Technology has long evolved beyond the point where kinetic weapons, either nuclear or not, could be placed into orbit and directed upon a point on Earth. Some individuals argue that the antisatellite systems employed by the old Soviet Union and, more recently, China have crossed that redline. Political constraints, whether treaties or conventions, currently prohibit or restrict warfare in space. However, few would argue that warfare will eventually come to the space domain. Where mankind endeavors, conflict has always followed. Once that occurs, space combat will be observed

and documented, and then war-fighting space doctrine will readily emerge. Space will then have its Mahan. ✪

Notes

1. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 16 July 2014), 237, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. On 21 February, 03:26 GMT, the *Ticonderoga*-class missile cruiser USS *Lake Erie* fired an SM-3 missile, intercepting a deorbiting US satellite (USA-193) about 133 nautical miles above the Pacific Ocean. Although a successful demonstration of the US missile defense system, technically this action was neither an antisatellite event nor destruction of a satellite on-orbit, as demonstrated by the Soviet Union (now Russia) and China.

3. JP 1-02, *Department of Defense Dictionary*, 78.

4. John Whiteclay Chambers II, ed., *The Oxford Companion to American Military History* (Oxford, UK: Oxford University Press, 1999), 720.

5. Edward H. Bonekemper III, "The Butcher's Bill," *Civil War Times* 50, no. 2 (April 2011): 36.

6. John Keegan, *The American Civil War: A Military History* (London: Hutchinson, 2009), 96–97.

7. Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington: Indiana University Press, 1973), 128.

8. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75–76.

9. Keegan, *American Civil War*, 272.

10. A. T. Mahan, *The Influence of Sea Power upon History, 1660–1783* (New York: Barnes & Noble Books, 2004).

11. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983).

12. Robert T. Finney, *History of the Air Corps Tactical School, 1920–1940* (Washington, DC: Center for Air Force History, 1992), 56–59.

13. John A. Warden III, *The Air Campaign: Planning for Combat* (Washington, DC: National Defense University Press, 1988). See also John Andreas Olsen, *John Warden and the Renaissance of American Air Power*, 1st ed. (Washington, DC: Potomac Books, 2007), 80.

14. Gordon C. Rhea, *Cold Harbor: Grant and Lee, May 26–June 3, 1864* (Baton Rouge: Louisiana State University Press, 2002), 234.

15. Michael B. Kelley, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, 20 November 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

16. Jonathan Shainin, "Rods from God," *New York Times*, 10 December 2006, http://www.nytimes.com/2006/12/10/magazine/10section3a.t-9.html?_r=0.

Dr. Dale L. Hayden

Dr. Hayden is the deputy director of the Air Force Research Institute (AFRI) at Maxwell AFB, Alabama. He possesses a broad background in US policy and space and missile operations. Dr. Hayden has served as dean of Air Command and Staff College, a member of the Secretary of the Air Force's Staff Group, an assistant professor of history at the United States Air Force Academy, and at AFRI as a faculty researcher and chief of research. Having earned the Master Space Badge, his experience in space and missile operations includes providing space support and missile warning in-theater during Operations Desert Storm and Provide Comfort and command in missile operations. Dr. Hayden has served as a Harvard Fellow and director of the Airpower Research Institute.

Let us know what you think! Leave a comment!

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

A Global Space Control Strategy

Dr. B. T. Cesul

The 2011 *National Security Space Strategy* notes that space is becoming an operating medium in which the continued dominance of the United States is not assured.[1] Already, potential adversaries have overtly demonstrated advancement in the development of space control systems that directly threaten the US use of space today—China's 2007 destruction of a domestic satellite with a direct-ascent antisatellite (ASAT) system is the highest exemplar.[2] Additionally, other nations such as Russia have surpassed the post–Cold War taboos of talking about the development of space control activity with the announcement of the fielding of the Sokol-Eshelon airborne laser ASAT system and continued references to new space control weapons under development to challenge the United States.[3] Consider also the lowered barrier of entry for space systems development because of small satellite and microelectronic technology advances and the perceived lack of tangible, international sanctions and punishment as a result of acknowledged ASAT testing. These factors have muddied the international-policy picture. Emboldened actors appear ready to push the envelope as to what the United States and international community will accept in ASAT testing and development before significant pushback is enacted. Further, a growing body of literature suggests that space-based intelligence, surveillance, and reconnaissance (ISR); communication; and precision navigation and timing assets are in various stages of development in potential adversary nations to support the employment and improvement of terrestrial weapons.[4]

Furthermore, a "space war" has been predicted in blue ribbon commission reports and congressional testimony, and the chances of conflict with an adversary possessing space control capabilities are high in the next 10 years.[5] In fact, open-source reports of events such as the 2003 jamming of a commercial communication satellite by Iran from Cuban locations and multiple satellite-jamming events reported during various Arab Spring events indicate that we have already entered an "Age of Space Warfare."[6]

Space warfare is a politically fraught concept. It encompasses sensitive government activities and commercial entities seeking a benign environment. It is politically taboo to discuss space control events. Doing so runs the risk of creating panic within the booming commercial satellite industry or, worse, suggesting a space arms race. The US Air Force uses the terminology of "space superiority" in which offensive space control, defensive space control, command and control, and space situational awareness (SSA) form a four-legged-stool construct.[7] Attempts to construct a framework in which to discuss the strategic implications of such have led to analogies based on other war-fighting mediums, such as John Klein's *Space Warfare* (naval analogy) or David Lupton's *On Space Warfare* (influenced by airpower theory).[8] These and other works attempt to cast the space warfare issue in light of an overall space security posture. Although these efforts are more appropriate for a national-level vision on the usage of space for power projection, this article attempts to lay a framework and establish basic conceptual tenets necessary for a discussion of the development of a national space control strategy consistent with our desire to remain the world's dominant space actor.

The intent behind the operations is different, but in reality offensive and defensive space control can be thought of as a single concept—space control—since adversaries will likely not draw those distinctions between offensive and defensive space control if the US action is to induce effects on their space or counterspace capability. Space control, as defined in this article, is the use of weapon systems or operational

concepts to gain military advantage by the denial or defense of space and counterspace assets. Simplistically, space control can be thought of as jammers, lasers, and missiles attacking satellites, but the capability has a depth beyond just "spearheads." The United States has acknowledged possessing a space control capability—the Counter Communications System, a ground-based option to "deny adversary IADS [integrated air defense system], deny satellite services (fixed, broadcast), and provide electronic support capabilities."[9] Other historical systems (F-15 ASAT, Brilliant Pebbles, etc.) can be brought up as well to show that space control technologies are not new to the Department of Defense (DOD).[10] However, in the contemporary context with budgetary pressures and a multipolar world threatening the entirety of US space usage, new space control capabilities need to be developed. But without a coherent, unifying space control strategy grounded in an understanding of the required missions and the means to do so, acquisition efforts may become exercises in developing individual capabilities with significant inefficiencies detrimental to operations, infrastructure, and purpose. If implemented, the space control strategy presented below can be used as a guidepost to ensure that new weapon systems are developed in the context of a holistic space control architecture, avoiding the customized acquisition solutions that may provide point solutions to specific threats which may never materialize in an adversary nation.

The Strategy

The United States, through the DOD and with support from the Office of the Director of National Intelligence, should develop space control capabilities in order to reach two goals:

1. Ensure an initial deterrent posture that discourages adversaries from conducting space control operations and continues US access to space, enabling terrestrial power projection. If deterrence fails, the United States will be able to conduct military operations without the use of individual, distinct space assets.

2. In case of crisis and conflict, exercise across a five-dimensional spectrum (deceive, deny, degrade, disrupt, and destroy) of effects capabilities against an adversary's space and counterspace systems that provide utility to his military capabilities.

To enact this strategy, the United States should pursue space control capabilities to

1. control the electromagnetic (EM) spectrum over and within a locale at a time and severity of our choosing to enable US freedom of action and information dominance;
2. counter, both kinetically and nonkinetically, adversary space and counterspace systems directly threatening US assets in space or terrestrially, with preference to options that minimize disruptions to US and allied space capabilities while defeating the enemy kill chain as early as possible in a crisis situation; and
3. utilize a command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) posture (including the development of SSA architecture) that allows the United States to develop and execute space control plans and operations, specifically provide indications and warning of catastrophic space events, discover indications and warning of impending hostile space control activities, maintain custody of threat systems, and deliver intelligence to support space control options.

Rationalizing the Strategy

First, acknowledgement that the space environment presents unique challenges that affect strategy must be addressed. Although it is true that space is largely a "transparent" environment (i.e., because of orbital mechanics, satellite overflight will be fundamentally repeatable over a certain ground area), space is not a clear operating environment. Lack of a globally shared tracking and monitoring network at an acceptable persistence tempo, staffed with sensors of a sufficiently

high performance metric, allows for blind spots to develop—even our SSA picture. Because of maneuver operations, intelligence exploitation of shortfalls in geographic sensor placement and performance, and the potential to change the apparent signature through a simple alteration of orientation with respect to sensor-point angles, we can never be certain about what a space object is and what it is doing. Therefore, a strategy must acknowledge that omniscience in SSA is not possible and that a risk-management process must be the foundation of planning space operations and responses.

Second, we must realize that in order to conduct effective space control efforts, the Title 10 and Title 50 communities in the United States have to be unified, at least in purpose if not in (limited instances) structure. The union of capabilities is necessary because (1) the space assets used are both Title 10 *and* Title 50 assets and (2) the Title 50 side has the preponderance of information necessary to enact space control operations. The intelligence community can bring the exquisite intelligence products on capabilities and performance of foreign space/counterspace systems as well as specific target-development data that the "space war fighter" needs to perform weaponeering against an adversary's space or counterspace capability. Because of the historical divide in the United States between Title 10 and Title 50 space and counterspace activities, we need a formal recognition of the need (and assignment of duty as provided with this language). Already some efforts have taken place (e.g., creation of the Space Security and Defense Program) inside the US government to establish bridgeheads across the Title 10 / Title 50 divide. Ideally a future Joint Intelligence Operational Center for space would be the focal point for space control support efforts and would have pre-positioned Title 50 intelligence available to support its operational activities. In today's force structure, this function would be filled by the Joint Space Operations Center under the Joint Functional Combatant Command for Space. However, the proposed strategy does not make that distinction since the Title 10 community's concept of how to conduct space control operations is still maturing and the proposed strategic construct does not desire to

force upon the Title 10 community a responsibility that it may not be ready to accept. But it does need to be absolutely clear that in matters of the development and operation of space control capabilities, the DOD has the lead with the elements of the Office of the Director of National Intelligence in a support role.

Strategic Goal One: Ready to Fight without Trying to Pick One

Maintaining a conflict-free environment is always preferred. The desired end state is avoidance and deterrence of conflict that may escalate into terrestrial battle with human casualties. In general the United States should try to maintain stability by using a strong deterrent posture to discourage escalatory activity in space. However, maintaining deterrence is complicated by three factors unique to the space fight: (1) demonstrating and fielding a believable deterrent capability is in itself a destabilizing position in the current geopolitical climate, (2) the physics of space and counterspace operations allow first strikes to occur in a relatively short time frame, reducing the response time for counter-countermeasures, and (3) in any calculus of a "space war," the potential adversary has a strategic advantage in challenging US space dominance since no other entity integrates and uses space-enabled capabilities into its war-fighting capacity to the extent the United States does. Consequently, the best defense in discouraging an adversary action against US space dominance may be to prove that the United States can fight and win without some space capabilities.

The current political climate, both internationally and domestically, is generally aligned against the "militarization of space." As enshrined in the 1967 Outer Space Treaty, space is to be treated as a global commons for mankind.[11] Indeed, even during the Cold War when both the United States and USSR flew dozens of national security space assets, these were considered immune from attack in most cases outside the imminent eruption of full-scale nuclear war.[12] Today the overwhelming shadow of US conventional military dominance, now definitively enabled by space utilization, has caused a knee-jerk reaction to try to

limit continued US development of military space capabilities through soft power mechanisms of United Nations treaties and other international agreements in proposal. With regard to space control specifically, multiple instances demonstrate a hypersensitivity to the perception of US space control activity.

This has likely caused an internal "pullback" within US leadership to avoid discussing the aspects of US space control development. Some people would argue that we are really seeing a realization of strategic ambiguity (e.g., the "Israeli nuclear posture"), but it is more a function of a desire to minimize international stressors. Effective development and employment of space control capabilities demand open recognition that the United States is willing to develop and field space control capabilities in an operational context. Adversaries already believe that the United States is a 10-foot-tall giant; however, they also believe that political pressure will voluntarily restrict our usage of overwhelming force and open windows for their victory (and continued aggressions). A clear and unambiguous statement of our capabilities and intention to use them may buy us the strategic pause necessary to try to de-escalate situations from a conflict state.

From the policy maker's perspective, space control is expensive and provocative, and the desire to enter into another costly military buildup has ebbed. The 2012 fact sheet on the DOD's space policy mentions resiliency of the architecture as a key acquisition strategy but does not address the active development of space control.[13] One can interpret this omission to mean that the United States cares only about defending current assets and not imposing conditions of our choosing in the space medium. Point number four on the 2011 fact sheet on the DOD's strategy for deterrence in space states that the United States will "be prepared to respond to an attack on U.S. or allied space systems proportionally, but not necessarily symmetrically and not necessarily in space, using any or all elements of national power."[14] This assertion reserves the right for space control development; additionally, it might increase the adversary's apprehension that should

the United States not have adequate space control measures, it could strike terrestrially, possibly increasing the enemy's desire to conduct operations on a larger scale to ensure that the US response is muted by loss of enabling space capability.

Transitioning to Strategic Goal Two: Bringing the Wood

The language in these two fact sheets reserves rights for response and a commitment to resiliency. However, because of the short time frames involved with many counterspace attacks, "he who shoots first wins the first battle." Direct-ascent attacks from launch to intercept in low Earth orbit are approximately 10 minutes in duration. Directed-energy attacks and radio frequency (RF) jamming attacks, once committed to, are nearly instantaneous in their effect because the attacking medium travels at the speed of light. This highlights the need for preemptive action to protect space assets. It differs from preemptively starting a war, and—in the context of a potential global conflict—striking an adversary before he can shoot is advantageous. A purely defensive posture of countermeasures, protective technology, and rapidly enacted changes in the concept of operations is less provocative but also probably more costly and less likely achievable, considering the nearly omniscient intelligence picture that would have to be developed for every potential adversary and action. Development of a multilayered space control strategy allows preemption to be on the table.

Another problem is that the DOD's use of space capabilities is not only a significant force multiplier but also a substantial vulnerability in the way we conduct modern warfare. No other nation uses space to as great a military utility as the United States. Therefore, any other country benefits in a risk/reward calculus about the trade-offs in conducting space control operations. Consequently, in any conflict, the United States would likely experience (1) attacks on space capabilities (including some that might take out an asset for the duration of the conflict) and (2) use of space assets against us in conducting military opera-

tions. Both of these cases supply the motivation to develop space control capabilities.

Regarding such development, we should give consideration to the fact that we have a range of options available—from reversible-effects capabilities like jammers that can surgically target transponders of interest, to destructive capabilities such as ground- and space-based interceptors that give the commander assurance of mission kill. Obviously the United States enjoys freedom in the terrestrial medium to select a spectrum of weapon effects, controlling collateral damage and limiting destruction to acceptable levels in accordance with the Law of Armed Conflict and rules of engagement in effect. No international or domestic legal restrictions on the conduct of space war exist, with the notable exception of the placement and usage of weapons of mass destruction in orbit, so we should make an effort to embrace the cultural shift of developing and acknowledging space control capabilities. The proposed strategy can be an embarkation point.

Goal two explicitly states that the United States will not fight a purely defensive space control war and will utilize capabilities to inflict a range of effects on the opponent's capabilities. Specifically, it also allows for actions on his space capabilities, providing a realization that foreign space capabilities like imagery satellites or navigation analogues to the Global Positioning System have matured and should be considered viable targets. The adversary hopes to negate US surprise operations or the extension of weapon system capabilities beyond the immediate theatre of conflict; the United States should be prepared to eliminate that advantage.

The "Three Enactions": Enabling a Coherent Acquisition and Planning Capability

Every strategy needs ways, means, and ends. The "three enactions" included in the proposed strategy offer the means to attain the two goals mentioned previously. Both provide guidance without being

overly prescriptive of the range of options the United States should pursue in the cultivation of space control capability—linked to a desired end-state effect. These are neither individually new nor groundbreaking concepts, but if they are linked in a strategic context, this proposal would add clarity of thought to one aspect of the space superiority discussion.

Enaction One: Controlling the Electromagnetic Spectrum

Information dominance is a central tenet of the United States' advantage in warfare. The EM spectrum (for this purpose, the EM spectrum is usable radio frequencies and other frequencies used for transmission of data, such as laser communication) is the means by which we and our adversaries attempt to transmit information and command forces. Control of this spectrum in the battlespace is crucial. At the simplest level, denying communication between the ground operator and satellite (and vice versa) essentially eliminates any capability that the satellite provides to the user community on Earth, thus preventing an adversary's use of his space assets. Opponents with less-developed terrestrial communication infrastructures have in many cases turned to relatively inexpensive and easy ways to initiate satellite communication services to supply wide-area propaganda dissemination as well as, in limited instances, military or national-level command and control. Satellite navigation services are enabled by the use of EM signals transmitted between terrestrial users and space assets. The evolution of small satellite technology and the miniaturization of RF components have made readily available space-based radar ISR assets a reality for potential enemies. All of these factors make it blindingly obvious why the United States would want to control the EM spectrum in conflict. Additionally, since the United States is almost always "playing an away game," the remote connectivity offered by space services is crucial in maintaining beyond-line-of-sight connectivity—hence the desire not simply to blanket an area with complete EM silence. Instead the United States should attain use of the EM spectrum on our terms,

having control over what the adversary uses the EM spectrum for and when he uses it.

This enaction is listed first since it also provides what is likely the most mature technology, most cost-effective solution (since many of the options here are ground-based solutions), greatest ability to scale-up production, and ability to impose a wider range of effects than those of some other capabilities. Furthermore, EM spectrum effects usually do not cause direct loss of life or property and can be executed so that they are reversible—typical goals when one conducts terrestrial warfare operations. Also, *complete* control of the EM spectrum would essentially deny the adversary command and control of *any* other space or counterspace capability unless it were completely independent of terrestrial command infrastructures.

Even then, complete control of the EM spectrum in the broadest definition could include some options to defeat autonomous systems such as cyber-enabled command intrusion against the adversary's weapon system or RF weapons. The language chosen would allow the consideration of cyber capabilities within the context of this strategy since the EM spectrum is the medium in which cyber actions are conducted.

Enaction Two: Crossing the Threshold into "Space Weapons"

We have to realize, though, that at some point in a future conflict, as much as we desire to control the EM spectrum, the United States might have an opportunity to take action and defeat an adversary's capability that threatens our use of space. This could come in the form of active defense technologies against an incoming direct-ascent interceptor, the use of directed-energy weapons against an enemy's space-based ISR sensors, or even satellite-on-satellite engagements. The United States must plan for this eventuality and become proficient not only in proposing these types of weapon systems but also in employing them. This is the most controversial piece of the strategy since we would be advocating the development and fielding of capabilities deemed by many policy analysts the most provocative. Much as evolu-

tions in acceptable behavior of warfare allowed for Minutemen firing on Redcoats from protected perches, the United States must not self-constrain the development of space control capabilities or risk falling unacceptably behind technology fronts that our potential adversaries are developing so that we are seen as acting "gentlemanly" in international circles. Winning the fight is paramount.

Acting as early in the Red kill chain as possible maintains the maximum options for courses of action available to a commander and increases the reaction time available to Blue forces. For that reason, we should give preference to those options stated in the proposed strategy. We should consider both kinetic and nonkinetic options since at times the commander may need the assurance of kill presented by a kinetic attack (debris or policy considerations aside). We would also impose costs on Red countermeasure design by forcing the opponent to account for our full continuum of options. Nonkinetic options at times present the advantages of hiding attribution or sowing seeds of doubt as to the cause of system failure, but they should not be considered a silver bullet. Typically, nonkinetic options require a higher level of fidelity of intelligence on the target (increasing the cost and risk of success by placing greater reliance on intelligence information), and the battle damage effects may be more difficult to discern after the engagement. This is especially true in the space medium, where the distance from Earth to space and the nature of orbits present a substantial challenge to maintaining adequate situational awareness. Thus in some sense, compared to nonkinetic options, kinetic options are "cheaper" when we consider the foundational intelligence workload that has to be applied. However, both have their place in the context of bringing a full continuum of capabilities to a commander's disposal, and both need to be supported within a strategic outlay.

The language in enaction two throws open the aperture to space control developers and planners, allowing them the freedom to consider all potential vectors, regardless of political sensitivity. Again, the objective of this strategy is to supply a context in which space control

capabilities can be developed and employed. If the situation is such that we must consider the employment of space control capabilities, we are likely past the point of trying to manage a crisis and instead should focus on what we need to do to emerge victorious on our conditions in the conflict.

Enaction Three: Someone Has to Control This

Inherent in the fielding of coherent space control capabilities is the need to provide coherent command and control for them. Enaction three specifically calls for development of a unified C4ISR structure that permits the success of space control operations. This includes in explicit language the development of an SSA architecture to support space control as well. Doing so has the effect of broadening one's understanding of the SSA mission from "traffic cop of space" or "where, who, and what is in space" to an end state where commanders considering multiple courses of action have a sensor architecture *and* a tasking, collection, processing, exploitation, and dissemination concept of operations in place to support target-folder-level decision making. Just as air-to-air superiority doesn't involve only the F-22 airframe, neither does space control involve only the weapon system. A supporting infrastructure needs to be in place and exercised to go all the way from indications and warning of a space or counterspace event counter to our interests through the execution and analysis of the space control option we conducted. This enaction makes it clear that these issues must be addressed at the same level of importance as the engineering and development of the actual weapon system. A deterrent posture is most effective when you demonstrate that you can operate the weapon system.

Conclusion

The strategy proposal laid out here provides a concise statement of US goals and means to produce an end state in which the United States

is prepared and willing to engage in space control activities in support of our national interests. It obliterates the line between defensive and offensive space control for the most part since in the greater context, our potential adversaries will rarely make that distinction. Moreover, it removes the strategy of space control from the greater umbrella of space superiority to reduce ambiguity in this crucial area. In clear terms, the strategy allows for the investigation and fielding of a full continuum of space control options by the United States. It declares that we prefer a stable order whereby deterrence rules the day and keeps space a global commons. However, it also clearly indicates that the United States will not settle for a situation in which we are only defending against a siege of our space capabilities and will not be held captive by unspoken international taboos. Although the individual concepts in this strategy are not new and many have been presented in other forums, this article offers this strategy for consideration as an original, organic, and coherent statement of guidance and direction as we traverse the Age of Space Warfare. ✪

Notes

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

2. Marc Kaufman and Dafna Linzer, "China Criticized for Anti-satellite Missile Test," *Washington Post*, 19 January 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/18/AR2007011801029.html.

3. Noah Schactman, "Look Out Above! Russia May Target U.S. Sats with Laser Jet," *Wired*, 13 June 2011, http://www.wired.com/2011/06/is-a-russian-laser-aiming-for-u-s-satellites/; and Brian Weeden, "Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space," *Space Review*, 17 March 2014, http://www.thespacereview.com/article/2473/1.

4. Harry Kazianis, "Lifting the Veil on China's 'Carrier Killer,' " *Diplomat*, 23 October 2013, http://thediplomat.com/2013/10/lifting-the-veil-on-chinas-carrier-killer/.

5. Jean-Michel Stoullig, "Rumsfeld Commission Warns against 'Space Pearl Harbor,' " *Space Daily*, 11 January 2001, http://www.spacedaily.com/news/bmdo-01b.html; and SFC Tyrone C. Marshall Jr., USA, "Officials Update Congress on Military Space Policy, Chal-

lenges," US Department of Defense, 12 March 2014, http://www.defense.gov/news/newsarticle.aspx?id=121826.

6. Safa Haeri, "Cuba Blows the Whistle on Iranian Jamming," *Asia Times Online*, 22 August 2003, http://www.atimes.com/atimes/Middle_East/EH22Ak03.html; and "Thuraya Satellite Telecom Says Jammed by Libya," Reuters, 24 February 2011, http://af.reuters.com/article/libyaNews/idAFLDE71N2CU20110224.

7. Col Don Wussler, "Space Superiority Systems Wing" (speech, SMC Industry Days, Los Angeles AFB, CA, 18 April 2007).

8. John J. Klein, *Space Warfare: Strategy, Principles and Policy* (New York: Routledge, 2006); and David E. Lupton, *On Space Warfare: A Space Power Doctrine* (Maxwell AFB, AL: Air University Press, 1988).

9. Wussler, "Space Superiority Systems Wing."

10. Peter Grier, "The Flying Tomato Can," *Air Force Magazine* 92, no. 2 (February 2009): 66–68; and William J. Broad, "What's Next for 'Star Wars'? 'Brilliant Pebbles,' " *New York Times*, 25 April 1989, http://www.nytimes.com/1989/04/25/science/what-s-next-for-star-wars-brilliant-pebbles.html.

11. "Outer Space Treaty of 1967," NASA History Program Office, 26 October 2006, http://history.nasa.gov/1967treaty.html.

12. Lupton, *On Space Warfare*, 6, 21–30.

13. Department of Defense, *Fact Sheet: DoD Space Policy* (Washington, DC: Office of the Secretary of Defense [Policy], October 2012), http://www.defense.gov/home/features/2011/0111_nsss/docs/Fact%20Sheet%20DoD%20Space%20Policy.pdf.

14. Department of Defense, *Fact Sheet: DoD Strategy for Deterrence in Space* (Washington, DC: Office of the Secretary of Defense [Policy], January 2011), http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Strategy%20for%20Deterrence%20in%20Space.pdf

Dr. B. T. Cesul

Dr. Cesul (BSE, MEng, University of Michigan; PhD, Air Force Institute of Technology) is the principal intelligence analyst at the National Air and Space Intelligence Center, Antisatellite (ASAT) Threat Flight. He is responsible for supervising the production of intelligence analysis related to foreign development of ASAT weapon systems and has been a contributing author to multiple national-level studies on space control theory, capabilities, and force structure. Prior to his supervisory role, Dr. Cesul was lead analyst for orbital ASAT weapon systems; foreign intelligence, surveillance, and reconnaissance satellite capabilities; and technology development for small satellites over his 12-year career. At the University of Michigan, he was chief engineer and student program manager for two NASA spaceflight-hardware development programs. Dr. Cesul's dissertation at the Air Force Institute of Technology discussed usage of nonorganic polymers for spaceflight applications.

Let us know what you think! Leave a comment!

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

Space Combat Capability . . . Do We Have It?

Capt Adam P. Jodice, USAF
Lt Col Mark R. Guerber, USAF

Space is a foundational capability for all military operations, yet we don't really plan for anything but success.

—Gen William Shelton
Commander, Air Force Space Command
Atlantic Council, July 2014

When General Welsh took the reins as the USAF chief of staff, he acknowledged the nation's dependence upon the space domain as it relates to our national security. In an interview published in *Strategic Studies Quarterly*, he highlights several asymmetric advantages: "Only the Air Force gives our decision makers the capability and capacity they need for air superiority, nuclear and global strike forces, ISR [intelligence, surveillance, and reconnaissance], rapid global mobility, and command and control operations, all enabled by space and cyber forces. I truly believe that . . . those are the areas where we must continue to focus." He adds, "I believe the air, space, and cyber domains are likely to be those most contested in the future."[1]

It is difficult to ascertain with certainty that the DOD and Air Force are postured for tomorrow's fight in the space domain. A comprehensive, coherent plan to deter adversary action and protect our space assets remains elusive. The 2011 *National Security Space Strategy* states,

"Space capabilities provide the United States and our allies unprecedented advantages in national decision-making, military operations, and homeland security. . . . Space systems allow people and governments around the world to see with clarity, communicate with certainty, navigate with accuracy, and operate with assurance. . . . Maintaining the benefits afforded to the United States by [our operational capabilities in] space is central to our national security."[2] The 2010 *National Security Strategy* asserts that maintaining these benefits means "ensuring the U.S. military continues to have the necessary capabilities across all domains."[3] Are the nation's space assets postured for tomorrow's fight? Does the United States have a comprehensive, coherent plan to deter adversary action and protect our space assets in place or in development? As for many difficult questions, the answer is yes and no. We need to rebalance and invest in space war-fighting expertise and capabilities or risk lengthy/costly conflicts that will undermine US sovereign options and freedom to act on a global stage. This article identifies areas where opportunities for improvement exist and provides recommendations to enhance the nation's unhindered access and utilization of the domain. It provides a brief analysis of the problem along with a recommendation that can be accomplished through increased active space ISR, real-time ISR to the space war fighter, force development, and coordinated command and control (C2). It does not recommend specific acquisition reforms, champion new space policy, or address operational decision criteria.

Context

Over the last several decades, the distance of military operations required near-instantaneous secure communications and ISR as well as precise timing and navigation in support of national security objectives. The demand for these services has multiplied exponentially and is likely to continue. As a nation, we eagerly sought and exploited the inherent advantages space offered. These capabilities now enhance our operational effectiveness in almost every facet and across the

range of military operations. Space operations have improved our ability to find, fix, track, target, engage, and assess (F2T2EA) as well as to maneuver and communicate across all domains on a global scale. The following vignettes illustrate the breadth of these applications and our reliance on space capabilities.

F2T2EA: Ground forces posturing for a capture/kill mission receive battlespace awareness and real-time ISR from space assets and are commanded and controlled through a common special operations center within an area of responsibility (AOR). These space assets provide critical data and intelligence to synchronize the sensor with the shooter.

Maneuver: Naval carrier strike groups around the world rely on space support for ship movement through the use of military-grade Global Positioning System (GPS) signals and ISR assets providing battlespace awareness of possible threats through various choke points. This supports and enables "strategic positioning of capabilities that bring potential airpower to bear within striking distance of potential or actual adversaries."[4]

Communicate: When establishing "no-fly zone" operations, fighter aircraft circle the desert sky performing vital combat air patrol (CAP) missions to defend US personnel, systems, and interests. Meanwhile, an E-3 Airborne Warning and Control System (AWACS) provides airspace awareness of inbound enemy aircraft and relays data throughout the force. At times, many of these aircraft are relying on satellite communications (SATCOM) to ensure message delivery to the war fighter.

In the scenarios above, a recurring pattern emerges: integrated ISR and C2 are vital prior to, during, and postoperations to ensure mission success and assessment. As integration of space capabilities has permeated military operations, the speed, range, and accuracy advantages provided offer a fundamental competitive edge over any adversary.

During Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF), Air Force Space Command (AFSPC) provided extensive space-based support to USCENTCOM through the areas of communications; positioning, navigation, and timing (GPS); meteorology; and warning.

As adversaries have seen our success, they have begun to develop ways to deny and mitigate our clear advantage and increase the costs of military operations that provide these benefits of speed, range, and accuracy. These efforts to undermine our operational advantage must be carefully considered and defeated though active defensive capabilities. To protect space capabilities, AFSPC began developing multiple defensive space control (DSC) systems in the early 2000s.[5] These systems were designed to monitor high-priority SATCOM to detect, characterize, and geolocate interference or jamming. But has our capability to defend our space assets kept pace with the technological developments of our potential adversaries? Recently addressing this topic, Former AFSPC Commander General Shelton pointed out "the growing threats in space, anything from jamming, which is very easy to do, all the way up through laser activity, to kinetic ASAT activity" and that "things are moving much faster than we would like and certainly they had predicted."[6] To this day, the DOD has yet to field a DSC program of record, and it terminated the most current system design—the Rapid Attack Identification, Detection, and Reporting System (RAIDRS) Block 10.[7]

More than a decade later, recent experience in Red Flag exercises and real-world operations make it difficult to affirm with a high degree of confidence that our capability to defend our space assets has kept up with adversarial technologies. Tasking orders have moved from machine-ingestible products to Word documents. Changes to taskings of space assets lack the structure inherent in typical air operations, such as dynamic targeting. Users of space resources and space defenders have no common operational picture, and the community has yet to adopt the brevity common throughout the joint community to standardize communications and improve interoperability.

We have fallen short in developing our ability to find, fix, and finish adversary counterspace. The lack of active ISR and a C2 posture to detect, characterize, and neutralize threats to these assets is alarming. In short, we have been *too slow* to develop an architecture optimized to detect and attribute interference and protect our space assets.

The concepts of continuous, persistent, and active ISR and C2 allow commanders to prepare for and defend against enemy threats at a moment's notice and have become synonymous with decisive, time-sensitive combat operations. While the DOD is well postured in the air, land, and sea domains, space remains ill-equipped to provide continued combat support operations when the domain becomes truly contested.

A "Known" Problem?

Current space ISR and space control operations focus on providing effects and protection to land, maritime, and airborne forces.[8] Using the example discussed earlier, if additional RC-135 and E-8 platforms provide real-time updates on adversaries that pose a threat to friendly forces, then the AWACS can immediately vector appropriate assets to neutralize those threats, the F-15 engages, and the same intelligence platforms assess the results. Though aircraft continue to advance, the reliance on space support and capabilities to F2T2EA does not change. Who performs each of the vital roles for space assets at risk? Where is the purpose-built space architecture to F2T2EA in a dynamic, contested domain? Simply, this architecture does not exist today.

Threats ranging from SATCOM jammers, sensor blinding lasers, and other antisatellite weaponry pose a threat to numerous high-value US assets and their capabilities. In 2012 Gil Klinger, deputy assistant secretary of defense for space and intelligence, remarked, "Every day we have visible signs that the importance of space to U.S. national security and national economic security continues to increase, making space capabilities not only an asymmetric strength and advantage, but also a potential vulnerability."[9] In a 2014 House subcommittee hearing, it was stated that "recent advancements in China's counterspace program, coupled with America's reliance on vulnerable space assets, poses a serious risk to national security."[10] Furthermore, various state and nonstate actors have developed, or are developing, capabilities to counter, attack, and defeat US space systems.[11] The DOD needs to focus

efforts within the space domain in an attempt to achieve and maintain space superiority against emerging threats.

Awareness of the problem is not enough. In 2013 the DOD experienced 200-plus reported SATCOM electromagnetic interference (EMI) events.[12] This number represents only those events conveyed through the proper chain of command and does not account for numerous events that either cleared before reports were generated or went undetected for a large period of time. The posture driven by the gap in current space ISR and C2 forces a reactionary approach to defense, preventing us from proactively mitigating these threats. If we are to compete in a contested space environment, we need solutions that allow space systems to identify, locate, move, block, and neutralize these new threats and a flexible infrastructure that enables rapid communication and reconfiguration.

Recommendations

The DOD and Air Force must invest resources and personnel to enable AFSPC to meet current and future space threats on the following four fronts:

1. Build situational awareness (SA).
2. Exploit what we know (through force enhancement).
3. Defend our capabilities.
4. Attack to defend our national interests (if required).

Increasing proactive ISR in the space domain delivers a more comprehensive and continuous picture, allowing war fighters to digest small changes rather than a flood of new information. Increasing real-time ISR and providing SA to the space war fighter enables predictive posturing executed by properly trained Airmen.

Establishing the proper force-development pipeline of personnel and equipment structures optimizes capabilities and expertise in line with

or ahead of the adversary development cycle. Building upon the current space C2 model to provide active space ISR capabilities for real-time threat reaction and mission defense puts action behind all the awareness, posturing, and expertise developed above.

For this solution to remain viable, there must be a fundamental difference between space asset utility (force enhancement) and combat capability.[13] As stated in the 2011 US *National Military Strategy* (*NMS*), the United States "must grow capabilities to enable operations when a common domain [space] is unusable or inaccessible."[14] In this instance, the *NMS* is referring to the United States' ability to fight through a contested, degraded environment to continue delivering effects in support of commanders and terrestrial forces (i.e., communication and information services). What the *NMS* does not address is the need to actively defend US space assets against threats in the first place, thus avoiding the need to operate in a degraded environment (i.e., combat capability).

The past strategy of focusing space assets solely as support entities to terrestrial forces (as seen in Operation Desert Storm, OIF, and OEF) has left the DOD's defensive space posture narrow in scope and has hindered advancements in active space ISR and coordinated C2. To ensure continuity of operations, future *NMS*s should outline a plan for operating space forces to protect space assets and engage threats (state and nonstate actors). Developing this concept will require a new lens not often considered if space is viewed simply as force enhancement—that of tooth versus tail. Tooth-versus-tail comparisons arise when the military seeks to maximize war-fighting capacity by converting tail (sustainment and force enhancement) to tooth. Adding teeth to the protection of our space forces is a necessary step in moving from force enhancement to combat capability. One inhibitor to this argument is the misinterpretation of outdated international space treaties. While the weaponing of space is prohibited, this does not preclude the United States from taking defensive action against hostile kinetic or nonkinetic attacks. Maj Gen James Armor, former director of the

Defense Department's National Security Space Office, expressed that the "DOD balances the need for improved space situational awareness [SSA] and protection of critical space assets with ensuring that the United States has the ability to deny an adversary access to space capabilities that can be used for hostile purposes contrary to U.S. national interests."[15] In this context, the United States can and should take action within space to ensure continued use and protection of space assets.

Increased Active Space ISR

Air Force ISR has largely been conducted these past 20-plus years in a permissive environment. We must plan for and invest in the future of the Air Force's incredible ISR contributions to our nation's defense. It's critically important that those contributions be possible in all scenarios, to include operations in contested battlespace.

—Gen Mark Welsh, USAF Chief of Staff

Lt Col William Danskine's article "Aggressive ISR in the War on Terrorism" contends that a vital aspect of modern warfare is relentless ISR from every possible avenue and explains that the "United States is searching for a proactive strategy for countering threats before they arrive upon its own shores."[16] In the case of the war on terrorism, the Air Force increased and improved airborne ISR within the AOR. The same concept should be applied to the space domain. According to Air Force core doctrine, tailorable products enable strategic, operational, and tactical effects with a better understanding of the operational environment (systematically, spatially, and temporally)[,] allowing decision-makers and warfighters to better orient themselves to the current and predicted situation and enable decisive action. [17] By this definition, ISR assets should be aggressively focused on providing these capabilities specifically to space operations as they integrate with terrestrial operations. Solely committing ISR to other domains fundamentally overlooks the freedom of action that aggressive ISR provides within the space domain.

To truly understand the space environment, we must increase and improve active space ISR for the purpose of threat indications and warning. The United States' heavy reliance on military and commercial space assets exposes a significant vulnerability for adversary exploitation. Those vulnerabilities can be mitigated; however, any lack of current SSA increases the difficulty of those mitigation actions. As space operations become more congested and contested, it will become more difficult to track foreign and possible threat space systems orbiting the earth. Since the launch of Sputnik 1 in 1954, nearly 4,000 rockets have delivered more than 6,000 payloads into Earth's orbit—some of which have either collided or broken apart to create more clutter in the operational environment.[18] This space debris makes active ISR very difficult and increases the requirement for additional observations, analyses, and communications to ensure mission success. If not tackled head-on, the United States may never have an adequate picture of what space threats exist today or in the future.

A key component of active space ISR is understanding the functions, purpose, and activity of adversary capabilities—both space-based and terrestrial. The DOD must establish a fleet of assets, or repurpose current ISR assets, to provide active space ISR that defensively postures space resources to proactively employ their combat capability. These ISR assets need to perform multiple functions: monitor space activity through radio frequency signal activity; visually identify satellite kinetic and nonkinetic space-based threats; and identify/characterize, track/find, fix, and target terrestrial nonkinetic threats to US military and commercially purchased/leased space assets. This fleet of assets would form the equivalent of ISR CAPs for each orbital regime (low, medium, high, and highly elliptical) and the accompanying infrastructure—a distributed common ground system for space.

Real-Time ISR to the Space War Fighter

Once an active space ISR fleet is established, data generated must be readily available to the space war fighter in a useable form. Air Force

core doctrine states that "as an essential element of all Air Force operations, global integrated ISR linked personnel should be fully aware of mission goals and objectives and be integrated into the operational environment at all levels," disseminating integrated, accurate, relevant, timely, accessible, and secure information."[19] Employing adequate active ISR for space threat indications and warning requires an architecture that meets these six requirements.

Space ISR assets, as configured today, are doctrinally divided into "military, nonmilitary, and national systems."[20] This division of assets has proven to work well in supporting traditional ISR collection for terrestrial threat warning and indications. However, it lacks dedicated capacity, priority, and focus to adequately employ the same systems to deliver integrated, accurate, relevant, timely, accessible, and secure data to those operating space systems.

Current space defensive measures are much more reactive rather than proactive. Consider a "typical" communications interference scenario: the first action taken to resolve interference requires the user to report a problem to a communication center.[21] The communications center troubleshoots or relays to C2, C2 may ask for space assistance through an additional process called joint spectrum interference resolution, and—if the interference remains active—the space system may be able to locate and/or attribute the interference to a user misconfiguration or a hostile actor. The process can take days or longer. While this chain of events may be adequate for responding to unintentional EMI, it in no way actively defends SATCOM against a hostile adversary. At this point, the adversary has accomplished its mission to disrupt or deny communications, and the DOD is unable to take defensive actions to stop that from happening in the first place. Mr. Douglas Loverro, deputy assistant secretary of defense for space policy, conveys that the DOD's space protection needs to consist of "defensive operations to provide warning of and interruption to an adversary's attack."[22] Countering Mr. Loverro's testimony, the 2013 DOD *Electromagnetic Spectrum Strategy*

does not address engaging or defeating a threat but only a need to outperform it.[23]

Unfortunately, once an event has occurred, the effects could be irreversible or, in some cases, the adversary's objective may have been achieved with even a short-duration denial of space capabilities at key times. Further, space operations are different from air, land, or sea platforms from the standpoint that an effect on one space asset may cause effects to multiple assets across different domains. A hypothetical kinetic attack on a military communications satellite could severely impact a national asset by creating a massive debris field within an already highly regulated and congested orbit. Enemy satellite jamming on a military satellite could easily spill over and affect numerous nonmilitary/commercial satellites.

Various space ISR assets exist today—some terrestrial, military-based defensive systems monitoring thousands of SATCOM signals and some space-based national systems. However, no common architecture is in place to provide real-time indications and warning to space system operators. Also lacking is a multiplatform data-link or common operating picture, and interoperability of systems is typically an afterthought upon system acceptance. Within the 16th Space Control Squadron, four separate systems—built to monitor priority SATCOM and to detect, characterize, and geolocate sources of interference—were designed by different contractors to operate on three different networks.[24] This problem compounds when communications and C2 must occur across squadrons, space wings, and joint mission partners. Who's holding the stick on data exposure and interoperability? Who suffers more when a degraded space capability affects ALL other joint war fighters?

To F2T2EA, maneuver, and communicate, our space forces need to know who to target, what to avoid when maneuvering, and how to communicate broadly, quickly, and clearly. Real-time, active ISR provides the starting point from which these branch plans arise.

Force Development

To effectively employ the recommended solution of increasing active ISR for space and providing real-time ISR for space war fighters, the DOD must also invest in building the proper force development pipeline for personnel and equipment to engage in a space-based contested and degraded operational environment. In 2001 the US Space Commission released a report concluding that "the DoD is not yet on course to develop the space cadre the nation needs."[25] While the DOD has come a long way in building a large and well-trained cadre of space operators and leaders, a deficiency of professionals dedicated to the active defense of US space assets remains.

The typical space operators in today's Air Force, Army, Marines, and/or Navy do not have the opportunity to sufficiently master one single space system. Instead, they are often moved to two or three different systems before taking a command/leadership role in one of the systems they previously operated. In some cases, Air Force space operators may take a command/leadership role within a mission area they have never operated. Within other Air Force flying specialties, members of that career field will spend years becoming experts in their weapons system. The Air Force does not place a tanker pilot into a fighter squadron or a remotely piloted aircraft pilot into an airlift unit, so why should it accept anything different within space operations? To effectively man and operate advanced space control, ISR, and C2 forces, AFSPC must develop space professionals capable of engaging adversary space actions while operating in a contested and degraded environment. Fortunately, the Fourteenth Air Force has taken initial steps with a proposal that targets increasing mission area expertise, cultivating manpower through prioritized assignments, and improving recruiting and retention. These efforts, however, are largely focused on platforms and may not sufficiently address development of tactical C2; additional steps are needed to capture service-level support and action.[26]

With a cadre of elite space control, ISR, and C2 war fighters, AFSPC can effectively employ and grow personnel to counter current and future space threats. Various reports and national-level hearings have historically shown that adversary capabilities continue to expand every year, and the United States continues to recognize a need for internal expansion in similar technology to counter those threats.[27] The Air Force and DOD need a process in which AFSPC can rapidly develop and employ space control and ISR systems operated by highly trained tactical operators. The desired end state is a force operating iterations of systems developed to outpace modern threats, with acquisition decisions based after delivered performance rather than on projected performance. These operators must develop effective tactics, techniques, and procedures for this new fleet of interoperable capabilities, creating the force structure that counters threats through real-time ISR, experienced/tactical space C2, and active defensive space systems.

Coordinated C2

The Joint Space Operations Center (JSpOC) commands and controls space assets. C2 of space assets today, along with the JSpOC Mission System (JMS) coming online in the future, centers primarily on spacecraft mission utility, space surveillance, and space control operations. The Air Force should expand the current space C2 model to provide collection of active space ISR capabilities for real-time threat reaction and mission defense. General Shelton touched on this topic in a recent address, saying that "we don't have a way to fuse all this data. We're operating right now on a kind of 1994 software package and a 1980s computer package at the Joint Space Operations Center out at Vandenberg–SPADOC, Space Defense Operations Center."[28] The Joint Functional Component Command for Space (JFCC Space) must be able to expand the operational C2 provided by the JSpOC to fuse ISR and space combat capabilities. Current C2 tools look at the operational control of a single domain (space) without concurrent visualization of space effects

across other domains and the protection of those effects against real-time threats. To defend space assets, ISR across all domains must be integrated through a common C2 node to identify real-time and future space threats and provide tactical C2 to employ space combat capabilities.

The current space C2 model and future JMS are designed to provide C2 of tactical space assets for payload operations and overall satellite health and orbital station keeping. This extremely important mission must remain in place. However, to implement real-time ISR for the space war fighter, a C2 node must intake, discriminate, decide, and disseminate data rapidly. In other words, posturing space assets to F2T2EA as well as maneuver and communicate in a contested and degraded environment requires a faster, more robust architecture to provide tactical C2. Similar to the airborne C2 model—comparable to that of the AWACS—the space domain needs to invest in personnel and resources that feed a common operating picture into a central, agile C2 node and then disseminate threat indications and warnings to tactical units for real-time reaction and protection. This C2 node must develop procedural controls for a mix of terrestrial- and space-based assets that provide high fidelity and shared battlespace awareness. So equipped, space professionals must bring air and joint tactical C2 constructs together to ensure integrated and complementary operations with assets in the other domains. Ultimately, tactical C2 needs to tell a space platform where to maneuver, how to distinguish between friendly forces and adversaries (i.e., deconflict orbits and then access satellite payload data), how the threat will not find the relocated space asset or be aware of the maneuver, and how the asset will reconstitute operations once in place. Enabling space combat capabilities to F2T2EA, maneuver, and communicate ensures remaining space assets survive to enable successful operations in the other war-fighting domains.

Conclusion

Space operations are more integrated today into combat operations than ever before, but that integration falls short when it comes to pro-

tecting critical space capabilities. The former AFSPC commander, General Shelton, recently commented that "space has really become a utility. You plug in, take it for granted, and don't even think about where the services came from."[29] Overlooking the source of these capabilities or how to properly protect them proves a fundamental flaw with the DOD's position. Any lapse in US capacity to ensure unhindered freedom to F2T2EA, maneuver, and communicate threatens the loss of the same air, land, and maritime capabilities. We must be aware of adversary actions to neutralize our competitive edge and use this awareness to posture our space assets. Then our cadre of professional space operators supported by a robust architecture will be fully capable of accomplishing the space mission with a more integrated battlespace consciousness than ever before. If we cannot achieve these goals, as noted by the 2014 SATCOM EMI Working Group, "with what we have today, we must be prepared to lose any serious conflict in the future."[30] ✪

Notes

1. "An Interview with Gen Mark A. Welsh III, Twentieth USAF Chief of Staff," *Strategic Studies Quarterly* 6, no. 4 (Winter 2012): 3, 7.
2. Secretary of Defense and Director of National Intelligence, *National Security Space Strategy: Unclassified Summary* (Washington, DC: DOD, Office of the Director of National Intelligence, January 2011), i.
3. Office of the President, *National Security Strategy* (Washington, DC: White House, May 2010), 22.
4. LeMay Center for Doctrine, vol. 1, Basic Doctrine, chap. 4, "Principles of War," 53, updated 14 October 2011, https://doctrine.af.mil/download.jsp?filename=Volume-1-Basic-Doctrine.pdf.
5. Office of the Chief of Staff of the Air Force, *Air Force Handbook: 109th Congress* (Washington, DC: Dept. of the Air Force, 2009), 38.
6. Gen William Shelton, "The Value of Space to the Warfighter" (address, Air Force Association, Mitchell Institute Friday Space Group Forum, Washington, DC, After 7 February 2014): Note: General Shelton retired from the US Air Force 1 September 2014.
7. AFPEO/SP (Air Force Program Executive Officer for Space) to SMC/SY (Space Superiority Systems Directorate), memorandum, subject: Terminal Acquisition Decision Memorandum (T-ADM) for the Rapid Attack Identification, Detection, and Reporting System (RAIDRS) Block 10 (RB-10) Program, 10 June 2014.
8. AFDD 3-14, *Space Operations*, 1.
9. "Statement of Mr. Gil I. Klinger, Deputy Assistant Secretary of Defense for Space and Intelligence, Before the House Committee on Armed Services Subcommittee on Strategic Forces," 8 March 2012, 2.

10. James Drew, "House Subcommittee Hears of Chinese Threats to U.S. Space Assets," *InsideDefense.com NewsStand*, Inside the Pentagon's Inside the Air Force, 31 January 2014.

11. "U.S. Faces Military Threat to Its Space Assets from Nations, Terrorists," *Space and Missile Defense Report* 7, no. 48 (18 December 2006): 1.

12. JFCC Space SATCOM EMI Working Group Conference, "Summary of Findings: Issues / Unanswered Questions / Recommendations" (Vandenberg AFB, CA, 17–21 March 2014).

13. For purposes of this argument, *space asset utility* refers to space-based capabilities provided to commanders and terrestrial forces, while *combat capability* refers to AFSPC's ability to actively engage in space-based defensive and offensive operations to preserve US freedom of action in space.

14. Michael G. Mullen, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership (*Washington, DC: Joint Chiefs of Staff, 2011), 9.

15. Michael Bruno, "Administration Reaffirms Space Treaty Opposition," *Aerospace Daily and Defense Report* 222, no. 40 (25 May 2007): 1, http://aviationweek.com/awin/administration-reaffirms-space-treaty-opposition.

16. Lt Col William B. Danskine, USAF, "Aggressive ISR in the War on Terrorism: Breaking the Cold War Paradigm," *Air and Space Power Journal* 19, no. 2 (Summer 2005): 73.

17. LeMay Center for Doctrine, annex 2, "Global Integrated Intelligence, Surveillance and Reconnaissance Operations," updated 6 January 2012, 8, https://doctrine.af.mil/download.jsp?filename=2-0-Annex-GLOBAL-INTEGRATED-ISR.pdf.

18. Shenyan Chen, "The Space Debris Problem," *Asian Perspective* 35, no. 4 (December 2011): 538.

19. LeMay Center for Doctrine, annex 2, "Global Integrated Intelligence," 8.

20. Ibid., 60.

21. Chairman of the Joint Chiefs of Staff Manual 3320.02D, *Joint Spectrum Interference Resolution (JSIR) Procedures*, Enclosures A, F, and H, 3 June 2013.

22. *Fiscal Year 2015 National Defense Authorization Budget Request for National Security Space Activities, U.S. House of Representatives*, *Committee on Armed Services, Subcommittee on Strategic Forces*, 113th Cong., 2d sess. (3 April 2014) (statement of Mr. Douglas Loverro, Deputy Assistant Secretary of Defense for Space Policy).

23. DOD, *Electromagnetic Spectrum Strategy 2013: A Call to Action* (Washington, DC: DOD Chief Information Officer, 2013), 5.

24. Briefing, Col Don Wussler, Space Superiority Systems Wing, subject: Transforming Military Space, 30 November 2006, 12. http://www.californiaspaceauthority.org/images/pdfs/061130-0830-Wussler.pdf.

25. Col Cal Hutto, USAF, "Developing Space Professionals," *Air and Space Power Journal* 18, no. 2 (Summer 2004): 28.

26. Mark R. Guerber and David N. Miller Jr., "An Operational Assessment of Air Force Space Control Force Management and Recommendations for Policy, Governance and Organization," white paper, 2014.

27. William B. Scott, "Space Chief Warns of Threats to U.S. Commercial Satellite," *Aviation Week and Space Technology* 150, no. 13 (29 March 1999): 51.

28. Shelton, "Value of Space to the Warfighter."

29. Sydney J. Freedberg, "US Can't 'Stick Our Heads in the Sand' on Space Threats: Gen. Shelton," *Breaking Defense*, 22 July 2014, http://breakingdefense.com/2014/07/us-cant-stick-our-heads-in-the-sand-over-rising-threats-to-space-gen-shelton.

30. JFCC Space SATCOM EMI Working Group Conference, "Summary of Findings."

Capt Adam P. Jodice, USAF

Captain Jodice (MS, American Military University) is the flight commander, weapons and tactics, at the 16th Space Control Squadron, Peterson AFB, Colorado. He is responsible for weapon systems enhancement of defensive space control (DSC) and space situational awareness capabilities. Additionally, he is responsible for developing and documenting system tactics, techniques, and procedures, as well as the integration of DSC and electronic support effects in support of combatant commanders' objectives. He served as a missile warning and space-surveillance crew commander at the 12th Space Warning Squadron, deputy flight commander of the 21st Operations Support Squadron Weapons and Tactics Flight, and the defensive space control officer on the United States Central Command's director of space forces staff. Captain Jodice is a distinguished graduate of the United States Air Force Weapons School.

Lt Col Mark R. Guerber, USAF

Lieutenant Colonel Guerber (MS, Illinois Institute of Technology; MMOAS, Air University) is commander, 16th Space Control Squadron. He is responsible for delivering defensive space control and space situational awareness capabilities, as appropriate, to rapidly achieve flexible and versatile effects in support of global and theater campaigns. He served in the Combined Air Operations Center during Operations Iraqi Freedom and Enduring Freedom. Additionally, he has commanded an expeditionary space control squadron in United States Central Command. Lieutenant Colonel Guerber is a former director of operations for the 76th Space Control Squadron, a graduate of the United States Air Force Weapons School and Air Command and Staff College, and a former instructor at the 328th Weapons Squadron.

Let us know what you think! Leave a comment!

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

We encourage you to e-mail your comments to us at aspj@maxwell.af.mil. We reserve the right to edit your remarks.

HAVE ADVERSARY MISSILES BECOME A REVOLUTION IN MILITARY AFFAIRS?

My compliments to Mr. William F. Bell on his excellent article "Have Adversary Missiles Become a Revolution in Military Affairs?" (September–October 2014). He has certainly captured most of the challenges faced by our integrated air and missile defense (IAMD) forces as ballistic and cruise missiles proliferate across boundaries, grow in numbers, and rapidly improve in capability. The concept of a single-theater missile fight is essentially obsolete—the increasing range of ballistic and even cruise missiles easily crosses artificial borders between combatant commands (COCOM), giving nearly any fight the potential to cause multitheater problems, including homeland defense, essentially turning "away games" into undesirable "home games."

Mr. Bell hit the nail on the head by naming affordability the first requirement of any IAMD system of systems. We can simply no longer afford to rely on what Adm James Winnefeld, vice-chairman of the Joint Chiefs of Staff, terms "Golden BBs"—the highly complex, very expensive sensor and interceptor systems used to knock down simple, inexpensive missiles and rockets fielded by adversaries. In fact, most of Mr. Bell's points fall right in line with those made by Gen Martin Dempsey, chairman of the Joint Chiefs of Staff (CJCS), in his December 2013 *Joint Integrated Air and Missile Defense: Vision 2020*. In that document, the chairman names six imperatives required for success in the future of IAMD: (1) "Incorporate, fuse, exploit, and leverage every bit of information available regardless of source or classification, and distribute it as needed to U.S. Forces and selected partners"; (2) "Make interdependent Joint and Combined force employment the baseline";

(3) "Target development, modernization, fielding, and science and technology efforts to meet specific gaps in IAMD capabilities, all the while stressing affordability and interoperability"; (4) "Focus Passive Defense efforts on addressing potential capability and capacity shortfalls in air and missile defense"; (5) "Establish and pursue policies to leverage partner contributions"; and (6) "Create an awareness of the IAMD mission and the benefits of its proper utilization across the Department of Defense." (Joint Chiefs of Staff, *Joint Integrated Air and Missile Defense: Vision 2020* [Washington, DC: Joint Chiefs of Staff, 5 December 2013], 4–5, http://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf.)

The one—in fact, the only—area where I must take issue with Mr. Bell is his conclusion, wherein he states that "perhaps the [Missile Defense Agency's (MDA)] responsibilities should be expanded to avoid creating unnecessary gaps in our defenses" (p. 63). MDA is an organization purpose-built as a materiel developer, neither intended nor equipped for involvement in strategy, doctrine, operations, or the like. I have a great relationship with MDA leadership and tremendous respect for everything the agency has accomplished so well, but the task Mr. Bell describes simply isn't its job.

I contend that the action agency for this purpose already exists—the Joint Integrated Air and Missile Defense Organization (JIAMDO) on the Joint Staff J-8. We at JIAMDO are at the forefront of cross-service integration and multi-COCOM coordination for all facets of IAMD, including ballistic missile defense; cruise missile defense; counter–unmanned aerial systems; and even counter-rockets, artillery, and mortars. Not only are we the prime implementing agency for instantiating the CJCS *Joint Integrated Air and Missile Defense: Vision 2020*, we have recently rewritten the IAMD Roadmap for 2020–2030 and expect the CJCS's signature on it in the near future. JIAMDO works closely with the COCOMs as they develop their integrated priority lists, using them to inform the chairman's Capability Gap Analysis for IAMD and monitoring service IAMD budgets for execution. We are also closely aligned with service and MDA research, development, and acquisition arms, and work to ensure compliance with interoperability requirements of the IAMD operational architecture that we developed. Moreover, we advocate IAMD issues with Congress, the State Department, and the National Security

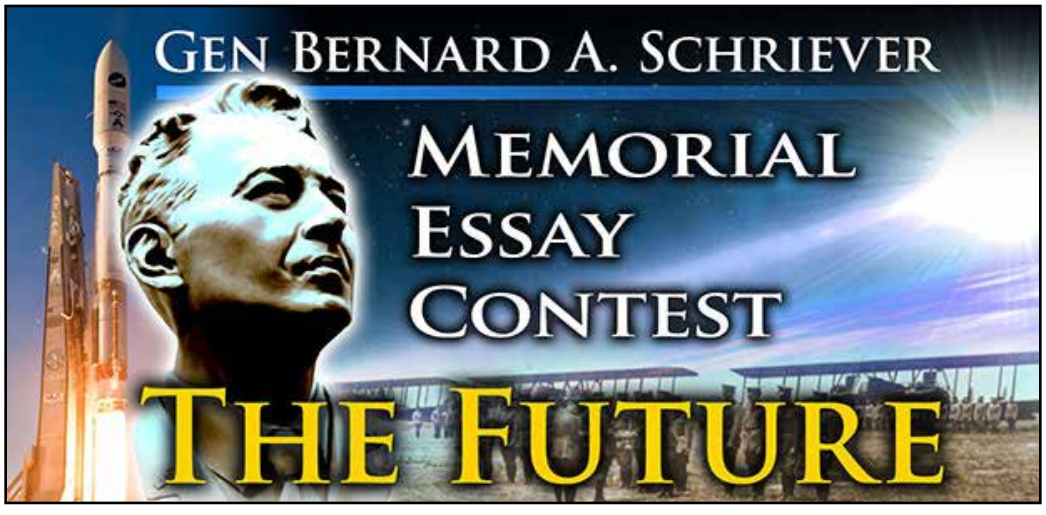
Staff. And we do it all dispassionately as unbiased, honest brokers and representatives of the CJCS, with a joint pedigree and direct access to senior leadership throughout the department.

However, JIAMDO isn't just about requirements, budgets, and acquisition. We run the world's only live-fly, live-fire counter–unmanned aerial systems technology demonstration and exercise annually at Black Dart. Additionally, we put on an operator-in-the-loop, future-epoch simulation for COCOM-based, campaign-level IAMD war games, the results of which inform the highest departmental leadership. JIAMDO is lead agent for rewriting Joint Publication 3-01, *Countering Air and Missile Threats*, 23 March 2012, and we are leading the charge to integrate cyber into IAMD and vice versa. Clearly, JIAMDO is deeply involved in every facet of IAMD, from doctrine to requirements to budgets to exercises to operations, and we do it on a worldwide basis through our experienced network of COCOM liaison officers and subject-matter experts. Anyone can contribute—join our JIAMDO Group on LinkedIn, and start contributing to the unclassified discussion.

Yes, Mr. Bell is quite right. We need a single organization that can coordinate across boundaries to make things happen in integrated air and missile defense, kinetic and nonkinetic, left and right of launch. There has never been a greater need for exactly that kind of central linchpin to the IAMD community, and the demand and workload are steadily increasing while the budgets dwindle.

But look no further—we are already here: JIAMDO.

JESSE A. WILSON JR.
Rear Admiral, USN
Director for Joint Integrated Air and Missile Defense Organization, J-8



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

First Place: Lt Col Joseph Iungerman

"What Happens If They Say No?: Preserving Access to Critical Commercial Space Capabilities during Future Crises"

Second Place: Lt Col Kris Barcomb

"Space Sustainment: A New Approach for America in Space"

Third Place: Capt Bryan Bell and 2d Lt Even Rogers

"Space Resilience and the Contested, Degraded, and Operationally Limited Environment: The Gaps in Tactical Space Operations"

Honorable Mention

1st Lt Gregory Eslinger, "Air Force Space Command and the OODA Loop"
Capt John H. Paek, "Strategic Space Training"
Capt Domenic Magazu III, "Bridging the Gap: Cyber Situational Awareness to the End User"

In addition to trophies, the winning essay received $1,000; second place, $750; and third place, $500.

What Happens If They Say No?

Preserving Access to Critical Commercial Space Capabilities during Future Crises

Lt Col Joseph Iungerman, USAF

In 2011 the *National Security Space Strategy* proclaimed that space was a "congested, competitive, and contested" domain. Since then, national security space professionals have paid considerable attention to the congested and contested aspects of the space domain. Alarmingly, despite the United States' dependence on commercial space capabilities for national security requirements, there has been little examination of the ways adversaries might influence commercial markets to obtain military advantages. Specifically, what would happen if US adversaries made the space and cyberspace business risks too great? Although some might find that concept outlandish, it is a plausible threat that warrants consideration. If the US government fails to prepare for such contingencies, the White House could lose decision and command and control (DC2) capability if worried vendors say no to the nation that needs them.

Why Would They Say No?

It is a simple business truth—the commercial space operators who augment US national space capabilities do so to generate revenues and other business opportunities that are "good for business." National security space professionals ignore this and assume that commercial

space operators will always be willing to offer their capabilities to Washington despite significant space and cyberspace risks. Instead, they mistakenly assume that commercial space operators universally view the loss of government service purchases as "bad for business" and they will tolerate great risks to avoid those losses. Although that was true previously, emerging market trends are diminishing that once considerable cachet. Space companies can tolerate losses of government business far better than they could ten years ago.

Currently, the US government relies on commercial augmentation for at least 40 percent of its military DC2 requirements. These include such operational staples as high-resolution satellite imagery, unmanned aerial systems (UAS), and Blue Force Tracking (BFT). However, Washington's purchases generate less revenue than demand from the energy (natural gas and oil), land management (forestry and mining), and commercial communications (television, radio, and broadband) sectors.[1] Respectively, those sectors represent greater potential for business growth than sales to the US government—especially when one considers the dilemmas posed by shrinking government budgets over the next decade. In the commercial satellite communications sector alone, some estimates project opportunities for five to 15 percent growth while government purchases of similar services only represent opportunities for a maximum of five percent growth.[2] In many cases, it is no exaggeration that a number of commercial space operators need Washington less than it needs them.

Adversaries can exploit that disparity of need to limit America's access to commercial space capabilities by holding revenues and growth opportunities at risk during crises. Many adversaries can launch missiles, operate lasers, create jamming, or wage cyber attacks that can make the cost of doing business with the US government too high with relative ease.

What Threats Could Influence Them to Say No?

As previously stated, adversaries opposed to US interests can bring an impressive array of threats to bear against commercial space operators to make it too risky for them to do business with the US government during a crisis. For example, DigitalGlobe and Astrium Geo-Information Services provide imagery to the US government using remote sensing platforms in low Earth orbit (LEO). Those assets are vulnerable to direct-ascent antisatellite (DA ASAT) missiles like the SC-19 that China used to destroy its FY-1C satellite- and ground-based lasers that illuminated US reconnaissance satellites.[3] For companies like DigitalGlobe, operating satellites costing $300 million in LEO without protective capabilities, destruction of a satellite, or damage to an imaging sensor could jeopardize revenues they depend on for survival.[4] Faced with such threats to expensive revenue-generating assets, companies might "turn off," reorient imaging sensors during passes over certain areas, or curtail business with the US government.

Satellites in geosynchronous Earth orbit (GEO) or stationary orbits that support UASs and BFT are safe from ground-based DA ASATs and lasers but remain vulnerable to radio frequency interference (RFI), which is easy to cause. In some cases, a hostile actor only needs to own an authorized equipment suite like the kind sold by Hughes or Intelsat and operate it in an improper configuration to overpower uplink signals on a satellite.[5] An adversary might also opt to keep a satellite signal from reaching a user on the ground by operating downlink jammers from companies like C.T.S. Technology and Aviaconversiya Ltd.[6] Although the commercial satellite industry has means to deal with uplink interference, it can do little to protect paying customers from downlink jamming. Knowing these things, an adversary could potentially cause RFI against transmissions from satellites carrying US government users such that the interference disrupted other paying customers using the same spacecraft. If a commercial operator were unable to mitigate RFI, clients might take their business to competitors and a commercial operator might choose to drop US government traffic.

Adversaries can also use a variety of cyberspace capabilities to influence commercial space operators during crises. For example, Internet denial of service attacks can prevent companies from communicating with their clients. Adversaries can also deploy malware to disable satellite command and control infrastructure and route terrestrial communications, or they can opt for complex command intrusions to reconfigure satellite subsystems in space.[7] At the same time, adversaries can execute industrial espionage to expose sensitive client data, compromise intellectual property, and reveal business plans from commercial space operators' computer networks. Such actions could cause stock devaluations, a loss of business, and undermine competitive advantages.[8] Many of those actions have already occurred. Cyber miscreants have attempted command intrusions against the US Geological Survey's Landsat-7 and NASA's Terra satellites and absconded with sensitive satellite design data from US space companies.[9] In the future, those trends will likely continue in volume and severity.

Why Would an Adversary Want to Make Them Say No?

It makes strategic sense for adversaries to target commercial space operators supporting Washington during future crises. Inviting swift retaliation with a "space Pearl Harbor" against America does not make asymmetrical sense. Cutting off the United States from commercial space augmentation in a gradual fashion could allow adversaries to slow down the red, white, and blue juggernaut.[10] Adversaries with enough patience could use the same methods to achieve larger strategic goals and avoid serious confrontations with the United States altogether.

For example, keeping commercial assets in LEO from imaging events in areas like the Ukraine and Sudan can limit the ability to justify sanctions or military actions against aggressors. As the Pentagon and Foggy Bottom struggle, hostile forces can take advantage of those delays to force native people off their lands, seize mineral wealth, and solidify territorial claims.[11] Meanwhile, interfering with commercial assets in GEO that support UASs would allow adversaries to limit a com-

batant commander's (CCDR) situational awareness in key areas like the East China Sea or the Straits of Hormuz.[12] If the United States did manage to observe aggressive acts, adversary interference could disrupt BFT and undermine large-scale distributed logistics needed to muster a response force to counter adversary moves.[13]

The most attractive aspect of disrupting commercial space support of the United States for an adversary during a crisis is an opportunity to degrade Washington's DC2 advantages without creating casus belli.[14] The United States is not required to retaliate for laser illumination of a commercial spacecraft that keeps it from sending imagery to an Air Force Eagle Vision platform.[15] Similarly, there is no obligation to respond to adversary-generated RFI against satellite links that support UAS and BFT.

In contrast, commercial space operators have contractual obligations to the customers paying premium rates for satellite services and to the investors who derive benefit from the value of those sales. Interference targeted against commercial space operators for doing business with Washington represents serious threats to company revenues. If the US government does not understand this or is unwilling to respond to such interference, commercial space operators might not have any recourse but to restrict or terminate their business with Washington in order to protect themselves.

Are There Precedents for Saying No?

Companies like Eutelsat, Intelsat, and Nilesat have dropped state-sponsored content from Russia, Iran, and Syria. They responded to world tensions caused by Moscow's forays into Georgia, Tehran's nuclear program, and the Arab Spring abuses in Damascus.[16] Those actions show that commercial satellite operators are willing to deny services to governments in the interest of preserving business with other clients. However, it is hard to consider those examples as precedents for the issues at the heart of this paper. None of those companies refused their

services to a government because they feared an adversary would target their businesses.

While the commercial space industry currently offers no historical precedent for those types of concerns, another industry does. For years, commercial augmentation has been essential to the United States' strategic force projection capability—particularly regarding long-range airlift. As with commercial space, the United States relies on the commercial sector for 37 percent of the long-haul airlift for rapid force projection capability, responses to crises, and delivery of aid to foreign partners. During the twilight of the Nixon administration, the situation was very much the same, but the White House's access to those capabilities suffered in the face of world tensions.[17]

In October 1973, Soviet-backed Arab forces attacked Israel across the Golan Heights and the Sinai Peninsula during what became known as the Yom Kippur War. As Israeli forces suffered terrible losses, Arab forces closed in and pushed the Jewish state to the edge of defeat.[18] Golda Meir's government called for resupply to their forces, and President Nixon expected to do so with a commercial airlift. Commercial flights would not disrupt the withdrawal of US forces from Southeast Asia or exacerbate tensions with the Soviets or oil-producing Arab states.[19]

To Washington's chagrin, American companies refused to place their planes, personnel, and profits at risk when the White House and Pentagon called on them. Companies feared that Arab states would drive up fuel prices, cut them off from transit routes, and contribute to increased air piracy that would undermine their bottom lines.[20]

As a result, Pentagon planners had to reallocate strategic airlift forces from the drawdown in Southeast Asia to support the Operation Nickel Grass (ONG) resupply of Israeli forces. Arab forces used the delay to inflict heavy losses on Israeli forces and secure territorial gains. Washington had no way to provide desperately needed aid to a key ally during a crisis because it had no plan to help the commercial sector offset risks associated with helping the White House during a crisis.

The basic lesson from ONG should speak loudly to national security space professionals. Despite Washington's cachet as a customer, American companies have refused to help when adversaries threatened business operations. It is simply a matter of time before the threat of adversary interference drives commercial space operators to do what their air cargo cousins did in 1973.

What Can We Do to Keep Them from Saying No?

Air Force Space Command (AFSPC) has an array of capabilities that could help commercial space operators overcome interference by an adversary.[21] However, it will be necessary to do more than ad hoc taskings of AFSPC units to deal with interference or to nominate important signals and networks for placement on a CCDR's defended asset list. In the future, the command will need to change how it interacts with commercial space operators fundamentally.

First, AFSPC needs to develop space and cyber professionals with a broader range of expertise than recent science, technology, engineering, and mathematics (STEM) recruitment efforts produce. In the future, it will not be enough to have a space and cyberspace workforce that understands the technical intricacies of space systems and their associated ground networks but knows little about the business operations behind them. AFSPC should consider adopting a "STEM-B" recruiting strategy that brings personnel with technically oriented business degrees into the space and cyber workforce. Further, once the command recruits those personnel, it needs to do a better job of tracking and utilizing them in the selection process for advanced academic degree programs.

To that end, AFSPC should create a commander's industrial research initiative (CIRI) to spur research into critical business matters that affect space. Shrinking headquarters staffs do not and will not have time or resources for that research. Under a CIRI, AFSPC could competitively select space and cyberspace personnel for attending the Air

Force Institute of Technology, National Intelligence University, Air Command and Staff College, and Air War College. These people should work on space industrial research topics and then go to follow-on assignments to AFSPC, Fourteenth Air Force, or Twenty-Fourth Air Force headquarters to put their research to practical use. To keep those officers' skills honed, the final element of CIRI would be a short-duration internship during the follow-on assignment to deepen their understanding of market forces and technical issues.[22]

AFSPC also needs to work with US Strategic Command (USSTRATCOM) for inclusion of threats to commercial space in the latter's 8000-series contingency plans.[23] Currently, it is not clear how much of those plans are applicable to commercial space operators or to the capabilities AFSPC and USSTRATCOM can use to protect them from targeted interference. There could be significant challenges under US Code Title 10 and Title 50. These define how AFSPC can use capabilities to protect terrestrial networks used by commercial space operators inside the United States. There could be liability concerns if the Pentagon used space and cyber capabilities to protect a commercial space operator and caused collateral damage in the process. The only way to address those challenges is to begin planning for them now. Failure to do so places the nation at risk of experiencing the same dilemma that occurred during ONG. Without meaningful plans to address threats directed at their business interests, commercial space operators will be no more likely to support the United States during future crises than the commercial air transport industry was in 1973.

With plans developed, they must be tested and evaluated, and AFSPC should work with USTRATCOM to create short-sprint exercises to test planning assumptions, courses of action, and authorities for critical commercial space capabilities. Ideally, such exercises would use industrial relations findings developed during AFSPC's "Schriever Wargames" and the National Reconnaissance Office's (NRO) "Thor's Hammer" war game." Commercial space operators need to be involved.[24]

Currently, industrial partners rarely participate in recurring exercises like Global Lightning and Global Thunder for a variety of security and procedural reasons. The same is also true for the Defense Information Systems Agency, the National Geospatial-Intelligence Agency, and at least five other federal agencies that act as the primary liaisons between the Department of Defense and commercial space vendors.[25] Because of that, personnel at the Joint Space Operations Center and US Cyber Command operations centers do not get the benefit of training with commercial representatives they would call for support during a conflict. Further, the infrequent participation of key federal agencies in recurring exercises means AFSPC and USSTRATCOM rarely get to evaluate how those organizations will fit within a joint interagency coordination group (JIACG) in a crisis. That kind of training needs to start happening as soon as possible. It will be too late to figure out how to preserve commercial augmentation after a crisis begins, and an adversary has already started interfering with commercial space operators.

Finally, AFSPC needs to organize better to facilitate its access to commercial space partners and their respective capabilities, which adversaries will likely target. AFSPC should organize an operations-focused commercial capabilities office (CCO) at the numbered air force level. The CCO would facilitate real-time information sharing, ease requirements updates, disseminate warnings of interference, and coordinate AFSPC and USSTRATCOM plans and responses.[26] Industry partners have asked the Pentagon to set up similar entities.Those efforts faltered for bureaucratic reasons or were diluted because they were formed under the auspices of obscure working groups better suited for policy development than for operations.[27] AFSPC should take the lead to reverse those trends and set up CCOs that can facilitate real-time interactions with commercial space operators and the operations centers and coordinate with intelligence community organizations such as the NRO Operations Center.

Conclusion

In the future, as the United States' dependence on commercial space capabilities increases, adversaries will be inclined to drive a wedge between the White House and the commercial space operators it depends on for DC2. Adversaries will want to make it too risky for commercial space operators to offer capabilities to the United States. If they succeed, the White House and the Pentagon might not be able to take decisive action. National security space professionals that AFSPC recruits and fosters need to reconsider current relationships with commercial space operators and better understand the business interests that drive them. With those space professionals, AFSPC and USSTRATCOM should develop plans to mitigate threats to commercial space partners. In addition, AFSPC must help test those plans and organize space and cyber professionals to support critical commercial space partnerships. Without these efforts, commercial space operators will have little reason to accept the business risks associated with helping the United States during a crisis. ✪

Notes

1. Sandra I. Erwin, "Satellite Shortages May Choke Off Military Drone Expansion," *National Defense*, April 2013, http://www.nationaldefensemagazine.org/archive/2013/April/Pages/SatelliteShortagesMayChokeOffMilitaryDroneExpansion.aspx; G. Ryan Faith and Mariel John, "Space Report 2011" in *Authoritative Guide to Global Space Activity*," ed. Micah Walter-Range (Colorado Springs, CO: Space Foundation, 2011), 14–15, 35–38, 42, 123–25; *2010 Futron Forecast of Global Satellite Services Demand Overview*, (Washington, DC: Futron Corporation, 2010); Satellite Industry Association, *State of the Satellite Industry Report* (Washington, DC: Futron Corporation, 2010 and 2012); and Defense Business Board, *Report to the Secretary of Defense: Taking Advantage of Opportunities for Commercial Satellite Communications Services*, Report FY 13-02 (Washington, DC: Department of Defense, undated). Although some industry estimates indicate the percentage of US government reliance on commercial space capabilities for decision and command and control requirements runs as high as 80 percent, this paper utilizes the lower end of the industry and government estimates for US government reliance on commercial capabilities. Even at the lower end of the estimates in current use, the concept that nearly half of the US government's space support requirements come from commercial sources is a significant planning consideration.

2. *2010 Futron Forecast of Global Satellite Services Demand Overview.*

3. Warren Ferster and Colin Clark, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," *Space News*, 3 October 2006, http://www.spacenews.com/article/nro-confirms-chinese-laser-test-illuminated-us-spacecraft; Shirley Kan, "China's Anti-Satellite Weapon Test," Report RS22652 (Washington, DC: Congressional Research Service, 23 April 2007), http://fas.org/sgp/crs/row/RS22652.pdf; and Air University, *Space Primer*, AU-18 (Maxwell AFB, AL: Air University Press, September 2009), http://aupress.maxwell.af.mil/digital/pdf/book/AU-18.pdf, 276–77.

4. Peter B. de Selding, "DigitalGlobe Awards $307M in Contracts for WorldView-3 Satellite," *Space News*, 31 October 2010, http://www.spacenews.com/article/digitalglobe-awards-307m-contracts-worldview-3-satellite; Associated Press, "Longmont's Digitalglobe Gets Final Tests On Satellite," *CBS Denver*, 13 May 2014, http://denver.cbslocal.com/2014/05/13/longmonts-digitalglobe-getting-final-tests-on-satellite; and J. J. McCoy, "DigitalGlobe Orders WorldView 2 Satellite," *Via Satellite - Integrating SatelliteToday.com*, 3 January 2007, http://www.satellitetoday.com/telecom/2007/01/03/digitalglobe-orders-worldview-2-satellite/.

5. Robert Ames, "Satellite Interference; What It Means for Your Bottom Line," Kratos Integral Systems Service Solutions, Satellite Trends, undated, http://www.integ.com/IS3/whitepapers/SKTelecommNews.pdf; Giovanni Verlini, "New Efforts to Mitigate Satellite Interference," *Via-Satellite - Integrating SatelliteToday.com*, 1 March 2010, http://www.satellitetoday.com/telecom/2010/03/01/new-efforts-to-mitigate-satellite-interference; "World Broadcasting Union Adopts Carrier ID to Combat Satellite Interference," *TVTechnology*, 2 August 2013, http://www.tvtechnology.com/cable-satellite-iptv/0149/world-broadcasting-union-adopts-carrier-id-to-combat-satellite-interference/224999; and Air University, *Space Primer*, 274–77.

6. Jacob Kastrenakes, "FCC Issues Largest Fine in History to Company Selling Signal Jammers," *Verge*, 19 June 2014, http://www.theverge.com/2014/6/19/5824344/fcc-issues-signal-jammer-seller-largest-fine-ever-34-9-million; Bob Bewin, "U.S. Army Awarded Contracts to Russian GPS Jammer Vendor," *ComputerWorld*, 27 March 2003, http://www.computerworld.com/s/article/79783/U.S._Army_awarded_contracts_to_Russian_GPS_jammer_vendor; and Air University, *Space Primer*.

7. Mark Clayton, "Can Military's Satellite Links Be Hacked? Cyber-Security Firm Cites Concerns," *Christian Science Monitor*, 25 April 2014, http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0425/Can-military-s-satellite-links-be-hacked-Cyber-security-firm-cites-concerns; and Debra Werner, "Cover Story: Hacking Cases Draw Attention to Satcom Vulnerabilities," *DefenseNews*, 23 January 2012, http://www.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities.

8. Leon Spencer, "Chinese Army Group Hacks US Satellite Partners: Crowdstrike," ZDNet, 10 June 2014, http://www.zdnet.com/chinese-army-group-hacks-us-satellite-partners-crowdstrike-7000030353.

9. Werner, "Cover Story"; John Walcott, "Chinese Espionage Campaign Targets U.S. Space Technology," *Bloomberg*, 18 April 2012, http://www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html.

10. *Report of the Commission to Assess United States National Security Space Management and Organization [CAUSNSSMO]* (Washington, DC: CAUSNSSMO, 11 January 2001), 25, http://www.dod.gov/pubs/space20010111.html.

11. "Troops in the Demilitarized Zone; Confirmation of Violations by Sudan and South Sudan," Satellite Sentinel Project: Monitoring the Crisis in the Sudans, 2013, http://www.enough project .org/files/Troops-in-the-Demilitarized-Zone.pdf; Scott Neuman, "U.S.: Satellite Images Show Russian Rockets Hitting Ukraine," Two-Way: Breaking News from NPR, 27 July 2014, http://www.npr .org/blogs/thetwo-way/2014/07/27/335829570/u-s-satellite-images-show-russian-rockets-hitting -ukraine; and Tom Withington, "Space Paparazzi," *C4ISR Journal* 10, no. 3 (27 March 2011): 24–26.

12. Craig Whitlock and Anne Gearan, "Agreement Will Allow U.S. To Fly Long-Range Surveillance Drones from Base in Japan," *Washington Post*, 3 October 2013, http://www.washington post.com/world/agreement-will-allow-us-to-fly-long-range-surveillance-drones-from-base-in -japan/2013/10/03/aeba1ccc-2be8-11e3-83fa-b82b8431dc92_story.html; and Robert Johnson, "US Navy and Allies Showed Iran Who Really Controls the Strait of Hormuz," *Business Insider*, 27 September 2012, http://www.businessinsider.com/photos-the-us-navy-protects-the -gulf-2012-9?op=1; and Tony Capaccio, "Strait of Hormuz Attack Iran 'Last Resort,' Author Says," *Bloomberg*, 5 August 2012, http://www.bloomberg.com/news/2012-08-06/strait-of-hormuz -attack-iran-last-resort-author-says.html.

13. *AIT&ITV: Automatic Identification Technology and In-Transit Visibility*, US Transportation Command [USTRANSCOM], undated, http://www.transcom.mil/ait; Erwin, "Satellite Shortages"; Jeffrey Hill, "Blue Force Tracking System Upgrade Seen as Crucial," *Via Satellite - Integrating SatelliteToday.com*, 11 November 2008, http://www.satellitetoday.com/publications /eletters/military/2008/11/11/blue-force-tracking-system-upgrade-seen-as-crucial; Rick Lober, "Why the Military Needs Commercial Satellite Technology," *Defense One*, http://www .defenseone.com/technology/2013/09/why-military-needs-commercial-satellite-technology /70836/; and "Blue Force Tracking 2," *ViaSat.com*, https://www.viasat.com/government -communications/blue-force-tracking.

14. Although a debris-causing attack like a missile launch would likely generate a response based on the worldwide reaction to the Chinese SC-19 intercept of their FY-1C satellite, other publicly acknowledged attempts at interference—like the lasing of US reconnaissance satellites and attempted command intrusions on the Landsat-7 and Terra satellites—hardly evoked any public response from the US government.

15. Robert K. Ackerman, "Special Report—Commercial Eyes on the Battlefield Sharpen Focus," *Signal Online*, March 2001, http://www.afcea.org/content/?q=node/568; and Capt James A. Hartmetz, USAF, "Eagle Vision—Exploiting Commercial Satellite Imagery," *DISAM [Defense Institute of Security Assistance Management] Journal* 23, no. 4 (Summer 2001): 22—25, http://www.disam.dsca.mil/pubs/v.23_4/hartmetz.pdf.

16. "Iran's Press TV Taken Off Air in N America," Al Jazeera, 9 February 2013, http:// www.aljazeera.com/news/middleeast/2013/02/20132913263566603.html; Agence France-Presse, "Intelsat Blocks Iranian Channels in Europe," *RawStory*, 25 October 2012, http:// www.rawstory.com/rs/2012/10/25/intelsat-blocks-iranian-channels-in-europe/?onswipe _redirect=no&oswrr=1; Reuters, "Nilesat Stops Broadcasting Three Syrian Channels," *Egypt Independent*, 9 May 2012, http://www.egyptindependent.com/news/nilesat-stops-broadcasting-three-syrian-channels; and David Smith, "Satellite Saga" *New Atlanticist*, 23 July 2010, http:// www.atlanticcouncil.org/blogs/new-atlanticist/satellite-saga.

17. *USTRANSCOM Annual Command Report* (Scott AFB, IL: USTRANSCOM, 2012), 16, http://www.transcom.mil/documents/annual_reports/annual_report.pdf; *Airlift Operations of the Military Airlift Command During the 1973 Middle East War* (Washington, DC: US Government Accountability Office, 1975), http://www.gao.gov/assets/120/115367.pdf; and Maj

Thomas J. Riney, USAF, "Transforming Past Lessons to Mold the Future: A Case Study on Operation Nickel Grass," Graduate Research Project AFIT/GMO/ENS/03E-11 (Wright-Patterson AFB, OH: Air Force Institute of Technology, June 2003), http://www.dtic.mil/dtic/tr/fulltext/u2/a430910.pdf.

18. Abraham Rabinovich, *Yom Kippur War: Epic Encounter that Transformed the Middle East* (New York: Schocken Books, 2004). 175.

19. Nina Howland, Craig Daigle, and Edward C. Keefer, eds., *Foreign Relations of the United States [FRUS]: 1969–1976*, vol. 25, *Arab-Israeli Crisis and War: 1973* (Washington, DC: Government Printing Office, 2011), http://static.history.state.gov/frus/frus1969-76v25/pdf/frus1969-76v25.pdf; Walter J. Boyne, *The Two O'Clock War: The 1973 Yom Kippur Conflict and the Airlift That Saved Israel*, 1st ed. (New York: Thomas Dunne Books, 2002). 77–8; and Rabinovich, *Yom Kippur War*, 24, 323, 491.

20. Howland, Daigle, and Keefer, *FRUS: 1969–1976*, vol. 25, *Arab-Israeli Crisis and War: 1973*; Boyne, *Two O'clock War*; and Rabinovich, *Yom Kippur War*.

21. 21st Space Wing, "Fact Sheet: 16th Space Control Squadron," http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403; AFSPC, "Fact Sheet: Air Force Cyberspace Defense Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20871; AFSPC, "Fact Sheet: Air Force Cyberspace Defense Analysis Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20873; and AFSPC, "Fact Sheet: Air Force Cyberspace Vulnerability Assessment/Hunter Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20874. This list is not all-inclusive.

22. Due to staffing limitations, high organizational workloads, and cost concerns, internships probably should not last longer than two to three months and should be limited to opportunities with companies that reside in the same geographic area where the officer is assigned.

23. Chairman of the Joint Chiefs of Staff Manual 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*, 18 October 2012, A-5. Personnel developed under a commander's industrial research initiative would be ideally suited for participation in joint planning working groups formed to develop, revise, and test planning assumptions and courses of action to preserve the nation's access to commercial space capabilities during a crisis

24. House, *Statement of Gen Keith B. Alexander, Commander, United States Cyber Command: Hearings before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities*, 112th Cong., 2d sess., 20 March 2012, 17, http://www.au.af.mil/au/awc/awcgate/postures/posture_cybercom_20mar2012.pdf; and Robert S. Dudney, "Hard Lessons at the Schriever Wargame," *Air Force Magazine* 94, no. 2 (February 2011), 88–89, http://www.airforce -magazine.com/MagazineArchive/Documents/2011/February%202011/0211wargame.pdf.

25. This passage considers the Federal Communications Commission, Federal Aviation Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, the National Aeronautics and Space Administration, and the Department of State's various space and arms control offices. As a contingency planner within US Strategic Command's Joint Functional Component Command for Space (JFCC-Space) and as a Headquarters Air Force staffer, the author has considerable firsthand experience with regard to interactions with commercial partners during exercises. The author of this paper also organized the JFCC-Space role in Schriever Wargames IV, V, and X as well as the Unified Engage-

ment Wargames that utilized the space and cyberspace game scenarios from Schriever Wargames V and X. The author also participated in Schriever Wargame XII as a member of the HQ AFSPC staff. Although game scenarios examine a wide variety of concerns, they do not normally explore underlying business concerns that affect the concerns of commercial space operators that augment national US capabilities. To explore such issues in depth, specific focus sessions are required before the main game events transpire.

26. The benefit of placing such an office at the numbered air force level is that each numbered air force has an operations center that commands and controls operations in support of a joint force commander. Placing the office at the staff level instead of within the operations center itself can alleviate many security and proprietary data concerns in the hectic environment of an operations floor and still offer close proximity to personnel commanding and controlling space and cyberspace operations.

27. Werner, "Cover Story."

Lt Col Joseph Iungerman, USAF

Lieutenant Colonel Iungerman (BA, Rider University; MS, National Intelligence University; MBA, Touro University International) is the executive officer for Air Force Space Command's Directorate of Programming and Financial Management. He is a joint-qualified space officer with previous operational experience as a contingency planner with the Joint Functional Component Command for Space, an intelligence analyst at the National Air and Space Intelligence Center, and a missile combat crewman with the 91st Missile Wing.

Space Sustainment

A New Approach for America in Space

Lt Col Kris Barcomb, USAF

Eisenhower was surely right—the American system was not set up for central planning, nor did its values condone it.

—Walter McDougall

Introduction

Promoting commercial development and fostering free-market capitalism are cornerstones of American economic policy. Since its inception, the United States has favored decentralization and privatization as the primary means of generating wealth. These fiscal core values should permeate all aspects of US policy, yet the history of American activity in space seems to indicate otherwise. Accessing and exploiting space involves highly specialized technologies, astronomically high costs, and considerable risk of failure. In the formative years for space, these technological factors coincided with an existential threat to the United States and its allies, emerging from within the Soviet technocracy. The perceived successes of the Soviet Union's centralized approach to advanced research and development cast doubt on the ability of free markets to maintain a competitive edge.[1] This combination of technological complexity and geopolitical pressure drove the

United States to break from its laissez-faire traditions and replace them with an ideology of control that has permeated the fabric of America's attitude toward the ultimate high ground ever since.

This philosophy must change. Fifty years of experience and a dramatically different global political climate have altered the conditions under which the current control-oriented system emerged. Many commercial space companies are on the cusp of fiscal viability or are already sustaining profits.[2] The Cold War ended, and the United States arose as the world's dominant space power. Space technology has improved, and new markets are emerging. Despite these changes, legal barriers in both international and domestic law continue to inhibit economic growth and competition, and the international community lacks a viable mechanism for ensuring order and promoting a rule of law in space.

Given these realities, the United States should extend its commitment to free markets into the space domain by rethinking its space strategy. In this paper, I advocate doing so by adopting a mind-set of *space sustainment* over the current paradigm of *space control*. A space sustainment strategy leverages US strengths to promote and maintain an international order sufficient to preserve a dynamic, functional, and growth-oriented marketplace for space activity. It includes a recommitment to traditional US economic principles and begins by modifying restrictive laws and fostering capitalism. It also acknowledges the need for defending private and public equities in space through all instruments of national power, including exercising legitimate uses of force for maintaining order within the boundaries of the rule of law. Finally, this strategy embraces transparency to enhance predictability for private enterprise and to preserve the credibility of actors within the emerging international legal framework. Adopting this approach will improve the overall security of the United States, promote a healthy economy, and increase access to force support and enhancement capabilities needed for promoting the rule of law. Further, it will enable the United States to maintain

its technological, military, and economic advantages despite a space domain that is increasingly "congested, contested, and competitive."[3]

Reforming Space Law

The current body of both international and domestic space law inhibits private enterprise, making it difficult for Air Force Space Command (AFSPC) and other government agencies to access space capabilities at affordable costs and within reasonable risk limits. Everett Dolman, author of *Astropolitik*, challenges the notion that space should be treated in a communal fashion. He attests, "The core problem in international space law is that the practical effect of collectivizing space has been counter to its intended purpose of encouraging the development of outer space. Indeed, it would seem to have had precisely the opposite effect."[4] Dolman's primary target for reform is the Outer Space Treaty (OST), since so many countries have ratified it, but he also highlights the significant problems with other legal frameworks, such as the Bogota Declaration and the Moon Treaty. Both of the latter agreements promote an idealistic interpretation of space as a purely public domain—a res communes, more in line with communism than capitalism.[5]

Lewis Solomon, a law professor at George Washington University, also aims to counter commercially stifling trends in international law. While he views the verbiage in the OST as uncertain, he sees the Moon Treaty as undeniably prohibitive. He writes, "By precluding private property rights and profits, [the Moon Treaty] negates the impetus for commercial development of the Moon. Simply put, the Moon Treaty is unacceptable to space-faring nations in light of the risks involved in getting to the Moon and extracting its resources."[6] The United States should embrace its traditional economic values and press the international community toward promoting market incentives in international space law. This would open up the competitive space for new entrants, increase the supply of vendors, and ultimately reduce cost and risk.

The restrictions contained in the current body of international law are not the only barriers the United States must overcome to successfully implement a space sustainment strategy. US export controls on dual-use aerospace technology, such as those contained in the International Traffic in Arms Regulations (ITAR), have often backfired "as other countries eagerly pick up the slack created by US market withdrawal."[7] By viewing space solely from the perspective of national security and failing to predict the economic consequences, protectionist regulation pushed markets overseas and forced other nations to develop indigenous capabilities. For example, self-imposed restrictions on domestic launch service providers allowed the European Space Agency's Arianne rocket, which did not enter the market until 1980, to capture 50 percent of worldwide commercial business by 2001.[8] In addition to the growth of non-US launch service suppliers, nations are creating their own capabilities for space navigation, earth observation, communication, and space exploration.

In addition to the loss of business, US companies also face harsh penalties for violating these regulations—whether the infringement was intentional or not. The United States severely penalized Hughes and Loral under the Cox Committee for allegedly helping the Chinese identify and overcome engineering deficiencies associated with the Long March rocket.[9] Fearing additional retribution, the aerospace industry has shied away from further developing international business opportunities to the extent they could if these prohibitions did not exist. These unfortunate conditions have led to a sharp decline in US space-related exports and a surge in international competition.

Paradoxically, the regulations designed to protect US technology created new international markets based solely on avoiding US export controls. Many foreign businesses offering space services eliminated all US subcontractors from their supply chains and began lucratively advertising themselves as "ITAR-free."[10] In some cases, these restrictions had the opposite effect of spawning new technologies equal to or better than those available from US suppliers.[11] In light of international ad-

vances in space technology and the associated increase in foreign availability of components, the Department of Defense (DOD) has at least acknowledged the need to review US export controls.[12] Without reform, the current body of regulation will continue to be detrimental to the health and welfare of the industrial base, especially lower-tier suppliers. Revising these laws will enable US firms of all sizes to compete more successfully in a global economy increasingly capable of independently producing advanced technologies.[13]

The primary strength of the US economy has always been its ability to continuously innovate. Protectionism fosters complacency, and complacency kills innovation. Therefore, the United States should enact domestic legal frameworks that foster its competitive edge rather than endeavoring to stifle global technological progress out of fear that the country may not be able to retain its historical advantage. The United States should trust its capacity to overcome challenges and not attempt to isolate itself from them. The bedrock of a space sustainment strategy is creating the conditions and incentives necessary for economic growth. It embodies a positivistic philosophy of sustained, continuous achievement through adaptation and innovation over the negative objective of focusing on the false hope of endlessly eliminating competition. AFSPC should be a leading advocate for this legal reform since it will be a primary recipient of the benefits that a healthy industrial base provides.

Defending Space Equities

Successfully promoting private industry requires a mechanism for protecting equity in space. This fact requires nations to analyze and agree, at least implicitly, upon the methods actors may employ to protect their investments and their livelihood. Current policy, such as the 2010 *National Space Policy* and the 2011 *National Security Space Strategy*, approaches the problem of defending space equities from the perspective of exercising the inherent right of self-defense.[14] The United States asserts that military force may be required to deter and possibly defeat

hostile actions taken against its own assets or those of its allies. While the right of self-defense will not go away, it may not be the only standard the United States should apply when considering future space operations.

For example, the legitimacy of police forces and their associated activity derives from the need to ensure social order. The use of force in a law enforcement context is not relegated solely toward self-defense, and the amount of force applied in a situation is dependent on the "amount of effort required by police to compel compliance by an unwilling subject."[15] Governments could apply this same standard to the space domain such that the use of force could be considered legitimate not only in the context of self-defense but also as a method for enforcing order.

If one agrees that force is appropriate for promoting order in space, then the next logical question becomes, who should be responsible for applying that force? The international community is not yet ready to answer that question in a formal sense, but that does not mean individual states cannot or will not assume that role on their own. If one takes the view of international relations as an "anarchical society," the United States, by virtue of its overwhelming capability, must resort to self-help behavior and "take upon [its] own shoulders the responsibility of determining that there has been a breach of the rules, and of attempting to enforce them."[16] Despite many mistakes, the United States has handled its hegemony to promote international order in a more positive way than has been typical of other significant powers in history. As Dolman remarks, the United States is "the most benign state that has ever attempted hegemony over the greater part of the world."[17] Mike Moore, author of *Twilight War*, expresses a similar view of the US record of accomplishment:

> "The fact that the United States over the past sixty-plus years has not used its extraordinary economic and military might to build a classic do-as-we-say-or-face-the-consequences global imperium makes America an exceptional nation when judged by the miserable standards of world history. To be sure, the United States works diligently, either overtly or covertly, to make things go

> its way. That has been true of all great powers in the history of the world. But America does not attempt to run the world like a modern-day Rome."[18]

While the preceding discussion helps demonstrate why the United States should assume the role of the primary custodian for maintaining order in space, it is obvious that implementing this aspect of a space sustainment strategy will be difficult. One difficulty stems from the military controlling, or at least maintaining significant influence over, the predominance of space capabilities. Terrestrially, observers can often divide the control of geographic territory into police forces for suppressing internal threats to order and military forces for defending against external threats. This makes for a relatively clean division of roles and responsibilities. Since space is inherently global, no such clear demarcations between law enforcement and military activity exist. From an international perspective, observers cannot easily distinguish the actions of military forces used in a self-help capacity to uphold the rule of law from those of conquest. Therefore, the use of military forces to police behavior in space may make it difficult for the international community to determine if the intent of those actions is to sustain the greater good or to seize a position of advantage.

Dolman also analyzes the role of power in space but overstates the appropriate role of force in promoting economic growth and protecting private interest. He states, "What is too little understood by advocates of the free market is that while economic monopolies destroy the market, a monopoly of power is essential to its success."[19] While this is true from the perspective that it would be counterproductive to have, for example, competing police forces within the same jurisdiction or more than one rule of law within a given country, one must be careful not to allow the monopoly of power to exceed its proper objective. The monopoly of power must be oriented toward facilitating economic growth and protecting private equity. It must not become an end unto itself by attempting to assert control over the direction of the market.

The global nature of space effects presents a second difficulty. In terrestrial domains, the violence employed by either police forces or

militaries is generally localized to the contested area. In space, aggressive behavior often has lasting, global consequences. The 2,200 pieces of orbital debris caused by the 2007 Chinese antisatellite demonstration is illustrative of this point.[20]

If commercial interests are to flourish in space, then an acceptable international rule of law will have to emerge from the existing anarchy. The United States is currently the only nation postured to take on the responsibility—largely due to the existing and future capabilities that AFSPC and its government partners provide. It is also the nation most reliant on space. In this sense, the United States has both the capacity and the incentive to sustain the space environment for peaceful commerce. Yet, given the current inability to distinguish between military and police actions in space, the international community is not likely to accept US unilateral behavior. Therefore, the United States should adopt a space sustainment strategy aimed at defending space in partnership with other nations to foster legitimacy. Transparency will be the foundation of these partnerships.

Enhancing Transparency

As Joan Johnson-Freese, a professor at the Naval War College, plainly states, "We need more and better information about what is going on in space."[21] Much of the existing international legal framework for space emerged from both the desire and the capability to monitor behavior. During the Cold War, nuclear deterrence rested on a careful balance of power. After tense negotiations, both sides came to understand that some amount of transparency was required to minimize the risk of starting a nuclear war. The first attempts at transparency were discouraging. Soviet leader Nikita Khrushchev rejected Pres. Dwight D. Eisenhower's call for "Open Skies."[22] He could not accept US aircraft in Soviet airspace, but due to an inability to strike a satellite in orbit and the precedence set by Sputnik, he tolerated reconnaissance from space. In 1972, following the Strategic Arms Limitations Talks, both sides codified the importance of employing national technical means

for nuclear treaty verification into the vernacular of the Cold War.[23] They accepted the need to cede some amount of secrecy and sovereignty for the larger objective of promoting security and international stability. While most surveillance has historically dealt with terrestrial activity, it is likely to expand toward monitoring space assets as well.

Transparency is a precondition of effective and legitimate international rule of law. In the future, both market competition and political disagreements will likely manifest themselves in space. Therefore, demand for AFSPC's space situational awareness (SSA) capabilities will continue to grow as the importance of monitoring space activity increases. Initially, this heightened awareness of space capabilities will cause alarm, just as Open Skies did in the 1950s. As before, nations will have to decide if revealing more about their capabilities (and potentially curtailing some forms of activity) for the greater good of international security is in their best interest. This decision could be especially difficult for the United States since it will likely be the primary financial backer of an international SSA capability and it could also have the most to lose from the perspective of secrecy. Despite these concerns, this will likely be the price of maintaining US leadership in space in the future.

As the historical evidence suggests, if the United States decides not to promote transparency in space, other nations will. In this scenario, the United States would lose credibility for not having participated in supporting the trend toward openness, jeopardizing the legitimacy of self-help behavior. The negative consequences could also spill over to US commercial entities, which would suffer economically if international competitors capture the market for SSA services.

Fortunately, the United States is already taking steps in this direction. The 2010 *National Space Policy* declares, "Space operations should be conducted in ways that *emphasize openness and transparency* to improve public awareness of government, and enable others to share in the benefits of space" (emphasis added).[24] Likewise, the 2011 *National Security Space Strategy* describes how the DOD "will continue to im-

prove the quantity and quality of the SSA information it obtains and expand provision of safety of flight services to US Government agencies, *other nations and commercial firms*" (emphasis added).[25] In line with this direction, Adm Cecil Haney, commander of United States Strategic Command (USSTRATCOM), recently testified before the Senate Armed Services Committee that

> sharing SSA information with other nations and commercial firms promotes safe and responsible space operations, reduces the potential for debris-making collisions, builds international confidence in US space systems, fosters US space leadership, and improves our own SSA through knowledge of other owner/operator satellite positional data.[26]

Similarly, Deputy Assistant Secretary of Defense for Space Policy Douglas Loverro highlighted before the House Armed Services Committee how USSTRATCOM has signed five SSA-sharing agreements with other governments—Australia, Japan, Italy, Canada, and France—and increased the number of agreements with commercial satellite operators to 41.[27] Finally, in early 2014, AFSPC commander Gen William Shelton took another important step forward toward transparency at the Air Force Association Air Warfare Symposium. During his speech, he announced that the USAF would send two Geosynchronous Space Situational Awareness Program satellites into orbit this year. Those satellites will augment the nation's ability to monitor satellites in geosynchronous orbit for collision avoidance and to detect potential threats.[28]

Each of these recent examples from senior defense leaders highlights a growing trend toward more openness in space. Yet, for the foreseeable future, a healthy tension between security and transparency will persist in the minds of policy makers. While Admiral Haney enumerated the benefits of sharing SSA, he also acknowledged the risks when he said, "For all its advantages, there is concern that SSA data sharing might aid potential adversaries."[29] His struggle to define an appropriate balance between secrecy and openness is a modern reflection of President Eisenhower's dilemma with the Soviet Union and Open Skies. President Eisenhower shifted his emphasis toward open-

ness and ultimately achieved a more stable international order. A similar decision with respect to SSA may prove equally beneficial for the future of international order in space.

This focus on increased transparency is an important step toward adopting a space sustainment strategy that embraces improvements in the monitoring and sharing of international space activity. Transparency will promote the rule of law, support international stability, and enhance the legitimacy of policing forces. These conditions will also foster commercial innovation, development, and risk taking in space.

Conclusion

Khrushchev once said, "Those 'rotten' capitalists keep coming up with things which make our jaws drop in surprise."[30] Promoting jaw-dropping innovation through free-market capitalism should be the focus of US space policy. Competing on the merits of the US economy will serve America far better than adopting protectionism and isolationism. The space sustainment strategy outlined here advocates three distinct steps to help the United States continue to succeed in space. First, both international and domestic law should be modified. International law should clearly protect private property rights. Domestic law should reduce the barriers inhibiting US companies from competing internationally. It should foster domestic innovation through a vigorous free market empowered to outcompete, rather than attempting to suppress, international actors. Second, the United States must lead the international community toward policing strategies aimed at promoting and protecting international rule of law in space so that a commercial marketplace can operate safely. In doing so, careful distinctions must be made between military and police forces. Finally, transparency will be a key factor in establishing a legitimate legal framework for space. Therefore, the United States should continue to enhance SSA capabilities and develop international partnerships for sharing that information.

AFSPC will play a critical role in the transformation of the current mind-set toward this new paradigm. It will also be the agency most called upon to monitor activity and ensure order within the space domain. Its participation and advocacy are crucial for a space sustainment strategy's success. The results will enable the United States to maintain its leadership role in space and foster a peaceful climate for future commerce and international space activity. ✪

Notes

1. Walter A. McDougall, *The Heavens and the Earth: A Political History of the Space Age* (Baltimore, MD: Johns Hopkins University Press, 1997), 6.
2. Lewis D. Solomon, *The Privatization of Space Exploration: Business, Technology, Law and Policy* (Oakland, CA: Transaction Publishers, 2011), 8–11.
3. Department of Defense, *National Security Space Strategy: Unclassified Summary* (Washington, DC: DOD, January 2011), 1, http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.
4. Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Portland, OR: Routledge, 2002), 138.
5. Ibid., 133.
6. Solomon, *Privatization of Space Exploration*, 111.
7. Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 159.
8. Ibid., 142–43.
9. Ibid., 146, 162.
10. Peter L. Hays, "Space Law and the Advancement of Spacepower," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes et al. (Washington, DC: National Defense University Press, 2011), 312.
11. Joseph Fuller Jr. et al., "The Commercial Space Industry: A Critical Spacepower Consideration," in *Toward a Theory of Spacepower*, 111–12.
12. DOD, *National Security Space Strategy*, 3.
13. Ibid., 7.
14. Ibid., 10; and Executive Office of the President, *National Space Policy of the United States of America* (Washington, DC: Executive Office of the President, 28 June 2010), 3, http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.
15. National Institute of Justice, "Police Use of Force," 20 January 2012, http://www.nij.gov/topics/law-enforcement/officer-safety/use-of-force/Pages/welcome.aspx.
16. Hedley Bull, *The Anarchical Society: A Study of Order in World Politics*, 3rd ed. (New York: Columbia University Press, 2002), 58.
17. Dolman, *Astropolitik*, 157–58.
18. Mike Moore, *Twilight War: The Folly of U.S. Space Dominance* (Oakland, CA: Independent Institute, 2008), 283.

19. Dolman, *Astropolitik*, 177.
20. James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests* (Stanford, CA: Stanford Security Studies, 2008), 53.
21. Johnson-Freese, *Space as a Strategic Asset*, 110.
22. McDougall, *Heavens and the Earth*, 127.
23. Ibid., 431.
24. Executive Office of the President, *National Space Policy*, 3.
25. DOD, *National Security Space Strategy*, 6.
26. Mike Gruss, "U.S. Space Assets Face Growing Threat from Adversaries, STRATCOM Chief Warns," *Spacenews.com*, 28 February 2014, http://www.spacenews.com/article/military-space/39669us-space-assets-face-growing-threat-from-adversaries-stratcom-chief.
27. House, *Testimony of Douglas Loverro before the House Committee on Armed Services Subcommittee on Strategic Forces*, 113th Cong., 2nd sess., 3 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Loverro_03-12-14.pdf.
28. Zachary Vucic, "Shelton Announces New Space Situational Awareness Satellite Program," Air Force News Service, 24 February 2014, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/473403/shelton-announces-new-space-situational-awareness-satellite-program.aspx.
29. Gruss, "U.S. Space Assets Face Growing Threat."
30. McDougall, *Heavens and the Earth*, 233.

Lt Col Kris Barcomb, USAF

Lieutenant Colonel Barcomb (BS, Clarkson University; MS, Air Force Institute of Technology; and MAAS, School of Advanced Air and Space Studies) is commander, 1st Air and Space Test Squadron, Vandenberg AFB, California, where he is responsible for leading a team of engineers, maintainers, and operators to evaluate and test a diverse array of innovative Air Force space capabilities. He is a career space professional and has held a range of positions across Air Force Space Command and the intelligence community spanning satellite operations, space systems acquisition, and research and development. He also led cyberspace planning and operations in support of multiple combatant commands as the chief of cyberspace strategy for Twenty-Fourth Air Force, Lackland AFB, Texas.

Space Resilience and the Contested, Degraded, and Operationally Limited Environment

The Gaps in Tactical Space Operations

Capt Bryan M. Bell, USAF
2d Lt Even T. Rogers, USAF

The ability of space assets to deliver combat effects to theater operators is at a critical juncture. Over the past decade, not only have adversary counterspace capability and strategy surged markedly but also the number of objects occupying space have risen exponentially.[1] A significant proportion of US Air Force space systems were conceived and brought online during a much different operational landscape, and we have continued to operate a number of them well past their design life. Space is not the invulnerable high ground it once was. National security space leadership has recognized these challenges and describes our present environment as contested, degraded, and operationally limited (CDO).[2] Gen William L. Shelton, who recently retired after serving as commander, Air Force Space Command (AFSPC), has challenged the space operations and acquisitions community to reevaluate mission resiliency in light of these new circumstances. This appeal has manifested in the institution of new strategy and policy focused on bolstering space situational awareness (SSA),

the disaggregation of system capability across new architectures, and the cultivation of international partnerships.[3]

While these initiatives may eventually result in the desired resiliency, they face implementation challenges in the form of tightened budgets and constrained manning. History has shown that the strategic advantages provided by technological capability are contingent upon their application by a well-trained, competent fighting force. These rules of warfare are no less applicable to space: the most effective defensive space control system will be the tactical crews and support personnel on whose shoulders mission assurance firmly sits. We assert that in a CDO environment, space operations squadrons are not prepared to provide global combat effects in support of joint force commander (JFC) objectives.

AFSPC's ability to deliver effects to JFCs while facing CDO threats requires timely and accurate characterization of the battlespace, rapid assessment and attribution of incidents, and precise prescription and employment of tactics.[4] In essence, this means achieving a fast and effective observe, orient, decide, act (OODA) loop. However, John Boyd's work indicates that as individuals make decisions, they often misunderstand their "relationship to the rapidly changing environment."[5] In light of this contextual misperception, we examine three common characteristics of tactical space operations that inhibit realizing the desired OODA loop:

1. Critical dependence upon on-call subject-matter experts (SME).
2. Inability to distinguish and attribute the source of mission degradation.
3. Limited awareness of the impacts of CDO events on supported operations.

These problems exist because current AFSPC training and operations frameworks are founded in past, pre-CDO space assumptions not sufficient for today's space domain. Since the operational environment has changed, AFSPC must reevaluate the assumptions it operates under

and find a CDO-centered path to organize, train, and equip its forces. We propose that the following no- or low-cost solutions be promptly instituted throughout the administrative and operational chains of command:

1. Inaugurate a tiered certification paradigm that develops *true* expertise.
2. Establish and focus intelligence support for tactical mission planning and execution.
3. Integrate CDO space operations into Air Force and joint exercises.

These solutions will begin to lift the self-imposed fog and friction of war resulting from AFSPC's legacy training and operations methods. If AFSPC does not take action to resolve these issues, space operations will be inadequately equipped to respond to the crises inherent in the CDO environment. As a result, JFCs will not be guaranteed the asymmetric advantage that has been fundamental to US force projection for over two decades.

Train for the Fight

> *Know and use all the capabilities in your airplane. If you don't, sooner or later, some guy who does use them will kick your ass.*
>
> —Lt Dave "Preacher" Pace
> US Navy Fighter Weapons School Instructor

Winning the CDO fight will come down to "whoever can handle the quickest rate of change."[6] In their current state, space crews fall short of this axiom. Their ability to provide timely characterization, assessment, and mitigation of anomalous events is restricted to the content outlined in system checklists. Consequently, this limits operator reaction to known problems with strict, demand-response solutions. Even still, many of those actions lead to contacting or recalling on-call specialists for assistance, despite prior occurrence. Put plainly, the support elements (e.g., engineering, intelligence, tactics, and user support) re-

quired to "fight through" CDO events are not truly organic to 24/7 operations environments. In a 168-hour calendar week, experts are readily available for only 45 hours—meaning that less than 30 percent of operations are performed with full capability to sustain the mission. In terms of John Boyd's loop, more than 70 percent of the time the phenomena that shape accurate observation and orientation are greatly impeded (see fig. 1).[7] In a growing CDO environment, crews are more likely to face the type of complex historical, or even zero-day, anomalies that currently require SME resolution.[8] When JFC operations are under way, the response time associated with alerting experts can severely degrade the mission.[9]

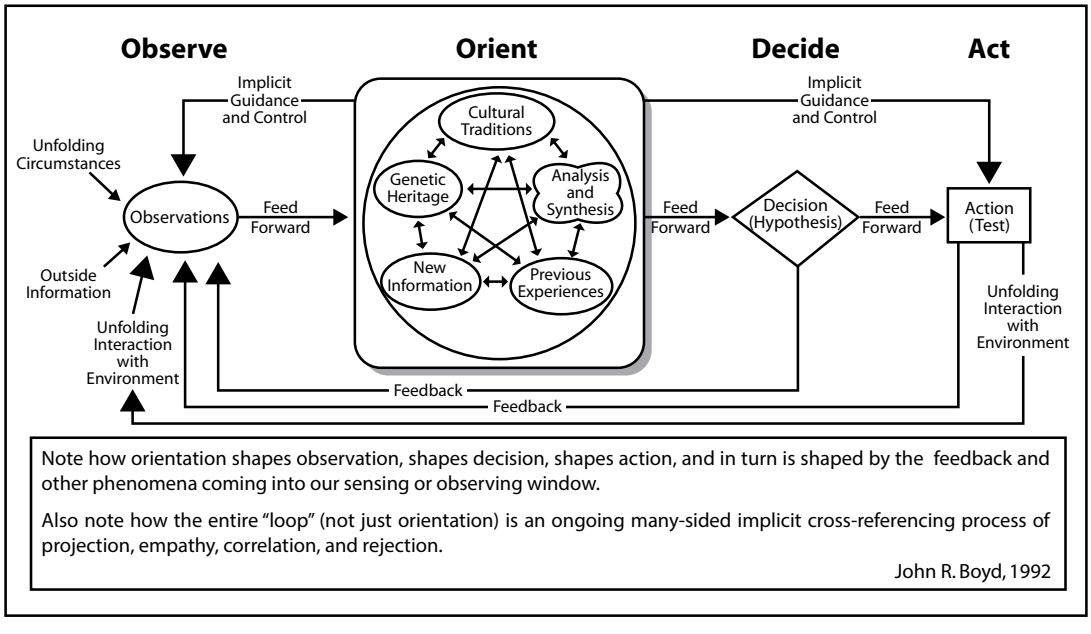


Figure 1. Boyd's OODA loop. (*Reproduced from* Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* [New York: Back Bay Books/Little, Brown and Company, 2002], 344.)

A heavy reliance on SMEs is predominantly a proficiency rather than a process problem. Space crews must turn to these experts because the skill sets are not inherent to operations certification programs.[10] AFSPC can reduce this dependency by codifying a new certification paradigm

that does more than prepare operators to "fly" their systems through fair weather. Instead, the focus should shift toward developing experts who can operate in adverse conditions while facing enemy activity. This will require restructuring initial, mission, and continuation training around the on-call subject areas within a broader, CDO-focused curriculum. We propose a commandwide standard that completely integrates system capabilities, nominal and CDO space operations, and combat effects content within a single complementary and graduated syllabus emphasizing the relationships between the same core areas of study (see table 1).

Table 1. Proposed CDO-focused space operations certification program

Training	System	Mission Operations (Nominal vs. CDO)		Combat Effects / User Application
Emphasis	40%	40%	10%	10%
Initial Qualification	Basic system and subsystem capabilities, limitations, integration, and employment considerations	Introduction to mission area Basic position-specific tasks	Threats, impacts, and tactics fundamentals Basic degraded and operationally limited threats, impacts, and tactics	Singular missions or weapon systems
Emphasis	30%	25%	25%	20%
Mission Qualification	Advanced subsystem functionality and integration	Advanced position-specific tasks Graduated crew integration tasks	Advanced degraded and operationally limited threats, impacts, and tactics Graduated integration of controlled threats, impacts, and tactics Graduated mission planning	Integration of multiple missions or weapon systems
Emphasis	20%	10%	40%	30%
Continuation	Advanced subsystem case studies	System upgrade specifics	Advanced threat integration, impacts, and tactics within enemy COAs	Integration of multiple missions or weapon systems within JFC missions and objectives

In the proposed construct, the goal of initial qualification training (IQT) is the development of system expertise. It begins with an in-depth understanding of system and subsystem capabilities, limitations, and employment considerations through academic study and practical application. As is common today, this branch of study will focus on developing proficiency in nominal operations. However, this is not enough for fighting through CDO; thus, an introduction to CDO concepts and combat effects fundamentals is necessary to begin connecting nominal operations to the reality of today's challenging space domain and the potential impacts to supported operations.

With this foundation, operators will be prepared for a mission qualification training (MQT) curriculum that caps system expertise with study of subsystem relationships and in-depth case studies of real-world anomaly resolution actions. In parallel, nominal operations training will expand beyond position-specific tasks to focus on crew-wide integration. Additionally, combat effects and CDO modules will emphasize friendly system integration and multiple simultaneous-threat scenarios, respectively, with a gradual increase in CDO concept difficulty. This will begin to provide operators with an understanding of how joint war fighting relies upon space capabilities.[11] A graduate of MQT, as a certified mission-ready operator, will be able to respond to known adversary threats and system malfunctions while minimizing impacts to supported missions. They will lack the ability to completely mitigate zero-day events but will possess the necessary expertise to identify, assess, and troubleshoot a problem while awaiting on-call SMEs.[12]

The knowledge and experience gained in IQT and MQT must be reinforced by robust continuation training (CT) that simultaneously prepares operators for the challenges of CDO space and acts as the basis of a space cadre "upgrade" program. The CT curriculum would focus on three critical areas: (1) in-depth analyses of recent real-world anomalies and their resolution for maintaining troubleshooting currency, (2) comprehensive training on the broad impacts of CDO events to current and future JFC missions, and (3) mastery of significant system

upgrades and/or changes. The rigorous nature of the proposed construct will require a tailored approach to training individuals at varying levels of expertise.

As suggested by Lt Col Phil Bauer, Lt Col Bill Woolf, and Maj Jon Slaughter in their briefing "USAF Warfare Center: 'How Can We Help?,'" this is an opportunity to institute an advanced space training construct similar to the "ready aircrew program." Unlike today's upgrade programs, a clearly documented, skills-based, and objective method of training and evaluation must be formalized to ensure only the most capable operators are in a position to develop, certify, and lead the next generation of crew members.[13] Colonel Bauer and company propose adapting the air operations "squadron letter of Xs" concept to track such progression. Their first draft drove our satellite operations–specific expansion (see table 2) that should be used by the command as a departure point to generate such a program.[14]

Combating CDO events requires frontline crews to conduct real-time analysis, synthesis, and problem solving of unfolding events. This starts with operators who possess the depth of system, operations, and combat effects proficiency currently expected of on-call SMEs. Current certification programs are not sufficient to this end since they develop only surface-level competence. To solve this problem, AFSPC must foster support personnel levels of expertise across all operator training curricula. The result would be a vast improvement in CDO-readiness capabilities over today's 30 percent availability rate. While enhanced mission-area expertise is certainly necessary for fighting through a CDO environment, it is not enough for a tactically advantageous OODA loop. Enhancing the fidelity of observation and orientation phenomena to drive more accurate and effective operator decisions and actions also requires a level of situational awareness (SA) that is largely absent from current space operations.

Table 2. Proposed satellite operations "letter of Xs"

NAME	CERT LVL	RANK	POSITION	EXP LVL	FLT LD	COMMAND SUPPORT	TRACK SUPPORT	BUS ALARM	PAYLOAD ALARM	UPLINK EMI	DOWNLINK EMI	STATIONKEEP	COLA STATIONKEEP	ANOMALY RESPONSE	EXERCISE	ADVANCED TRG	UPGRADE TRG	REMARKS
A	MR	Lt Col	MC															
B	MR	Capt	MC															
C	MR	1st Lt	SVO															
D	MR	2d Lt	SVO															
E	MR	SSgt	SVO															
F	MQT	2d Lt	SVO															
G	MQT	SrA	SVO															

You Can't Fight What You Can't See

The essence of information is the negation of uncertainties, or negative entropy. Entropy is disorder, thus negative entropy means order. This means that areas with the greatest uncertainties will have the greatest demands for information. Whoever can turn uncertainties into certainties will gain the upper hand under such conditions.

—Timothy L. Thomas, paraphrasing Shu Enze

When responding to mission degradation, tactics implementation is critically dependent upon an operator's ability to distinguish between

incidents caused by system malfunction or environmental factors and those resulting from adversary activity. It is unlikely that present space operations crews and support personnel would be able to adequately make this distinction even if problems of proficiency were resolved. The source of this predicament is the lack of "capabilities that enable rapid threat identification and attribution, [which] facilitate a defensible architecture and provide a fundamental shift in space awareness."[15] Because operators are blind to their environment—physically, spectrally, and environmentally—they are confined to initiating OODA loops that lead to the execution of tactics focused solely on system malfunction.[16] The operational exigencies of CDO space make this an unacceptable risk. The solution is to provide space operations units with battlespace characterization for both ongoing operations and forecasted conditions, thereby leveraging and incorporating intelligence preparation of the operational environment (IPOE) and real-time, full-spectrum factor-threat identification in support of tactical-level mission planning and execution, respectively.[17]

Since IPOE is not standard in tactical space operations—there was no need for these functions below the operational level prior to the rise of a CDO space environment—AFSPC must start by assigning dedicated intelligence personnel to each space operations squadron. As unit representatives for the Joint Space Operations Center's operational intelligence functions, they would provide mission-specific "multidimensional understanding of the operational environment."[18] With this integrated IPOE support, crews will be able to "anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities."[19] Accounting for adversary and environmental disposition and their associated indications and warning (I&W) can mean the difference between correctly attributing commanding anomalies to environmental perturbations caused by heightened solar activity, for example, as opposed to loosely speculating on ground system or spacecraft malfunctions. More importantly, it can provide operators the preliminary context for relating anomalies to enemy counterspace operations. However, complete attribution—and subsequent

implementation of tactics—will be limited if crews are unable to perceive the threat environment in near real-time. As stated in Joint Publication 2-0, *Joint Intelligence*, "precise threat location, tracking, and target capabilities and status, in particular, are essential for success during actual mission execution."[20]

The uniqueness of the space domain requires SA tools that fuse all aspects of potential adversary attack vectors and environmental susceptibilities—spatial/orbital, spectral, and environmental, to name a few. While multiple tools currently available provide independent, unintegrated SA on some of these aspects, they are limited in capability. Their use for this function is not standard operational practice. Formalizing the use of Web-based Integrated SSA (WebISSA), Joint Spectrum Interference Resolution Online (JSIRO), and the Air Force Weather Agency's space environment global situational awareness chart will provide crews elementary physical, spectral, and environmental SSA, respectively. WebISSA can alert spacecraft operators of encroaching satellites.[21] JSIRO can be used, at best, for ad hoc spectral SSA to identify potentially related electromagnetic interference (EMI) incidents.[22] The space environment global situational awareness chart's stoplight table can provide a rough estimate of the space environment's contributions to CDO events.[23]

While these tools can provide a basic level of battlespace characterization, they are not sufficient for confident, near real-time attribution of external causes, nefarious activity, or environmental conditions, for example, over internal system malfunction. Instead, their shortcomings can easily lead to misattribution. What the command needs is a single tool that fuses physical, spectral, and environmental SSA into a tailorable common operating picture. Such a tool should be able to deduce the difference between a benign close approach and an intended attack vector simply based on relative orbital geometries and known adversary system capabilities. Additionally, it should leverage global electronic intelligence (ELINT) collection to report past and present EM threats, just as ELINT provides aircrews the ability to "locate adver-

sary radars and air defense systems."[24] Finally, it must deliver orbit-, location-, spectrum-, and mission-specific environmental conditions, impacts, and probabilities just as air operations are supplied terrestrial weather status and impacts based on altitude blocks above an area of operations.

Just as "modern air, sea, and land commanders would never consider placing their highest valued assets into an essentially blind operating environment," space commanders must no longer accept the current gap in tactical SSA as adequate for mission accomplishment in CDO.[25] Taking the actions outlined above will ensure that the same fidelity of threat activity relished by air, sea, and land forces becomes a standard of tactical space operations centers. Although such SA is essential for crews to accurately attribute I&W and swiftly mitigate local threats, it does not provide the complete context needed to ensure tactical decisions and actions do not create undesired secondary and tertiary effects across multiple theaters and levels of war simultaneously. This necessitates that tactical integration of space operations with the other domains surpasses levels seen today at the operational and strategic levels of war.

Ramping Up Integration

> *The ordinary man is much more likely to do the right thing if he really understands why he is doing it, and what will probably happen if he does something else; and the best basis for sound judgment is a knowledge of what has been done in the past, and with what results.*
>
> —J. C. Slessor

As CDO matures and evolves, operational-level decision cycles will likely be unable to cope with rapid changes occurring concurrently across multiple systems and their distinct environments. Tactical space operations units executing timely and effective tactics will be increasingly fundamental to mission assurance. This presents a distinct

challenge: the tactical OODA loops of space operations crews can have instantaneous consequences—both intended and unintended—to supported missions across numerous areas of operation (AO) at multiple levels of war. At present, space crews are largely oblivious to the missions and operations their systems are supporting at any given time. The result is a precarious situation in which tactic selection and execution are grounded in incomplete or faulty precepts. An appropriate solution requires that space crews are not only equipped with the requisite decision authority to execute potentially decisive tactics but also that they are seamlessly integrated into the mission planning and execution process of their supported AOs (which, in most cases, crosses multiple combatant commands [CCMD]).[26] AFSPC must begin this process by expanding space participation in CAF exercises like Red Flag and working with the CCMDs to integrate advanced CDO scenarios into their recurring combined large-force exercises.

A measure of space participation has occurred in exercises like Red Flag for a number of years. However, it is typically limited to space force enhancement products used to facilitate air planning and/or the simulated effects of deployable space forces. A more appropriate construct for the CDO environment would be the creation of a "collateral space package" (CSP) equivalent to the other Red Flag planning packages.[27] The CSP should be comprised of satellite operators whose nondeployable systems and capabilities are being leveraged for the exercise scenario.[28] As such, the CSP would be the focal point for synchronizing the tactical mission planning of geographically separated space operations units and integrating those efforts (to include collateral space asset disposition, threats, and contingencies) with the overarching air scheme of maneuver. They would identify the appropriate contracts necessary for notifying air players of the impacts of system degradation to successful accomplishment of the air mission (e.g., the consequences of overhead persistent infrared degradation to specific assets executing a "SCUD Hunt" or of the loss of protected military satellite communications to a B-2 strike mission).

The result of integrating planning and execution for the full spectrum of space capabilities used during Red Flag vulnerability windows is the insertion of critical observation and orientation phenomena into space crew OODA loops. Thus, space crews not only can execute tactics that benefit their "survival" but also can consider those that minimize impacts to terrestrial operating areas. The lessons learned developed from this integration will surely prove invaluable when crews are faced with real-world CDO events. In the end, however, not every OODA loop can be timely and/or effective. Red Flag is arguably the ideal initial testing ground for this construct of integration. However, the benefits described above come to fruition only when the space operations role is considered in the joint environment—both from the perspective of understanding the actual consequences of lost space capabilities to supported operations and to the development of courses of action at the tactical and operational levels of space command and control.

The benefits of the proposed degree of integration are not fully realized except in the context of joint exercises and the application of resulting lessons learned to actual operations. JFCs must integrate the consequences of potential CDO incidents into their OODA loops, just as space operations crews must incorporate one or more JFC's priorities into their tactics execution. In their 2010 "AirSea Battle" study, the Center for Strategic and Budgetary Assessments (CSBA) advocated that "the Air Force and Navy should rigorously train for and recurrently conduct exercises that simulate operations under conditions of lost or degraded space capabilities and capacities."[29] Introducing tactical CDO space operations into these heavily operational and strategic level-of-war exercises will highlight the importance for space crews and supported JFCs to examine "the world from a number of perspectives so that [they] can generate mental images or impressions that correspond to that world," thus preventing the mismatches between reality and their perceptions that ultimately generate incorrect response.[30]

Summary

There are no "battle management" magic bullets that will substitute for the ability of on-scene commanders, soldiers, and airmen to make appropriate decisions based on the ebb and flow of events.

—Richard P. Hallion

One of the widely known principles of the Chinese People's Liberation Army anti-access, area-denial (A2/AD) strategy is to impede US freedom of action by targeting space capabilities. The CSBA provides insight into how an A2/AD scenario might unfold:

> In the opening minutes of conflict, [the enemy would] seek to render US and allied forces "deaf, dumb and blind" by destroying or degrading US and allied Low Earth Orbit (LEO) [intelligence, surveillance, and reconnaissance], Space-Based Infrared System (SBIRS), third-generation Infrared System (3GIRS) sensors and communication satellites. This would be accomplished by employing directed-energy weapons, direct-ascent and co-orbital anti-satellite weapons, or terrestrial jamming, in concert with coordinated cyber and electronic warfare attacks.[31]

An instance such as this will reveal the true caliber of AFSPC's mission resilience. If the command continues to operate under legacy training and operations methodologies, mission resilience will be found wanting. Seventy years of air operations experience has shown that the ability to accomplish the mission and survive the return trip hinges upon an aircrew's weapon system and domain mastery. To answer the demands of CDO, AFSPC must adapt this axiom to the present environment and center its organize, train, and equip function on furnishing operators with the expertise, tools, and operational experiences necessary to do so. It must train operators who can characterize, assess, and respond to mission-impacting events; equip them with the tactical intelligence for comprehending the threat landscape; and clearly connect tactical tasks with supported commander operational objectives and priorities.

To accomplish this, the command must first adopt a certification program that creates and develops operators who are system, threat, tactics, and combat effects (user) experts. Second, intelligence personnel and functions should be integrated into all space crew operations centers, where spatial, spectral, and environmental intelligence can be fused to support active- and factor-threat identification. Finally, Air Force and joint exercises should expand the incorporation of space operations. This change would better characterize air component commander and JFC reliance on space capabilities, impacts to strategy when those capabilities are lost, and processes required to mitigate these losses. By enacting these remedies, AFSPC can ensure that the tactical initiative resulting from space crew OODA loops maintains operational and strategic harmony with supported operations.[32] ✪

Notes

1. Office of the Director of National Intelligence (ODNI) and Department of Defense (DOD), *National Security Space Strategy* (*NSSS*): *Unclassified Summary* (Washington, DC: ODNI and DOD, January 2011), 1–2.

2. In his briefing "Training for [CDO] Environments," Maj Patrick "Weezer" Slaughter, 561st Joint Tactics Squadron, establishes the following definitions and examples for CDO. *Contested operations* are defined by degradation caused by enemy action, for example, laser, direct ascent, and co-orbital antisatellite (ASATs) weapons, electronic warfare threats, cyber attacks, and foreign space object surveillance and identification. *Degraded system operations* are defined by degradation caused by failed systems or battle damage (e.g., uplink and downlink anomalies, bus and payload anomalies and malfunctions, ground system malfunction, and mission partner system failures. *Operational limitations* are defined by reduced mission effectiveness caused by the physical or operational environment (e.g., conjunctions and collision avoidance, terrestrial and space weather, classification, decision authorities, policy, and many others).

3. Gen William L. Shelton, commander, Air Force Space Command, "Space and Cyberspace: Foundational Capabilities for the Joint Warfighter and the Nation" (address, Air Force Association Air Warfare Symposium, Orlando, FL, 21 February 2014).

4. Hereafter the term *threats* is used to generically refer to any action or function that facilitates a CDO space environment and the term *tactics* to generically refer to any action taken to mitigate a threat.

5. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books/Little, Brown and Company, 2002), 334–38.

6. Ibid., 328. While speed of the decision cycle is important, it is not—as is commonly espoused—the sole or even most important metric for evaluating effectiveness. Rapidly executing decision cycles with inaccurate input/feedback can exacerbate the confusion that is already inherent in conflict. Furthermore, imprecise interpretation of and orientation to those

phenomena can lead to execution of courses of action that are not adequate to the realities of the situation, leading to the collapse of the decision cycle and defeat. Prevailing through conflict results from the continuous effective, accurate, and rapid execution of the decision cycle, which creates an unmanageable uncertainty and ambiguity in an adversary's loop (ibid., 328). For a comprehensive study of the entirety of Boyd's work, see Frans P. B. Osinga's *Science, Strategy and War: The Strategic Theory of John Boyd*.

7. Observation is influenced by unfolding circumstances and interaction with the environment. Orientation, on the other hand, is influenced by new information, previous experience, and analyses and synthesis. As indicated by their required participation for anomaly response, the ability to fully comprehend these phenomena is currently resident with on-call SMEs.

8. *Zero-day*, common vernacular in cyberspace operations and security, refers to exploits or attacks that take advantage of previously unknown vulnerabilities in computer systems.

9. Depending on squadron or group standards, this varies between one and two hours.

10. Of course, in the case of contractor or civilian technical advisors, dependence cannot be completely avoided since these individuals have decades of hands-on experience with their particular space system. However, the instances when this depth of expertise is required are rare. This is illustrated by the fact that active duty personnel from different specialties, to include space operations, are regularly qualified as "on-call" experts.

11. A similar focus on air and space integration training was previously called for by Lt Col J. Christopher Moss, "Bridging the Gap: Five Observations on Air and Space Integration," in *Space Power Integration: Perspectives from Space Weapons Officers*, ed. Lt Col Kendall K. Brown, PhD (Maxwell AFB, AL: Air University Press, December 2006), 174–75.

12. The authors acknowledge that today's operations environment does not permit such cavalier dismissal of checklist discipline. However, they suggest that such adherence to legacy standards in a new, dynamic operating environment is equally as dangerous as delaying tactics by hours. Rest at ease; in the proposed construct, troubleshooting will be utilized only when the limitations of standing procedures are reached.

13. Each position must have a "basic" and "advanced" experience level. When operators complete all basic-level milestones, they will be eligible for advanced-level upgrade nomination by their squadron commander. When nominated, individuals will enter a training pipeline that will develop and test their ability to perform at the upgraded position. Completing upgrade training must be dependent on an individual demonstrating increased depth of knowledge and breadth of application to prevailing in a CDO environment. As operators surpass advanced-level milestones, they will be eligible for additional upgrades to crew leadership positions (e.g., crew chief for enlisted operators and crew commander for officers) and/or instructor or evaluator. Upgrades can no longer be a simple formality for the sake of career progression, as is often the case today. In particular, instructor and evaluator upgrades must go beyond an introduction to academic or evaluation techniques, product development, or simulator familiarization. Fighting through CDO events is critically dependent on certifying operators with the correct level of proven capability; this will not occur if our instructors and evaluators have not proven themselves as the most capable through a rigorous upgrade program.

14. Lt Col Phil Bauer, Lt Col Bill Woolf, and Maj Jon Slaughter, "USAF Warfare Center: 'How Can We Help?' " (briefing, 50th Space Wing, Schriever AFB, CO, May 2014).

15. Quoted in Lt Col Anthony J. Mastalir, *The US Response to China's ASAT Test: An International Security Space Alliance for the Future* (Maxwell AFB, AL: Air University Press, August 2009), 76.

16. In other words, crews lack adequate SSA. Air Force doctrine states that "SSA is crucial to accurately determining space system failures, whether from environmental effects, un-

intentional interference, or attack, giving decision makers and commanders information needed to pursue appropriate actions." LeMay Center for Doctrine, annex 3-14, "Space Operations," updated 19 June 2012, 34, https://doctrine.af.mil/download.jsp?filename=3-14-Annex-SPACE-OPS.pdf.

17. Air Force doctrine states that IPOE "is a process requiring detailed research, analysis, and knowledge of the adversary regarding topics such as force disposition, force sustainment, deployment of forces, weapon system capabilities and employment doctrine, environmental conditions, and courses of action." Ibid., 72, https://doctrine.af.mil/download.jsp?filename=3-14-Annex-SPACE-OPS.pdf.

18. Ibid.

19. Ibid.

20. Joint Publication 2-0, *Joint Intelligence*, 22 October 2013, I-25.

21. As AFSPC's Web-based, shared SSA tool, WebISSA is optional for satellite operators to determine safe-distance threshold violations in concert with collision avoidance analysis. For example, their "Neighborhood Watch" function can alert spacecraft operators to encroaching satellites and provide graphic representation of the associated orbital geometries.

22. As the DOD's Secret Internet Protocol Router Network (SIPRNET) portal for resolving EMI incidents, JSIRO is required for space crews to report EMI. Operators upload impacted frequencies, locations, and times of events into the JSIRO database. The database provides situational awareness to operational chains of command throughout resolution activities.

23. As the Air Force Weather Agency's environmental characterization status tracker, the space environment global situational awareness chart reflects observed events, probable impacts, and reported impacts for the previous two weeks, the current day, and a three-day forecast. The observed events include solar, charged particle, and geomagnetic activity. They are characterized generically as quiet, active, or very active. The probable impacts include high-frequency (HF) communications, satellite operations, space object tracking, high-altitude flight, and radar interference. They are characterized generically as favorable, marginal, or unfavorable. The reported impacts include HF communications, ultra-HF (UHF) satellite communications, satellite operations, space object tracking, high-altitude flight, and radar interference. They are characterized generically as favorable, marginal, unfavorable, or no report.

24. LeMay Center for Doctrine, annex 2-0, "Global Integrated Intelligence, Surveillance and Reconnaissance Operations, updated 6 January 2012, 56, https://doctrine.af.mil/download.jsp?filename=2-0-Annex-GLOBAL-INTEGRATED-ISR.pdf.

25. Lt Col Anthony J. Mastalir, *The US Response to China's ASAT Test: An International Security Space Alliance for the Future,* Drew Paper No. 8 (Maxwell AFB, AL: Air University Press, August 2009), 76.

26. In fact, the first steps in such changes to space command and control have already manifested in the delegation of emergency procedure execution to squadron commanders in standing orders from the United States Strategic Command's Joint Functional Component Command for Space. In the opinion of the authors, current authorities are inadequate, unbalanced, and ill-equipped. But that is a topic for another time.

27. While collateral space planning has been wrapped into the "nonkinetic package" previously, collateral space considerations are typically secondary to the effects created by deployable space assets.

28. Examples include the Global Positioning System (GPS), wideband military satellite communications (MILSATCOM), protected MILSATCOM, and space-based missile warning, for starters. Additionally, the authors are not demanding the physical presence of operators who would be geographically separated during real-world execution. Instead, exercising

with real-world, friendly-force disposition is essential to gaining the most complete lessons learned.

29. Jan van Tol et al., CSBA, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington, DC: CSBA, 2010), 87.

30. Quoted in Lt Col David S. Fadok, "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Col Phillip S. Meilinger, (Maxwell AFB, AL: Air University Press, 1997), 367.

31. Tol et al., *AirSea Battle*, 21.

32. Fadok, "John Boyd and John Warden," 365.

Capt Bryan M. Bell, USAF

Captain Bell (BS, University of Florida; MS, Air Force Institute of Technology) is assistant operations officer and weapons officer, 4th Space Operations Squadron, 50th Space Wing, Schriever AFB, Colorado. He is responsible for synchronizing operations, training, and maintenance activities of the Milstar and Advanced Extremely High Frequency Protected-MILSATCOM constellation and preparing its operators to prevail through a contested environment. Previously, Captain Bell was a future operations planner for US Cyber Command. He is a graduate of the US Air Force Weapons School.

2d Lt Even T. Rogers, USAF

Lieutenant Rogers (BA, Virginia Military Institute) is chief, Weapons and Tactics Training, 4th Space Operations Squadron, 50th Space Wing, Schriever AFB, Colorado. He is responsible for the development and training of contested operations curriculum for Milstar and Advanced Extremely High Frequency (AEHF) satellite operators. Prior to his current position, Lieutenant Rogers operated the AEHF Satellite Mission Control Subsystem, providing satellite command and control and over-the-air cryptographic rekey in support of strategic and tactical Protected-MILSATCOM users. Lieutenant Rogers is pursuing an MA at the University of Chicago with a focus on space policy.

Robot Futures by Illah Reza Nourbakhsh. MIT Press (http://mitpress.mit.edu/), 55 Hayward Street, Cambridge, Massachusetts 02142-1493, 2013, 160 pages, $24.95 (hardcover), ISBN 978-0-262-01862-3.

Dr. Illah Reza Nourbakhsh, a professor of robotics at Carnegie Mellon University and the coauthor of *Introduction to Autonomous Mobile Robots*, also directs the Community Robotics, Education, and Technology Empowerment (CREATE) Lab. His book *Robot Futures* offers a compelling look at the likely developmental path for the robotics field and its implications for society. Nourbakhsh has produced a work relevant to individuals who focus on air and space issues, doing so by first breaking down stereotypical views of what robotics encompasses and creating an intellectual bridge for readers at all levels through the use of creative fictional scenarios that have easy parallel applications to military efforts.

Perhaps one of the most powerful aspects of *Robot Futures* is its opening of the aperture of what most people today would recognize as a robot. Examples might include simple systems that vacuum carpet or assemble cars in factories. However, Nourbakhsh broadens this scope to include systems and subsystems that are denizens of both the physical and virtual world. Smartphones of ever increasing power and sophistication, for example, can sense our activities and tap into the Internet to provide us with useful and needed information (p. xv). Further, the concept of "interaction tuning" extends the data-mining capabilities of web pages to all interactions with a company and individuals in the real world, allowing for complex experimentation on what works best to increase revenue (p. 9). These creations will become increasingly able to survey and interact in the physical world while simultaneously tapping the deep knowledge base of the Internet to best determine a course of action at perhaps a great advantage over the abilities of mere

mortals. The implications of this progression are broad and perhaps disruptive, as exemplified by the author's examination of advertising and the manipulation of human desire and public opinion. Similarly significant are the potentially chaotic effects that might arise following the mass proliferation of these systems. Finally, he considers the unfolding struggle to create an ethical structure for these more-than-machine constructs and the enfolding of this technology into human physiology for enhancement or even control. The examples are both strong and illustrative of the possible implications of this technology.

Nourbakhsh does a remarkable job of building instances of technological concepts that are an extension of cutting-edge doctoral work by creating a framework which anyone can understand through his use of fanciful accounts at the beginning of chapters. These renditions, providing a recognizable construct in which to place the follow-on discussion of the technology and making it accessible to all readers, are perhaps the real strength of the book. Readers can not only grasp the concepts presented but also, by extension, correlate them in multiple areas of application. People conversant with the air and space domains are already familiar with what robotics has brought to the field of remotely piloted aircraft and space systems. But the author's examples expand the possibilities even further. Examinations of robotic marketing systems that can sense and respond to their environment have obvious ties to security systems, public affairs, and psychological operations. Nanobots that can interact with and manipulate the human body have direct connections to enhancing capability and survivability of the individual Soldier, Sailor, Airman, or Marine, a prospect that also leads the reader to obvious ethical considerations.

Nourbakhsh concludes by examining the ethical aspects of robotic technology and how it should be approached. More specifically, current research and funding provide more capability and power to institutions at the expense of societal concerns (p. 110). We must purposely drive this balance back in favor of societal needs if we wish to see the full benefit of this emergent technology. Although this line of discussion

is obviously important, given the implications suggested by the examples, it still seems a bit out of place—for two possible reasons. First, the author's rich examples and technical discussion draw the reader into intuitively considering the ethical implications of the technology. Therefore, having a separate discussion or chapter on the subject almost strikes the reader as redundant. Second, Nourbakhsh effectively addresses the issue in the fictional accounts, making an additional chapter dedicated to the ethical construct seem somewhat unnecessary. In the end, though, one can understand why he felt compelled to include this discussion so that readers arrive at a common conclusion.

Any student of air and space power will find *Robot Futures* an outstanding piece of work. A leader in the field, the author is perfectly positioned to observe the glide path for this technology. All readers, regardless of their familiarity with the subject, will easily grasp this rich, well-supported material. Finally, and perhaps most importantly, Nourbakhsh's broad forecasting allows individuals from multiple communities of interest to apply the information presented.

Lt Col Thomas P. Allison, USAF
US Air Force Academy, Colorado

Black Sheep: The Life of Pappy Boyington by John F. Wukovits. Naval Institute Press (http://www.usni.org/store/books), 291 Wood Road, Annapolis, Maryland 21402, 2011, 288 pages, $34.95 (hardcover), ISBN 978-1-59114-977-4; 2013, 288 pages, $22.95 (softcover), ISBN 978-1-59114-980-4.

Col Gregory "Pappy" Boyington, one of the most colorful, controversial, and complicated characters in military history, is considered a cult hero by some and a pariah by others—an irreplaceable leader or a liability as a follower. Regardless of his place in history, Boyington undoubtedly left an indelible mark on the American military landscape. *Black Sheep* by John F. Wukovits paints a complete and unbiased picture of this man.

The author begins framing Boyington's character by detailing his difficult upbringing, focusing on his quest to find acceptance—a reoccurring theme in this book. Boyington had a series of abusive father figures and, for all practical purposes, an absent mother. To complicate matters further, he did not even find out who his real father was until he left home. Aviation became his first outlet for acceptance, and Boyington used the heroes of early aviation as role models to replace the ones from home.

Boyington's quest to find his rightful place in society continued into his early adult life. Factory work proved unsatisfying, and college sports merely provided an outlet for his pent-up aggression. Even his early time in the Marine Corps was riddled with failure, insubordination, and alcohol abuse. Though his skills as an aviator forecasted a promising career, his personal and professional troubles led him to join the famed American Volunteer Group (AVG) in an attempt once again to restart his life, looking for some acceptance.

Disappointment after disappointment characterized his time with the Flying Tigers. Boyington always seemed to miss out on the action, a problem that he attributed to the disdain that Flying Tiger leader Claire Chennault had for him. Furthermore, leadership opportunities eluded Boyington—further evidence, at least in his own mind, that everybody was out to get him. As his time with the AVG ended, Boyington fought hard to get back to the Marine Corps, where he thought he could be appreciated and accepted.

The timing of his return to the Corps could not have been more perfect. Shortly thereafter, he found himself in command of the famed Black Sheep Squadron—a perfect fit for the prodigal son, who finally got his opportunity to lead, and his men unhesitatingly followed. Boyington led by example, shielding his men from outside distractions so they could concentrate on dominating the air in the South Pacific. He and his Black Sheep compiled an unmatched record in the mere 84 days that his squadron was on the front. After spending some time as a prisoner of war, Boyington returned to civilian life. But the same troubles

that had haunted him before reappeared, stymieing a lucrative postwar career that awaited him as a Medal of Honor recipient and war hero.

Wukovits's depth and breadth of research into the life of Pappy Boyington are remarkable. Rather than solely focusing on his subject's exploits, the author paints a picture of the man from all angles. It is no secret that Boyington had his faults, but one must first understand them in order to appreciate his successes. Wukovits pulled stories of Boyington from a variety of first-person accounts, both complimentary and caustic—an analysis that this reviewer considers completely objective. Readers can draw their own conclusions and judge him without any implied bias from the author. Furthermore, Wukovits makes the book easy to read by dividing Boyington's story into manageable, digestible vignettes.

Boyington's story is an important one for Airmen to know and understand. He was the classic disillusioned follower who faltered when confronted with incompatible leadership styles. Had his early leaders understood Boyington's potential, he could have experienced success much earlier—evidenced by his achievements in leading the Black Sheep Squadron as his superiors recognized and molded his talent. Boyington's story also offers an example of how a disillusioned follower can hamper his own potential by entering a downward spiral of self-pity rather than finding areas where he can contribute, regardless of how small the contribution may seem. Lastly, the success of Boyington and his Black Sheep allowed them to modify their tactics by going on the offensive with airpower. This development changed the strategy of the air campaign in the South Pacific for both the Americans and the Japanese, turning the tide of the war and demonstrating how tactical success can have far-reaching strategic implications.

Although Boyington failed miserably as a follower, his leadership proved vital not only to the men of the Black Sheep Squadron but also to the air campaign in the South Pacific. Regardless of Boyington's triumphs, some individuals cannot see past his well-documented failures.

As Wukovits puts it, however, success as a leader is measured not by that leader or his superiors but by those he leads (p. 144).

Maj Nicholas Foster, USAF
Seymour Johnson AFB, North Carolina

Find, Fix, Finish: Inside the Counterterrorism Campaigns That Killed Osama Bin Laden and Devastated Al-Qaeda by Aki Peritz and Eric Rosenbach. PublicAffairs (http://www.publicaffairsbooks.com/), 250 West 57th Street, Suite 1321, New York, New York 10107, 2012, 320 pages, $27.99 (hardcover), ISBN 978-1-61039-128-3; 2013, 320 pages, $16.99 (softcover), ISNB 978-1-61039-238-9.

Find, Fix, Finish is a behind-the-scenes look into the counterterrorism campaign waged since 12 September 2001, the day after al-Qaeda attacked the United States of America. This campaign ultimately led to the capture of Osama bin Laden and continues into the present day. The authors argue that prior to the attacks of 11 September 2001 (9/11), the United States lacked a comprehensive strategy and the capabilities to disrupt terrorist networks from a counterterrorism perspective. The book offers a microlevel account of the policies adopted and then executed by the Bush and Obama administrations, detailing how this doctrine, although at times controversial, shaped the new battlefield—one not often seen or reported on the nightly news.

The coauthors have a substantial background in the subject. Aki Peritz, a senior national security adviser for the Third Way think tank, attained this position after several years of working at the Central Intelligence Agency's (CIA) Counterterrorism Center. Prior to assuming duties as a deputy assistant secretary of defense, Eric Rosenbach taught counterterrorism at the Harvard Kennedy School and served as a staff member for the Senate Select Committee on Intelligence, where he led oversight of US counterterrorism programs. Due to the nature of the information contained within the book, it underwent several prepublication reviews—including one by the CIA. Consequently, some

portions are redacted, indicating that it once contained sensitive information not suited for publication. In the reviewer's opinion, the redacted text does not detract from either the book's content or its ability to accurately reveal details of the events.

The book begins by defining the find-fix-finish cycle: find the enemy, ensure that he stays in that location, and then defeat him (p. 4). Most of our society's focus is on the "finish" aspect because that remains the most commonly reported portion during a news cycle and because that is where the action is. However, Peritz and Rosenbach do a nice job illustrating that the "find" and "fix" elements are critical pieces of this cycle. Without these cultivation steps, the "finish" does not happen.

The coauthors present several case studies on the hunt, capture, or killing of high-value targets, including Khalid Sheikh Mohammed, the accused mastermind of the 9/11 attacks. Moreover, they discuss how the United States quickly realized that al-Qaeda's number-three commander was filling the role of operations director. This revelation led to a systematic dismantling of the terrorist organization's infrastructure by directly targeting the individual(s) holding that position, thus crippling al-Qaeda's ability to conduct substantial operations.

Peritz and Rosenbach also offer significant details about some of the most controversial security policies implemented since 9/11, including the use of enhanced interrogation methods on high-value detainees, the employment of remotely piloted aircraft to conduct targeted killings, and the housing of detainees at Guantanamo Bay, Cuba. Interestingly and most timely in relation to current events, they also examine the use of roving wiretaps via the Foreign Intelligence and Surveillance Acts (FISA) and the use of FISA courts to authorize the monitoring of electronic communications related to the surveillance of international terrorist suspects (p. 173).

The book relates the lead-up to and execution of the mission that killed Osama bin Laden. To their credit, the coauthors abstain from tying individual administration policies to the event's success to avoid injecting partisanship into the discussion. They frame the book to ade-

quately capture the achievements of the years leading up to the operation along with the dismantling of interagency barriers, political leadership, and pure chance. Peritz and Rosenbach conclude with some lessons learned that could serve as foundations for future strategy planning and policy making in this realm, based on events that have unfolded over the past decade.

In aggregate, *Find, Fix, Finish* resembles a scholarly text, presenting several case studies throughout. Given the amount of detailed and potentially controversial material, the coauthors do an exceptional job of citing their sources, offering a bibliography that runs to more than 40 pages. The material presented is impressive, but this publication is not for novice readers, who, for example, may have difficulty keeping track of the many foreign names identified and subsequently referenced throughout the events depicted in the book's case studies. However, the work should prove useful to experienced readers with a significant interest in defense, counterterrorism, foreign relations, and/or government policy. A minor criticism is that the text contains some misspellings and out-of-place wording (p. 218)—surprising in light of the number of reviews it underwent prior to publication. Overall, though, *Find, Fix, Finish* is a highly recommended and educational behind-the-scenes study by two individuals close to this side of the fight.

Capt Jason S. Henderson, USAF
Osan AB, Korea

Rockets and People, vol. 3, **Hot Days of the Cold War** by Boris Chertok. Superintendent of Documents, US Government Printing Office (http://bookstore.gpo.gov), Washington, DC 20402-0001, 2009, 832 pages, $79.00 (hardcover), ISBN 978-0-16-081733-5. Available free from http://www.nasa.gov/pdf/636007main_RocketsPeopleVolume3-ebook.pdf.

Rockets and People, Boris Chertok's seminal series, serves as a de facto report on the Soviet space program from its inception through the moon race of the late 1960s. Volume 3, *Hot Days of the Cold War*, begins with

the efforts toward manned spaceflight and traces the evolution of the Soviet Voskshod, Vostok, and Soyuz manned spacecraft and their variants (i.e., the Zenit-2 photoreconnaissance satellite). Additionally, Chertok covers the first Soviet communications satellite and its intrepid orbital design, the so-called Molniya ("lightning" in Russian), with gusto and aplomb. The final focus of volume 3 chronicles Chertok's interaction and friendship with Sergei Korolev, chief Soviet rocket designer.

The fact that an analogous Western memoir would have to contain the (observed) words and thoughts of Dr. Wernher von Braun, Dr. James Van Allen, Dr. Joseph Charyk, Gen Bernard Schriever, and Lt Colonel Ed Hall, to name just a few, gives future readers some idea of the breadth of this volume. Chertok's chapters are chronological, varying widely with the memoir's thread that holds the piece together. Of specific interest to Air Force space professionals, aside from the stories of Yuri Gagarin's derring-do and Gherman Titov's spacewalking exploits, are the chapters on strategic systems: missiles and satellites. Chapters 4 and 5 ("The Cuban Missile Crisis . . . and Mars" and "Strategic Missile Selection," respectively) tie the space race into the greater context of the Cold War. Anecdotal stories about the failures of the R-7 booster and R-9 missiles on the launchpad—or directly above it—and design frustrations with antiballistic missiles set up the reader for the mirror story of the well-publicized American nuclear combat systems. Stepping back from the emotional highs of space exploration, the reader is slapped into reality regarding why these systems existed in the first place.

In this reviewer's fully admitted job-induced tunnel vision, the highlight of the book is the development of the first Soviet reconnaissance and communication satellites. Recounting the creation of the Zenit-2 series of photoreconnaissance satellites completes the puzzle of Cold War silent sentinels whose intelligence "takes" shaped the decisions of leaders on both sides of the Iron Curtain. These exploits, from the side of the American Central Intelligence Agency (CIA) and the National Reconnaissance Office (NRO), have been celebrated since the release of the Corona, Argon, and Lanyard satellite records in 1995. Information

about Zenit-2 has trickled out slowly to the rest of the world through professional space journals and books like Chertok's. His holistic view of rocket, payload, designer, and outside political forces within the Zenit-2 program equals the strides taken in Curtis Peebles's *The Corona Project* but not the programmatic details of Frederick Oder's *The Corona Story*—the de facto chronology from the CIA and NRO. Anecdotes of the design of the Molniya-1 communications satellite also colorize the story behind the engineers and scientists whose work remained relatively unknown during the Cold War years.

Confusing nomenclature constitutes one major drawback of *any* account translated from the original Russian government documents. Perhaps intentionally obfuscating, the differences between a 1KP spacecraft and 1K (a Vostok without and with a life-support system, respectively) can get confusing quickly, along with design bureau designations (OKB-1 versus OKB-2, compared to NII-88, for example) and their chief designers. Die-hard students of the Soviet space program may breeze through this with ease whereas casual readers may not. In defense of the author's native language, the index does list the North Atlantic Treaty Organization's reporting names of ballistic missiles and rightfully orients the reader to their Soviet designations.

In any memoir, the fading of time and memory is a given, and errors within are wholly expected. One can check factual information against records and other sources. Similarly, Asif Siddiqi, editor of the *Rockets and People* series, did an amazing job of marrying the ocean of knowledge from published Western sources to Chertok's reminiscences. The effort is almost seamless, with a cornucopia of footnotes interspersed throughout; however, the notes themselves are not without error. Siddiqi footnotes Chertok's description of the "CIA's [spy satellite] initiative," later known as the Discoverer/Corona series (p. 18), with "The first successful recovery of a Discoverer reentry capsule was in August 1960 during the Discoverer 14 mission." In reality, it was "lucky" number 13 (*Discoverer XIII*) that returned the first reentry capsule on that date.

Although readily dismissed as a typographic error, this and other minor hiccups are not enough to detract from Chertok's memoir.

Future memoir writers of the US space program's multiple entities would do well to read one tome from Chertok's series, all of whose volumes are easily categorized into the realm of a space geek library's "must haves." The macroscopic lessons from *Hot Days of the Cold War* unearth truths inside the management of overly complex enterprises and provide moments of levity with anecdotal tales of celebratory vodka and cognac flowing in the wake of overwhelming successes. Boris Chertok's writing will entertain a wide variety of readers—those brave souls not easily deterred by the overwhelming 754 pages of text!

Maj Joseph T. Page II, USAF
Joint Space Operations Center
Vandenberg AFB, California

In the Gray Area: A Marine Advisor Team at War by Seth W. B. Folsom. Naval Institute Press (http://www.usni.org/store/books), 291 Wood Road, Annapolis, Maryland 21402, 2010, 256 pages, $34.95 (hardcover), ISBN 978-1-59114-281-2.

In the Gray Area by Lt Col Seth Folsom, USMC, is an informative, insightful, and timely memoir of his experience as a military advisor to the Iraqi army in 2008. He references his personal journal to bluntly and candidly recount the numerous frustrations and occasional triumphs that a growing number of military members can relate to: trying to train members of a vastly different culture to function as a Western-style military.

The work has dark overtones as the advisors of Military Transition Team (MiTT) 0733, the "Outlanders," struggled daily with their Iraqi counterparts. Folsom recalls the difficulties of dealing with the corruption and occasional incompetence of the newly reconstituted Iraqi army and its leadership in particular. As the Outlanders' commander, he explores his personal fears and exasperation that the Iraqi military would never be able to operate without direct US support. The dark

sense of humor that the Marines developed to cope with the situation is conveyed throughout the book and helps the reader understand what it is like to train members of a vastly different culture in the difficulties not only of fighting a war but also of training, equipping, and maintaining a military. In the end, Folsom asks difficult questions about whether his team's and other MiTT teams' sacrifices were worthwhile. He concludes that the answers may not be the ones the US military desires, but they provide an honest analysis of the situation from someone who was there.

This memoir does not break new ground in military history, but the author's story offers a meaningful examination of a little-considered aspect of warfare. The number of military advisors is growing in every service, and—as with past conflicts—their stories are seldom told or understood by the general public or even history buffs. This work will appeal to anyone trying to understand the US military's attempts to build competent forces in countries like Iraq and Afghanistan. Anyone who has served as a military advisor or even worked with foreign forces will also appreciate Folsom's work and chuckle at his team's experiences and frustrations.

Perhaps the greatest praise for *In the Gray Area* comes from my recommendation that any Air Force or other military member preparing to deploy as a military advisor should read it. Although no two cultures or experiences will ever be the same, Folsom's stories will help prepare someone for the myriad difficulties an advisor will encounter.

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

Sword and Shield of Zion: The Israel Air Force in the Arab-Israeli Conflict, 1948–2012 by David Rodman. Sussex Academic Press (http://www.sussex-academic.com/), P.O. Box 139, Eastbourne BN24 9BP, United Kingdom, 2013, 168 pages, $50.00 (hardcover), ISBN 978-1-84519-583-0.

Without pretending to examine the actions of the Israel Air Force (IAF) completely and exhaustively, David Rodman's *Sword and Shield of Zion* manages to discuss in some detail the broad and important scope of its activities in military and humanitarian affairs. The book addresses how the IAF succeeded in its four main combat roles (air superiority, close air support, interdiction, and strategic attack) as well as four noncombat functions (troop transport, casualty evacuation, logistical support, and reconnaissance), focusing most of its attention on the time after the 1956 Suez War. During this period, the IAF began to give Israel a major advantage in combat against its hostile Arab neighbors.

Organized efficiently and effectively, the book first introduces Israeli national security and national airpower matters and then comments on the support role of Israeli airpower and the Arab-Israeli conflict before taking up its principal subject. Rodman also discusses how the IAF has helped Israel win diplomatic recognition through its humanitarian efforts after natural and man-made disasters in a way that simultaneously allows the country to maintain its capacity to deal with potential conflicts. After reviewing airpower and maneuver warfare in the Six-Day and Yom Kippur Wars, the author then turns to Israel's dependence upon the IAF for attritional conflicts against Egypt (1969–70), Hezbollah (2006), and Hamas (2008–9), concluding that decisive results required the Israel Defense Forces to provide ground troops and that dependence on the IAF alone produced stalemates. He then comments at some length on airpower, counterinsurgency, and special operations that take place between major wars and that form part of the day-to-day duties of the IAF, showing that its role in such matters began in the 1960s and has become more important. Rodman then hints at the significance of the IAF's remotely piloted aircraft (RPA) before

closing with a discussion of ground-based air defense, space-based reconnaissance, and the infrastructure of the IAF; he also comments on its past and future contributions to the well-being of Israel as a whole (and, to a lesser extent, the world at large).

Despite the fact that *Sword and Shield of Zion* uses a fair amount of military jargon, it remains accessible to both general readers attracted to military history or issues of grand strategy and to those concerned with the confluence of tactics and political goals as well as Israel's particular interest in logistics and attacks on its enemies' logistical capabilities. All readers will be especially intrigued by the author's broad hints about the advanced capabilities of Israel's RPAs (popularly known as drones) and the possibility that it possesses the means to use satellites in an attack role in future conflicts—areas in which the IAF desires to employ its indigenous military capabilities for deterrence.

One should also note that this book, though critical of some aspects of Israel's political and military behavior (especially with regard to its leadership), staunchly supports the larger aims and goals of the nation's military. From its use of pro-Israel terms for territory (e.g., *Judea* and *Samaria* instead of *West Bank*) to its firm labeling of Hamas and Hezbollah as terrorist organizations, it makes no pretense of being unbiased but openly and unabashedly assumes a pro-Israeli perspective. Consequently, Rodman paints an essentially favorable picture of the IAF and its role in preserving both Israeli security and the safety of the Jewish people (historically done through airlift operations like those that brought the Falasha Jews of Ethiopia to Israel in the 1980s and 1990s), as well as helping Israel in its diplomatic ambitions through extensive humanitarian aid in such diverse locations as Turkey, Mexico, India, Japan, and Haiti.

A slim but detailed volume containing a striking amount of analysis of the function and importance of the IAF in the overall defensive strategy and capabilities of the state of Israel, *Sword and Shield of Zion* will be of considerable interest to students of airpower. It reveals not only the immense capability of a well-developed nation to defend itself

and control battlefields in enemy territory but also the limitations of airpower in achieving strategic and political goals without employing ground troops against determined opposition. The book should also appeal to those who study revolutions in military affairs—especially its revealing intimations about Israel's drone capabilities. A close reading will prove rewarding in terms of understanding the prowess and strategic doctrine of the IAF. Clearly, anyone who has an interest in the IAF and its activities will find *Sword and Shield of Zion* worthwhile.

Nathan Albright
Portland, Oregon

Breach of Trust: How Americans Failed Their Soldiers and Their Country by Andrew J. Bacevich. Metropolitan Books, Henry Holt and Company (http://www.henryholt.com), 175 Fifth Avenue, New York, New York 10010, 2013, 238 pages, $26.00 (hardcover), ISBN 978-0-8050-8296-8.

Prof. Andrew Bacevich pulls no punches in *Breach of Trust* as he argues for a return to the military draft system. He draws a sharp distinction between the "citizen-soldier" of World War II, Korea, and Vietnam, and the "warrior professional" of Iraq and Afghanistan. Such a distinction clarifies his point: When going to war means putting the populace in harm's way, the populace will be reluctant to go to war, and such reluctance may be just what a post–Cold War United States needs.

Although the author has ammunition enough to blame Congress, multiple presidents, the citizenry, senior military officers, many secretaries of defense and state, think tanks, pundits, and "Washington" in general, he levels his primary accusation against the American people. Bacevich posits that the all-volunteer force has resulted in "three no's" emanating from the populace: (1) we will not change, (2) we will not pay, and (3) we will not bleed. Insofar as these criteria are met, the people will coalesce to "Washington's war." The only solution to this problem is to "repeal the three no's. . . . Only [when Americans have

skin in the game] . . . can they expect to have any say in how (and whether) the game gets played" (pp. 190, 191).

Andrew J. Bacevich, a retired Army colonel who holds a PhD from Princeton, is a professor of international relations and history and chair of Boston University's International Relations Department. Clearly, he is supremely qualified to take on the project of assessing US domestic military policy from World War II to the present. Indeed, his critical eye and expansive research draw from the last 60 years both the causes and effects of President Nixon's abolishment of military conscription.

The book makes four claims. After Vietnam the American people (1) abandoned the tradition of the citizen-soldier, (2) promoted the model of the warrior professional, (3) embraced militarized globalism, and (4) allowed for "contractor encroachment on matters that soldiers had once claimed as their own" (p. 137). *Breach of Trust* argues for and expands upon these four assertions.

Bacevich's presentation of post–World War II American history is thorough and informative, but his position on conscription is weakened by hyperbole and incendiary language. What otherwise would have been a convincing, rational argument sinks too often to an overly rhetorical one. By way of example, he asserts that, leading up to 9/11, a *perception* existed that the Greater Middle East had become an "incubator of radicalism" (p. 165), without addressing whether that perception reflected reality. Similarly, in response to Gen Carter Ham's claim that US Africa Command's mission includes "sustained engagement," Bacevich translates "engagement" to "preparing for war" (p. 169). Again, in acknowledging that a drafted Army may perform less competently than the current one, Bacevich glibly remarks that "crewing a tank or an artillery piece, [and] conducting patrols or ambushes are not rocket science" (p. 192), without acknowledging that conducting them *well* is, in fact, challenging. Further, conducting them well limits the collateral damage he bemoans 15 pages earlier. He chooses the term *assassination* to describe President Obama's remotely piloted air-

craft campaign while failing to recognize the legal distinction between *assignation* in peacetime and *targeted killing* in time of war. In these cases and many others, the author sacrifices clear and effective deliberation for appeals to emotion and cynicism.

Congress does not escape criticism. Bacevich has, in fact, modified the classic pejorative to include that body in the "military-industrial-*congressional* complex" (emphasis added) (p. 190). "For those who ride the gravy train," he writes, "doing what's necessary to keep it rolling takes precedence over contemplating . . . the wreckage left in its wake" (p. 124).

Certainly some of his points are valid, but it takes a great deal of care to determine which ones. After being subjected to a barrage of clever, loaded language and ad homonym caricatures, one ends up taking even the straightforward language with an ample dose of skepticism. This is not to mention the fact that for all his emphasis on conscription, Bacevich does little to counter his known opposition. Those in favor of an all-volunteer force will suggest that draftees cannot do the job as well as volunteers. The author seems to dismiss this claim with a wave of the hand. Fighting wars is "not rocket science," after all. I would have preferred a good deal more discussion and analysis on this particularly sticky point.

The shining light in the case for conscription comes through Bacevich from Gen George C. Marshall (later secretary of state and defense). War conducted by a professional warrior class "is a criminal doctrine. . . . There must not be a large standing army subject to the behest of a group of schemers. The citizen-soldier is the guarantee against such a misuse of power" (pp. 195, 196).

All told, *Breach of Trust* is an important read for any active, Reserve, or Guard member. Those of us in the all-volunteer force tend to have a conditioned response against conscription. As unpopular as the idea is, Bacevich offers a rare voice in its favor. It is incumbent upon those who serve to wrestle with this issue and determine for themselves

whether the United States stands to benefit from such a significant change.

Capt Joseph O. Chapa, USAF
AFIT Graduate Student
Boston College

Boeing B-17 Flying Fortress: Owners' Workshop Manual, 1935 Onwards (All Marks) by Graeme Douglas. Zenith Press (http://www.zenithpress.com), 400 First Avenue North, Suite 300, Minneapolis, Minnesota 55401, 2011, 160 pages, $21.00 (hardcover), ISBN 9780760340776.

Writing a book touted as an *Owners' Workshop Manual* for an aircraft that, according to author Graeme Douglas, has reached "something of an iconic status" (p. 9) certainly would not be easy. Douglas, however, proves himself equal to the task. *Boeing B-17 Flying Fortress* is part of a series of aircraft books released by the original British publisher (Haynes Publishing). Anyone hoping to own and operate a B-17 will certainly require a good deal of information about it. Douglas does not claim to have written an all-encompassing study of the four-engine bomber; rather, he uses his more than 30 years of experience as both a B-17 ground-crew member and volunteer restorer to give readers rare insight into today's challenges of flying and maintaining this aircraft.

To tell the story of the legendary Boeing B-17, the author divides his monograph into four main areas: the bomber's development, its use in combat, technical aspects, and details about operating and sustaining B-17s that have survived. In 1934 the Boeing Company financed development of a four-engine platform as its entry in the Army Air Corps (AAC) competition for a new bomber. Known as the Model 299, the aircraft performed well but was eliminated from competition when the test version tragically crashed after the pilots failed to remove the control locks before takeoff. Fortunately, the AAC recognized the 299's superior performance and signed a contract with Boeing for 13 test-and-development aircraft, thus marking the birth of the B-17. Douglas then

briefly discusses the major models (B through G) and assorted unique variants (e.g., transport, photoreconnaissance, and special mission).

Beginning with the British Royal Air Force's initial efforts to use the B-17 to bomb Fortress Europe, the author examines the aircraft's combat experience in both the European and Pacific theaters, dedicating an entire chapter to the events of a typical mission and including a wealth of photos of B-17 crew members manning their positions. He then turns to the heart of the book: a technical assessment of both the B-17's anatomy and its four powerful Wright Cyclone engines. Beginning with the fuselage, Douglas describes the major components—heavily supplementing the text with both photographs and technical drawings—and addresses system operations, including any wartime changes made to the system. Though specialized, the author's approach does not alienate readers who lack a strong technical background.

Douglas concludes his work by reviewing the challenges of maintaining two surviving B-17Gs—the *Mary Alice* and the *Pink Lady*. After a nearly 20-year restoration effort, the *Mary Alice* is on display at the American Air Museum at Duxford, England. Indeed, the author helped restore the bomber to its present status as one of the "faithful and fully equipped examples of a static Fortress" (p. 115). Until its recent retirement, the *Pink Lady* was one of only two B-17s flying in Europe and the only potentially airworthy variant that had seen combat. After relating its aircrew's experiences flying this vintage B-17 on the modern European air-show circuit, Douglas concludes with a discussion of current maintenance procedures.

As one might expect of a book of only 160 pages, the degree of detail is somewhat deficient. To compensate, the author includes numerous insightful inset articles that provide considerable information on topics ranging from the seemingly trivial (Boeing's part-number system and instructions for reading an aircraft data block) to the essential (the B-17's technical specifications, the Norden bombsight, or the *Pink Lady*'s combat history). Finally, a large number of both historical and present-day pictures and diagrams serve as an excellent complement to the text.

The author has made a solid and enjoyable contribution to the vast number of books about the B-17 Flying Fortress. Inclusion of *Owners' Workshop Manual* as a subtitle is a marketing ploy that no book of this length can fully live up to. That point aside, Douglas's blending of broad-brush discussions and detailed sidebars of specific topics works well. Furthermore, the photos and technical diagrams accent and clarify the text. Clearly, this book does not target members of the academic or engineering communities; rather, it is intended for readers who want to know more about the technical aspects of the B-17. In that regard, *Boeing B-17 Flying Fortress* definitely delivers bombs on target.

Lt Col Dan Simonsen, USAF, Retired
Bossier City, Louisiana