ASPJ
Air & Space Power Journal

September–October 2013
Volume 27, No. 5
AFRP 10-1

Senior Leader Perspectives

Features

Military Space

At a Strategic Crossroad

Gen William L. Shelton, USAF

The future of space capabilities in the United States Air Force is at a strategic crossroad. A crossroad that requires us to address our means of protecting mission-critical constellations, to challenge traditional acquisition practices, to analyze new operational constructs, and to widen cooperative relationships both domestically and abroad. Our military satellites are technological marvels providing time-critical global access, global persistence, and awareness. These systems not only provide foundational, game-changing capabilities for our joint forces, they also have become vital assets for the global community and our world economy. Dependence on these space capabilities gives our nation a great advantage—an advantage some would like to minimize. Satellites designed and built for a benign environment are now operating in an increasingly hostile domain. The challenge before us, then, is to assure these vital services will be present in times and places of our choosing while simultaneously lowering the cost.

The Air Force has been in continuous combat operations since January 1991, when Operation Desert Storm commenced. It seems hard to believe now, but Global Positioning System (GPS) receivers were literally duct-taped to windscreens of helicopters to capitalize on the nascent navigation capability provided by the not-yet-completed GPS constellation. Similarly simplistic was the voice-only provision of missile warning data to our deployed forces and allies to warn them of Iraqi Scud missile launches. We learned much in the early 1990s about the need to further integrate space capability into tactical operations.

For example, the utility enhancements of our GPS constellation have enabled us to develop real-time integration with the war fighter. Our GPS User Operations Center provides over 230 position accuracy assessments to our deliberate and contingency mission planners daily. Our space-based infrared system (SBIRS) is also a significant improvement over our capabilities in the first Gulf War. The infrared processing of SBIRS GEO-1 and -2 presents the war fighter with faster and more accurate launch information and impact-point predictions, and the SBIRS staring sensor will enable tremendous enhancements to our battlespace awareness.

The entire joint force is now dependent on space assets for all operations, ranging from humanitarian relief through major combat. Space-derived data, once the purview of strategic-level users only, now reaches to the lowest tactical echelons. But with this dependence comes a corresponding vulnerability.

As we learned in the crucible of combat, others were watching and learning lessons of a far different kind. As we continue to take significant strides in the integration of space-enabled data into all aspects of operations, our adversaries seek ways to disrupt this asymmetric advantage. The most obvious example of these counterspace efforts is the Chinese antisatellite test in 2007. In this test, a kinetic-kill vehicle successfully engaged a nonoperational Chinese weather satellite. Although China demonstrated its ASAT prowess to the world, the unfortunate by-product of this test is tens of thousands of pieces of space

debris which will be a navigation hazard to manned and unmanned spacecraft for decades to come.

The growing debris problem is a concern to spacecraft operators in all sectors: military, civil, and commercial. The collision between an active Iridium communications satellite and a defunct Soviet-era Cosmos satellite produced yet another debris field. These were two relatively large objects coming together at precisely the wrong time. Much smaller objects, which are much greater in number, also represent catastrophic risk to fragile spacecraft. Therefore, the potential exists for further collisions, creating a cascading effect of increasing debris in low Earth orbit. We must control debris creation, and we must increase our ability to track the debris to enable collision avoidance when possible.

Another troublesome development is the proliferation of jamming assets. GPS jammers are widely available, complicating our employment of GPS navigation and timing signals in weapons and platforms. Satellite communications jammers also are plentiful, which impairs our confidence in over-the-horizon communications when we would need it most.

Other threats to our space capabilities either exist or are being actively researched, so the broader point is that increasing counterspace capabilities, combined with a growing debris threat, make the space domain a much more hostile place. Therefore, it should be obvious that we cannot expect space assets designed to operate within a very permissive environment to operate effectively in this "new normal" of a challenged space domain.

The other important factor defining the strategic crossroad is the downturn in the budget. While there is substantial uncertainty in the actual budget figures for the future, it is very safe to say the peak budgets are behind us. If we are to continue providing foundational space services for our war fighters, we must look for less expensive alternatives to our current systems.

It's instructive to look first at how we arrived at the decisions to build highly complex, expensive satellites. Because the cost of launch

is so high, our business-case analyses told us that we gained highest efficiencies by packing as much capability as possible onto each satellite. Tightly packaged and integrated satellites, such as the SBIRS and the advanced extremely high frequency (AEHF), were borne of this design philosophy. Additionally, in both of these examples, we pushed hard on advancing certain technologies, resulting in significant, nonrecurring engineering costs—and corresponding program delays. Those development challenges are behind us, but even the production models of these spacecraft, bought under more efficient acquisition frameworks, still are very expensive.

Either of the two key factors cited—a radically different operating environment and a declining budget—should be a shouting mandate for change. When we combine these factors at this epoch in time, however, it should be obvious that a status quo approach is simply inadequate for our future. To sustain space superiority and the space services our joint force now takes for granted, we must consider future architectural alternatives. These alternatives must balance required capability, affordability, and resilience.

Resilience in the face of the previously discussed growing space threats is an imperative. If space assets come under attack, either as a precursor to conflict or as an integral part of terrestrial hostilities, our architectures must be resilient enough to assure mission accomplishment. Maintaining a fragile-by-design architecture, which is vulnerable to a golden BB, could result in the loss of a critical resource when we need that capability the most. For example, the AEHF satellites are designed to operate in extremis—in a trans- and post-nuclear environment to enable the National Command Authority to command and control forces necessary to ensure national survival. As currently envisioned, we will procure just enough of these satellites to provide a minimal constellation with no resiliency to attack. Just as we would have trouble with a cheap shot, we also are not resilient to premature failure of a satellite in the constellation. Building replacement satellites takes years, and the high cost precludes spares on the shelf.

While we could merely buy more of the same designs to provide the needed resilience, we are studying much less expensive concepts. The first is called disaggregation. Again using the example of AEHF, both strategic and tactical protected communications payloads are hosted on the satellite. As a result, the satellite is both large and complex—and size and complexity are drivers of cost in both design and launch. Separating the two payloads on different satellites would accomplish three things: (1) the complexity would decrease, thereby driving down the cost; (2) the satellites would be smaller, enabling smaller boosters and driving down the cost; and (3) at a minimum, the adversary's targeting calculus would be complicated with more satellites, thereby producing at least a modicum of resilience in the face of intentional acts. Another potential advantage of disaggregation is the ability to host payloads on other platforms, including commercial satellites. The Commercially Hosted Infrared Payload has been a trailblazer in this regard, and much more work with industry is already under way.

We have learned that the commercial enterprise, which can integrate military payloads and the acquisition process to get capability into space, is both flexible and affordable. We continue to look into other pathfinders and have engaged in industry outreach to discuss ways to better partner and apply synergies within this rapidly evolving domain.

A disciplined adherence to high technological readiness-level hardware also is required to make this approach affordable and achievable. Technological refresh will prove necessary in some areas as we approach these alternatives, but there is no reason today to push technology as hard as we have in the past. Space Modernization Initiative (SMI) funds will help mature sensor designs, communications packages, and software, which then allows for wiser choices in the actual development programs for these alternatives. These SMI funds must be protected in future budgets to better equip program managers with design alternatives.

As we contemplate smaller satellites and smaller boosters, we can also consider using commercial, off-the-shelf satellite buses rather

than building specialized buses for each of our spacecraft. This also opens the window for commercial software to fly those buses, avoiding software and ground station development efforts for each new spacecraft. Clearly, we would still require payload-related software, but the simplicity and cost-savings of buying both off-the-shelf buses and ground software are worthy of exploration.

Because spacecraft production timelines are long, the lead time on decisions is correspondingly long. The die is already cast for SBIRS 5 and 6 as well as AEHF 5 and 6. Assuming these spacecraft achieve their required lifetimes, replacement spacecraft are not needed until the mid-2020s. However, that also means decisions on these replacements must be made in the 2017–2018 time frame. Budgetary decisions on an architectural direction, then, must be made in 2015 or 2016.

Clearly, the theories of providing required capability with enhanced resilience at a reduced cost will be rightly debated in the coming months. The Space and Missile Systems Center has several study efforts under contract today to produce empirical data to inform this debate. A business case analysis is absolutely required. A technological feasibility determination is needed. But the signs all point to a good marriage of affordability and resilience while procuring required capability.

Augmentation of some key mission areas through international partnerships can help relieve some of the budget pressure and strengthen strategic international ties. Building partnerships increases capacity and shares the responsibility for international security. For example, significant work in the area of protected and survivable satellite communications has been ongoing with Canada, the Netherlands, and the United Kingdom. Australia has committed to participating in the Wideband Global Satellite Communications program, as well as hosting sensors important to our Space Situational Awareness capability. Our international cooperation and partnership with industry increases our capacity, improves our capability, shares in the cost burden, and helps extend global presence.

Much work remains, but time is short. A fundamental restructuring of our space architecture is under consideration, and opinions will be offered from many quarters. But given the new normal in space, given the new budget climate, isn't it good common sense to look at alternatives to the status quo? Let's protect our SMI funds, let's do the hard study work, and let's have the data do the talking.

In this century, we face a growing number of nations with near-peer or peer capabilities, which may challenge our notions about space superiority. In order to maintain our edge, we must continue to lead in space innovation. Tomorrow starts with the vision we develop today. We must capitalize on the present opportunity to reshape the space environment, sustain global capabilities, and continue our asymmetric advantage in space. ✪

Gen William L. Shelton, USAF

General Shelton (USAFA; MS, Air Force Institute of Technology; MS, National War College) is commander of Air Force Space Command, Peterson AFB, Colorado. He is responsible for organizing, equipping, training, and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, US Strategic Command, and other combatant commands around the world. General Shelton not only oversees Air Force network operations and manages a global network of satellite command and control, communications, missile warning, and space launch facilities but also has responsibility for space system development and acquisition. He leads more than 42,000 professionals assigned to 134 locations worldwide.

Let us know what you think! Leave a comment!

Space Acquisition Issues in 2013

Lt Gen Ellen M. Pawlikowski, USAF

Space systems acquisitions for national security have always been very challenging. It literally is rocket science! Our ability to truly leverage the advantages that the space domain offers has always depended on the availability of state-of-the-art technology to apply to our space capabilities. The level of requisite technology has demanded top-dollar investment and zero tolerance for errors. One small flaw in a launch vehicle can result in complete loss of the space vehicle. One small flaw in the space vehicle can result in total loss of mission on orbit. If not done correctly, the launch of a satellite is an irreversible process with dire and prohibitively expensive consequences. From the days of the "Schoolhouse Gang" led by Gen Bernard Schriever to the Space and Missile Systems Center of 2013, space acquisition has always required a team of dedicated, technically competent professionals and a significant dollar investment.

Although there are many constants about space acquisition, there are also some significant changes about the environment of the twenty-first century that compel us to evolve the way we acquire our space systems. The national security environment of 2013 is vastly different than that of 1947 or even that of 2005. First and foremost, our space systems are absolutely critical to our national security operations today. The world relies on space-based capabilities to provide humanitarian help in the aftermath of natural and technological disasters such as the Indian Ocean tsunami, the Kashmir earthquake, and the Japanese nuclear reactor incident to assess damage and evaluate the situation on the ground. Space-based capabilities provide rapid mapping and high-resolution imaging that have become important support tools in emergency relief operations. The capabilities also aid in executing logistics, staff security, distribution, transportation, and setup of telecommunication networks and refugee camps.

We also have a growing dependence on space-based capabilities for our military combat operations. Immediately after the terrorist attacks of 2001, small groups of elite American military units were deployed to Afghanistan to support the anti-Taliban Afghan fighters. Those units carried 2.75-pound precision lightweight Global Positioning System (GPS) receivers as well as satellite-based communication devices they used to pinpoint enemy targets and call in devastating air strikes against them. Because GPS-guided munitions strike with such accuracy, they greatly reduce the number of air sorties needed to destroy a target. This is a far cry from the Vietnam War when Soldiers would look at a map to call in friendly and enemy coordinates and then pop smoke so the aircraft could know where they were! Whether it is humanitarian operations in support of tsunami relief or combat operations in Afghanistan, we cannot accomplish the mission without our space capabilities.

Another change is the fact that the physical environment in which our satellites and space systems must operate is now competitive, congested, and contested. Currently, more than 60 countries or consortia

are operating satellites, and citizens of 39 nations have actually flown in space. Of the 190-plus countries around the globe, over 120 now own at least part of a satellite. There are over 1,000 active satellites in orbit today! In addition, the total amount of space debris has increased considerably in the past six years, primarily due to two events. The first was in 2007 when the Chinese tested an antisatellite weapon against one of their weather satellites. That test created more than 3,000 pieces of trackable debris along with thousands of pieces of debris too small to track—objects that will threaten other satellites for decades, if not centuries, to come. The second event was in 2009 when a dead Russian communications satellite hit an Iridium satellite, scattering about another 2,000 pieces of trackable debris around the earth and, again, many more pieces too small to track. Even more troublesome are the estimated hundreds of thousands of small pieces of debris we cannot track in space today. Traveling at nearly 18,000 miles per hour, an object does not have to be very large to create havoc for fragile satellites. Furthermore, the cyber domain is becoming a realm of possibly devastating attacks on our space assets.

Lastly, the budgets available for acquiring and maintaining space systems are declining. We have traditionally focused our decisions about space systems exclusively on performance first, schedule second, and costs a distant third. We can no longer afford to do that. Affordability needs to be in the forefront of our acquisition planning and requirements discussions. This changing landscape provides both challenges and opportunities for space acquisition.

Mandates for Space Systems Acquisitions

This environment drives three mandates for space system acquisitions today. First, we must continue to deliver on the space capabilities in the pipeline today. After several years (sometimes a decade or more) of development of these satellites and space systems, it is time to capitalize on that investment. We must consistently complete the build of these satellites and associated systems, safely and assuredly

launch them into orbit, and turn over operations to Fourteenth Air Force. Second, we must aggressively pursue opportunities to make these systems more affordable. We must ensure that we explore options to drive down costs as well as streamline and lean out our production and oversight mechanisms. In short, we make sure that every dollar counts. Certainly, we must maintain high standards for mission assurance. However, we must also make sure that we are not spending money doing things that provide no value and do not contribute to mission assurance. We must challenge the adage "We've always done it that way." Third, we must explore new architectures and constructs for providing space capability in the future. We must reassess our basic architectures and employment concepts against the changing threat environment, respond to the challenges, and leverage the opportunities presented by the competitive, congested, and contested space domain.

Our current space acquisition strategy and programs confront these mandates head on. For protected satellite communications (SATCOM), we are on schedule to ship and launch the third Advanced Extremely High Frequency (AEHF) satellite in the fourth quarter of 2013. Soon, AEHF will have three operational satellites providing Earth coverage between 65˚ north and 65˚ south latitude. AEHF is scheduled to reach initial operational capability by June 2015, providing a 10-fold increase of communication throughput to the war fighter, compared to its Milstar predecessor.[1] AEHF will provide over 400 megabits per second (Mbps) of data-throughput capability as compared to Milstar's 40 Mbps. We will still continue to exploit Milstar capability, as AEHF satellites are backwards compatible and cross-linked with Milstar to provide an integrated, protected communications network for the United States and our allies. Canada, the Netherlands, and the United Kingdom are international partners to the program with planned initial operational capabilities in July 2013, March 2014, and May 2016, respectively.

For wideband communications, we launched the fifth Wideband Global SATCOM (WGS) in May 2013 and will declare full operational capability in early 2014. This will provide unprecedented wideband

communications to US and international partner users. We plan to launch the sixth WGS satellite in the fourth quarter of 2013. The WGS-6, which completes the three space vehicle (SV) buy for WGS Block II, is part of an international partnership whereby the Australian government purchased the SV in exchange for a certain percentage of bandwidth from the constellation. Further down the pipeline, we are scheduled to launch WGS-7 in August 2015 to further augment the constellation. We also have plans for WGS 8–10 to deliver a new wideband digital channelizer that will almost double the capacity of the older systems. As was the case with WGS-6, international partners purchased WGS-9. New Zealand, Canada, Luxemburg, Denmark, and the Netherlands will get access to constellation bandwidth in return for their purchase of WGS-9.

The GPS IIF will complete production of its 12 satellites by the end of 2013. We plan to launch one GPS IIF SV in October 2013, three SVs in 2014, two SVs in 2015, and the final two SVs in 2016. We also expect the Next-Generation GPS Control Segment Block 1 to begin its transition to the operations process in 2016, providing GPS III SV launch and simulation as well as telemetry, tracking, and command capabilities. It will also enable GPS Blocks II and III on-orbit capability, including control of L1 C/A, L1 P(Y), L2 P(Y), L5, and L2C signals.[2]

Striving for Affordability in an Austere Budgetary Environment

At the same time, we have a razor-sharp focus on making these systems more affordable. We have experienced shrinking budgets these past few years, and we have been finding innovative and creative solutions to be able to continue providing our war fighters and nation the space-based capabilities they depend on every day. We are changing our mind-set on our strategic and tactical outlook as we transition from development to production mode in a number of our programs. We've

also reassessed many of our processes to ensure that we are as efficient as possible while maintaining mission assurance as our top priority.

Transition Programs from Development to Production

We have shifted from product development to production mode in several key programs, presenting many opportunities for us to make our systems more affordable. One example is in our Space-Based Infrared System (SBIRS) program with the second Geosynchronous Earth Orbit / Highly Elliptical Orbit (GEO/HEO) block (GEO/HEO 3–4) contract in 2008. Due to a 12-year gap between the GEO/HEO 1–2 block and the GEO/HEO 3–4 block contract awards, we've faced challenges with obsolescence, processes, and procedures, which increased government oversight and contractor interaction. However, these increased interactions led to production and cost-savings initiatives. Our plan for GEO 5–6 continues our block-buy strategy to leverage economic order-quantity efficiencies, and it benefits from having all developmental spacecraft/payloads delivered on orbit with the exception of a complete ground system. Although there are some challenges related to parts obsolescence that require initial nonrecurring engineering and advance procurement efforts, we can realize savings from using a fixed-price, firm-target contract since we are now acquiring the fifth and sixth of its kind.

GPS III implements processes established during development. Currently, GPS III SV01 is in the process of completing development integration and testing, with an expected completion date in the second quarter of 2014. Meanwhile, GPS III SV02 is at the beginning of the production line. It will begin assembly, integration, and testing in July 2013. GPS III SV03 and SV04 are on contract and have begun assembly-level production. GPS III SV05–08 long-lead parts procurement is also on contract, with production contract award expected in 2013. Because we have firm requirements, design proven through developmental testing, established manufacturing processes, and qualified suppliers, GPS III made a great candidate for fixed-price-incentive firm request

for proposal, which reduces contract data requirements lists (CDRL) from 115 to 20.

AEHF is also firmly in the production phase. As with SBIRS, we are focused on satellite block buy and production practices to shorten schedules and lower the unit cost.

Introduce Lean Processing and Production Flow

We have introduced lean processing and production flow into many of our major programs to identify and realize efficiencies in the way we conduct business. Working with contractor Lockheed Martin, our AEHF program office proposed new production timelines for AEHF-5 and AEHF-6, reducing 73 months to 63.5 months and 71.5 months, respectively. We were able to simplify the process by eliminating multiple mechanical reconfigurations and vehicle repositionings and executing streamlined testing.

For SBIRS, we are striving to resolve the challenges we faced due to small production quantities and multiple gap years between contract awards by aligning new contract awards to the delivery of the previous block. This way, we may maintain a consistent production-floor team and processing capacity. For example, we can time the GEO 5–6 staffing ramp-up to coincide with the GEO/HEO 3–4 effort ramp-down to sustain a steady battle rhythm on our production floor.

More specifically within our SBIRS production efforts, we have implemented several initiatives to streamline flow and reduce costs. Our GEO-3 single-line flow production saved $4.3 million in real dollars! These savings were made possible by true team effort with collaboration across government, industry, and subcontractor team members. Together, we championed several efforts, including a series of 21 recommendations to reduce single-line flow production to about 70 days as well as streamlined vehicle assembly flow, mechanical operations, test preparation, and test execution. We saved additional dollars by reducing unit thermal cycles and powered vibration tests.[3] We maintained a minimum of three thermal vacuum cycles for electronic/

electromechanical units, with an average savings of about 18 hours per thermal cycle per unit and a reduction of four cycles. This saved three days on a schedule of 24/7 critical-path operation.

Furthermore, payload integrator Northrop Grumman reused GEO-3 hardware for the GEO-4 payload test, saving us $1.3 million. It used fully integrated Flight 3 Payload Control Assembly to test both GEO-3 and GEO-4 payloads. Doing so eliminated tasks such as packing and shipping of payload-control assembly boxes and reintegrating test units.

For GPS IIF, we use a pulse-line production method based on lean processing and production principles.[4] We continuously evaluate each of our four assembly and test work centers for rebalancing, ensuring that there is no production bottleneck at any one station. This has allowed a savings of 96 days in production from SV-4 to SV-5, the first two full-production GPS IIF SVs.

With GPS III, we have introduced and completed 59/59 (100 percent) manufacture-readiness design reviews to optimize build-process flow. We used 3-D modeling to digitally illustrate in real time the manufacturing integration assembly and test hookup. This has reduced manufacturing work instruction by 70–83 percent.

Reduce and Eliminate Unnecessary Testing

We've further made our systems more affordable through reduction and elimination of unnecessary testing. By leveraging our lessons learned from the SBIRS GEO-1 campaign, we have reduced our GEO-2 planned duration by 55 percent to 105 days. Essentially, we were able to reduce development and testing for later iterations of software included in GEO-2. Whereas our system was unable to meet our suite of performance parameters until the fifth build for GEO-1, we are planning to achieve suitable performance using just three builds for GEO-2. We have also reduced the total number of sensor calibrations by assuming first-pass success, and we have eliminated unnecessary background collections for the GEO-2 test campaign. Finally, we are scaling

back the trial period for GEO-2. Because GEO-1 was a first-of-a-kind satellite and ground system, we put it through a 60-day trial period. For GEO-2, we are planning a 30-day period since it is the second delivery and we already have a good understanding of the payload.

We also leveraged lessons learned from prior efforts for GPS IIF. We gained significant confidence in the structural integrity of the first three SVs, which allowed us to eliminate acoustic testing for SVs 4–12. This amounts to a savings of approximately 15 days in each subsequent production flow. Meanwhile, GPS III has reduced cycle time by 57 percent through test reduction, extensive engineering, and prototype use.

Our AEHF program office and Lockheed Martin evaluated the test program to identify potential efficiencies and reductions. This resulted in reduced SV single-line flow testing for bus, payload, and SV-level tests. We also eliminated vehicle-level anomaly detection and resolution testing, which can be run on the Networked AEHF System Test Bed Tool or payload engineering model.

Reduce Unnecessary and Costly Oversight

Along with the programmatic streamlining, we have found further efficiencies in human resource management. The program operating plan (POP) defines and describes for each program the interaction and information exchange between the government and contractor. Some highlights of the POP include reducing the frequency of formal meetings/reviews and streamlining informal interactions between the government and contractor. The POP also identifies the core set of meetings, roles, responsibilities, and authorities for such meetings as well as requirements for informal government and contractor interaction.

With our WGS Program Office, we were able to reduce the number of required personnel by implementing a commercial-sector-like approach for the production of WGS 7–10. The Air Force deemed appropriate a commercial-like acquisition approach for the production of WGS 7–10 to account for the maturity of the production and acceptable

level of recurring technical risk. Thus, production contracts for WGS 7–10 were negotiated for firm fixed price, relying heavily on Boeing's commercial processes for systems engineering, management, production, test, and early on-orbit activities. Although this "commercial" acquisition model allows for limited customer interaction compared to traditional Department of Defense satellite acquisition models, the WGS Program Office has in exchange established a seven-person team located in the Boeing plant. These seven government members have full access to Boeing data and meetings, but their primary role is risk identification. This arrangement, along with closing Block II, allowed the government program office to reduce personnel by about 40 percent. Furthermore, using Boeing's commercial processes will reduce production and government-specific reviews, such as program management and mission assurance reviews, to almost zero. The stable design of WGS affords us the flexibility to limit government oversight, which saves Boeing "standing army" costs while still delivering robust satellites.

Reduce Reporting Requirements

We have also significantly reduced reporting requirements from our contractors, which drives down costs. We have streamlined integrated baseline reviews to a one-day event and removed thresholds for variance reporting. Contractors now report only the variances they determine would have significant impacts on the contract.

Additionally, we greatly reduced the number of CDRLs from many of our programs.[5] In order to make such reductions, we created the Data Accession List as a mechanism to deliver technical assessments and products to the government on an "as-needed" basis, maintained a streamlined list of programmatic-status CDRLs, monitored financial and small-business CDRLs for oversight, and focused on current needs so that we are not bound to outdated contractual obligations. As a result, we reduced System Engineering and Integration CDRL items from 46 to nine for SBIRS. This allowed us to build up the flexibility to

tackle emerging needs with decision-quality information. For AEHF-5/6, we reduced the total number of CDRLs by 48 percent and reduced government-approved CDRLs by 44 percent from AEHF-4. And for GPS III, we reduced CDRLs from 115 to 20.

Introduce Competition

Introducing competition is another way we are making our space systems more affordable. Full and open competition consistent with the Better Buying Power initiatives of the Office of the Secretary of Defense for Acquisition, Technology, and Logistics was a major driver in cost reduction for our GPS Control Segment sustainment contract award. We were able to use the lowest priced, technically acceptable source-selection strategy and select a firm-fixed-price contract because the system is in the operations and sustainment phase of its life cycle, and therefore the requirements are well understood. As a result, the actual contract award came in at $119 million, a savings of $68 million from the original government budget / cost estimate of $187 million.

We also held a competitive source selection for the Command and Control System–Consolidated (CCS-C) Production and Sustainment Contract (CPASC). Including CCS-C production for WGS 6–9, production for AEHF 3–5, development studies, and sustainment, our estimate for the CPASC was $199 million. However, after we used predominantly fixed-price-incentive contract line-item numbers, set ceiling prices on those line-item numbers to prevent overrun expenses to the government, and provided a 50/50 share ratio in cost-incentive arrangement, the competition led to a six-year negotiated contract price of $133 million, including options. That's a savings of $66 million!

Consolidate Baselines and Contracts

We have been working to increase efficiencies through consolidating baselines and contracts. For our SBIRS ground system, we initiated Increment 2 Completion (Inc2C) in November 2012 for a full ground-program baseline, restructuring the Block 10 baseline into four incre-

mental deliveries with one Program Executive Officer Certification and Operational Acceptance event for a primary operations center (MCS-2) at Buckley AFB, Colorado, and a backup operations facility (MCSB-2) at Schriever AFB, Colorado.[6] Under the program, we have consolidated SBIRS satellite command and control operations from Buckley AFB (Defense Support Program), Schriever AFB (HEO1 and HEO2), and the Interim Test Center (GEO1 and GEO2) into MCS-2 and MCSB-2. This has allowed us to combine ground and system test activities early in the testing process and streamline test and verification processes in concert with the Air Force Operational Test and Evaluation Center. Moreover, the incorporated simulator data allow earlier defect discovery within an operational environment, and we can increase use of flight-test assets for more robust system test resources. Another major consolidation effort is the Consolidated Orbital Operations Logistics Sustainment (COOLS) contract, which will yield efficiencies by merging existing sustainment efforts supporting the Defense Satellite Communications System, Milstar, and AEHF constellations under a single contract. As the contractor shares component experts across an even broader range of programs such as Military SATCOM, SBIRS, and GPS, we expect to gain even more efficiencies. Through these efficiencies and scope reductions, the team predicts a 35 percent cost reduction by the end of the five-year COOLS contract.

We are currently experiencing significant duplication of work because no single contractor is responsible for total system performance of the Eastern Range and Western Range, and the government must intervene whenever contractors work together.[7] To eliminate some of that duplication, we are partnering with the 45th and 30th Space Wings to select a single contractor for a consolidated Launch and Test Range System (LTRS) Integrated Support Contract (LISC) Operations, Maintenance, and Sustainment Contract (LISC OM&S) of more than $2.5 billion for 10 years. This effort is designed to enhance mission effectiveness and generate cost efficiencies at both the Eastern Range

and Western Range, which allows us to reinvest the savings in the ranges.

Under the LISC, one contractor will be required to keep the range "green" (or "go for launch"). The government will hold the single contractor accountable to meet system metrics, and the contractor will bear the risk if the system does not perform. This construct allows the selected contractor to optimize manpower to meet mission needs and increase profits while providing a system that meets the government's requirements. We released the LISC OM&S request for proposal to industry in late March this year, began source selection on 30 May 2013, and expect to award the contract the second quarter of 2014.

Planning for the Future

All of our ongoing efforts are allowing us to continue providing current capabilities for about another decade. But what happens after that? As the current congested, contested, and competitive space environment continues to evolve, we will also have to evolve our architectures to maintain space superiority. The following are the main concepts that are more fully discussed in an article I coauthored entitled "Space: Disruptive Challenges, New Opportunities, and New Strategies," published in *Strategic Studies Quarterly*.[8]

Traditionally, our strategy has been to load multiple missions onto every spacecraft because the cost of launch has been prohibitively expensive. Now with robust constellations of satellites already set in place and a thriving commercial medium-launch market at hand, we are looking to exploit the new commercial trade space by reducing the size of our missions and spreading them across multiple launches. Doing so is beneficial to us in many ways. First, the up-front costs are significantly lower for us. Traditional gargantuan satellites can weigh up to 10,000 pounds, including spacecraft and fuel at launch. Of course, the more size, weight, and power a satellite requires, the heftier the overall price tag. By using much smaller free-fliers or payloads that are

attached to host space vehicles, we can drastically reduce costs typically associated with traditional programs. This affords us both the flexibility to make quick-turn decisions when faced with unforeseen circumstances at the action level instead of waiting for approval up the chain and the ability to send updated technology into space more frequently.

We can further cut costs by employing commercial buses to leverage the commercial market. The government has traditionally emphasized use of unique buses for each launch, and the maintenance and repair costs of several one-of-a-kind buses have been monumental. To be sure, we had to develop first-of-a-kind spacecraft more out of necessity than preference in the early days of space exploration, but now we have a competitive commercial market of spaceflight-proven buses that we can essentially buy off an assembly line. Eliminating nonrecurring engineering along with the expensive knowledge legacy and maintenance that go along with these unique buses will lead to huge cost savings for us.

Leveraging the international space environment with cooperative programs and shared capabilities can further reduce cost while strengthening international relationships. As mentioned above, the WGS-6 and WGS-9 international arrangements allow us to get more assets into space, and we collectively benefit from increased data bandwidth. Another example is the Constellation Observing System for Meteorology Ionosphere and Climate (COSMIC), a joint Taiwan-US science mission for weather, climate, space weather, and geodetic research. The COSMIC payload science data are routinely downloaded every orbit and have demonstrated their value for operational weather forecasting, hurricane forecasting, and investigations of the atmospheric boundary layer. Due to the success of the first COSMIC, Taiwan and the United States have decided to move forward with COSMIC-2, a follow-on mission that will launch six satellites into low-inclination orbits in early 2016 and another six satellites into high-inclination orbits in early 2018. The US Air Force will provide two space weather payloads

that will fly on the first six satellites of COSMIC-2, and Taiwan will help with costs of the overall program, resulting in about 50/50 cost sharing between Taiwan and the United States for COSMIC-2.

Hosted payloads offer us another alternative to save up-front costs and to leverage the competitive and congested aspects of space. Because we are operating in such a crowded manifest, partnerships with both commercial companies and other nations will become increasingly important to access the spectrum we need. By reducing the size of our missions and riding on commercial or international hosts as payloads, we can multiply the opportunities we have to gain access to space.

As a corollary to cost, resiliency is driving us to consider alternatives to traditional ways of accessing space. Taking new orbits and non-space systems is part of the new equation when examining potential architectures. For example, we are starting to examine orbits that are higher in altitude and more inclined than traditional orbits as space becomes more congested and contested. We are also looking at ways to improve the timeliness of our command and control systems to quickly send commands and adjust our spacecraft posture to known threats or space debris. These new options require the flexibility that disaggregation allows in order to be feasible. Moreover, distributing our assets improves our resiliency to attacks and system failure by not putting "all of our eggs in one basket." Because our past strategy has been to load multiple missions onto every spacecraft, if one of our multimission spacecraft goes down due to either technical failure or adversarial attack, all of those capabilities that our nation relies on will be lost. Distributing those missions across several platforms will ensure that we can continue to count on other capabilities should a spacecraft carrying one of our missions fail. Additionally, placing missions on buses hosted by commercial or international partners can really complicate an adversary's decision to attack our capabilities.

Lastly, we need to develop new and robust architectures based on new technology and the foundational work we've conducted to develop

methods of assessing future systems. For instance, the wide-field-of-view technology proven by the successful Commercially Hosted Infra-Red Payload technology demonstration gives us the ability to detect multiple objects simultaneously and increases detection accuracy. We need to leverage such technological advances along with improved processing time and improvements in cyberspace to continue to be the best Air Force in the world! ✪

Notes

1. Milstar provides the president, secretary of defense, and the US armed forces with assured, survivable SATCOM with low probability of interception and detection. The objective of the Milstar program was to create a survivable, secure, nuclear-survivable, space-based communication system, which was considered a top national priority during the Reagan administration. There are five operational Milstar satellites. The first two satellites (Milstar I) carry a low-data-rate payload that can transmit 75 to 2,400 bits per second of data over 192 channels in the extremely high frequency range. Encryption technology and satellite-to-satellite cross-links provide secure communications, data exchange, and global coverage. The other three satellites (Milstar II) carry both low-data-rate and medium-data-rate payloads. The latter can transmit 4,800 bits per second to 1.544 megabits per second of data over 32 channels. The higher data rates allow the user to transmit large amounts of data in a short period of time.

2. L1 C/A is the legacy civil signal, which will continue broadcasting in the future. Users must upgrade their equipment to benefit from the new signals. The military precise (P) code is encrypted by the military—using a technique known as antispoofing—and is available only to authorized personnel. The encrypted P code is referred to as the Y code. Civilian GPS receivers use the C/A code on the L1 frequency to compute positions—although high-end, survey-grade civilian receivers use the L1 and L2 frequencies' carrier waves directly. Military GPS receivers use the P (Y) code on both L1 and L2 frequencies to compute positions. L5 is the third civilian GPS signal, designed to meet demanding requirements for safety-of-life transportation and other high-performance applications. L5 is broadcast in a radio band reserved exclusively for aviation safety services. It features higher power, greater bandwidth, and an advanced signal design. L2C is the second civilian GPS signal, designed specifically to meet commercial needs. When combined with L1 C/A in a dual-frequency receiver, L2C enables ionospheric correction—a technique that boosts accuracy. Civilians with dual-frequency GPS receivers enjoy the same accuracy as the military (or better). For professional users with existing dual-frequency operations, L2C delivers faster signal acquisition, enhanced reliability, and greater operating range. L2C broadcasts at a higher effective power than the legacy L1 C/A signal, making it easier to receive under trees and even indoors. The Commerce Department estimates that L2C could generate $5.8 billion in economic productivity benefits through the year 2030.

3. Unit-level thermal cycle and powered vibration tests screen hardware for design and workmanship issues by simulating the on-orbit operating environment that the units will experience. On-orbit performance of the GEO-1 space vehicle and ground test performance of the GEO-2 space vehicle demonstrated the sound design of the units under test and thereby provided confidence that the additional thermal cycles and powered vibration tests could be eliminated. This would save cost with a very modest but acceptable increase in risk for workmanship issues that might not be discovered until later at a higher level of assembly.

4. Similar to an aircraft assembly line, the GPS IIF pulse line efficiently moves a satellite from one designated work area to the next at a fixed rate. The GPS pulse line can accommodate four satellites at any given time. Wait time between tasks is reduced or eliminated by staging necessary parts and tools at the point of use at each workstation, creating a smooth process flow. Along the pulse line, satellites flow to work centers dedicated to four manufacturing stages: vehicle assembly, initial test, thermal-vacuum testing, and final test. The line delivers one SV to storage every two to three months.

5. The CDRL includes authorized data requirements for a specific procurement that forms part of a contract. It is comprised of either a single DD Form 1423 or a series of such forms containing data requirements and delivery information. The CDRL is the standard format for identifying potential data requirements in a solicitation and deliverable data requirements in a contract.

6. Increment 2 completion represents the ground program baseline that consolidates operations of the Department of Defense's overhead persistent infrared satellite constellation supporting missile warning, missile defense, technical intelligence, and battlespace awareness missions. The constellation consists of three major systems: the Defense Support Program, SBIRS GEO satellites, and SBIRS HEO payloads. Increment 2 completion will relocate ground operations for each of these systems from their individual locations known as the mission control station (MCS) at Buckley AFB and the MCSB at Schriever AFB. Additionally, the Increment 2 baseline delivers a satellite command and control, mission processing, and external reporting architecture that allows for data fusion and fast, accurate reporting on infrared events around the globe.

7. The Eastern Range (ER) and Western Range (WR) are the national security space rocket ranges for the United States. The ER supports missile and rocket launches from the two major launch heads located at Cape Canaveral Air Force Station and the Kennedy Space Center, Florida. It is managed by the 45th Space Wing. The WR supports the major launch head at Vandenberg AFB, California. Managed by the 30th Space Wing, the WR extends from the West Coast of the United States to 90˚ east longitude in the Indian Ocean.

8. Lt Gen Ellen Pawlikowski, Doug Loverro, and Col Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 27–54, http://www.au.af.mil/au/ssq/2012/spring/spring12.pdf.

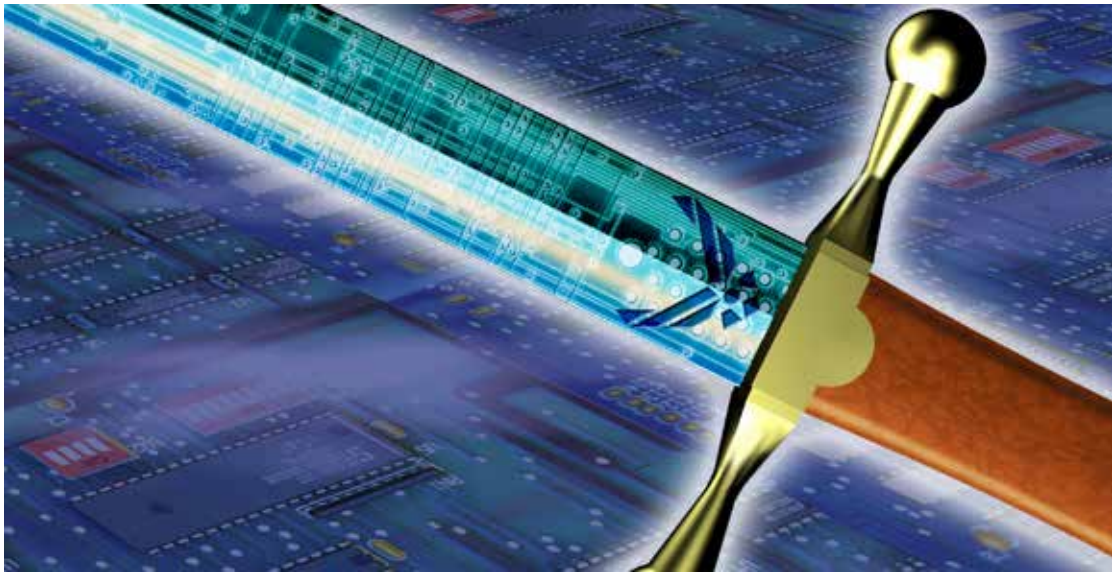
Lt Gen Ellen M. Pawlikowski, USAF

Lieutenant General Pawlikowski (BS, New Jersey Institute of Technology–Newark; PhD, University of California–Berkeley) is commander of the Space and Missile Systems Center, Air Force Space Command, Los Angeles AFB, California. She is responsible for more than 6,000 employees nationwide and an annual budget of $10 billion. As the Air Force program executive officer for space, General Pawlikowski manages the research, design, development, acquisition, and sustainment of satellites and the associated command and control systems.

Let us know what you think! Leave a comment!

The Importance of Designating Cyberspace Weapon Systems

Brig Gen Robert J. Skinner, USAF



Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *weapon system* as "a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency."[1] When one thinks of the US Air Force and weapon systems, the B-2 Spirit stealth bomber, F-15E Strike Eagle fighter jet, or F-16 Fighting Falcon aircraft quickly come to mind. Even the Minuteman III missile, the Global Positioning System, or KC-135 Stratotanker air refueling aircraft could become part of the discussion because, after all, the Air Force's mission is to fly, fight, and win in air, space, and cyberspace. These assets, which fall under the air and space umbrella, have served as tried and true weapon systems for many years. The Air Force has now added to the long line of its

weapon systems that support cyberspace operations "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." These systems are unique in that they are tied to the newest domain of cyber—"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2]

On 24 March 2013, the chief of staff of the Air Force approved the official designation of six cyberspace weapon systems under the lead of Air Force Space Command (AFSPC), which is responsible for organizing these systems, equipping units with them, and training individuals to use the systems. The Air Force's provision of global reach, power, and vigilance across the domains of air and space now applies to the cyberspace domain through the designation of the following cyberspace weapon systems:

- Air Force Cyberspace Defense
- Cyberspace Defense Analysis
- Cyberspace Vulnerability Assessment / Hunter
- Air Force Intranet Control
- Air Force Cyber Security and Control System
- Cyber Command and Control Mission System

Although the names may imply some duplication of effort with respect to these capabilities, the personnel and equipment that comprise these systems perform unique missions and complement each other. All of them focus on providing and securing cyberspace as a mission enabler and protecting critical information while defending our networks from attack. Any consideration of the capabilities of these weapon systems would benefit from comparing this suite of cyberspace weapon systems to the Air Force's military airlift weapon systems (the C-5, C-17, C-130, etc.), each of which contributes uniquely to

the overall air mobility mission. Just as clear distinctions exist among these platforms, based upon the operational capabilities required, so do the cyberspace weapon systems differ from each other. The systems may have overlapping mission areas, but they are complementary in much the same way as our airlift platforms—they offer comprehensive capabilities.

Revelations of Chinese activities on our networks, as outlined earlier this year in the Mandiant Company's report titled *Advanced Persistent Threat (APT) 1: Exposing One of China's Cyber Espionage Units*, emphasize the urgent need for the Air Force and the nation to develop capabilities to defend this critical domain and thereby ensure information superiority. The report illustrates the persistent threat, noting that "the details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them. . . . Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors." The Mandiant report on APT 1 highlights only one of more than 20 APT groups based in China, tracking this single group to cyber attacks on nearly 150 victims over seven years with hundreds of terabytes of data exfiltrated.[3] Clearly, though, this discussion does not confine itself to any particular adversary. Many aggressors inhabit the cyberspace domain, and the executor of these activities ranges from an individual in the basement of his house, to groups of individuals working as teams, to nation-states. Their intentions can also cover a spectrum of activities, including espionage, theft of intellectual capital, organized crime, identity theft, military operations, and so forth.

This article examines each weapon system, highlights its history and unique capabilities, and describes the specific units that operate the system. It then discusses the importance of classifying these capabilities as "weapon systems," illustrating how they directly address the threats we face today. Before doing so, however, the article presents a

stage-setting vignette to establish an understanding of weapon system capabilities and their employment against an adversary.

Assume that you are a government civilian sitting at your desk at a major command headquarters when you receive an e-mail concerning sequestration and a potential furlough. Included in the e-mail is a link to a website for more information. You attempt to open the link but receive an error message. You try again with the same result. You then resume work on your tasks. Unknown to you, the link has directed you to a malicious web server that downloaded malware enabling an adversary to take command of your desktop computer. How could this occur, and why would anyone specifically target you? Actually, it was not difficult. Remember the conference you attended a few months ago, before temporary duty became restricted? The adversary lifted your e-mail address from the conference sign-in sheet, also available to the event sponsors. Why you? Adversaries consider your unique expertise and access to valuable information a "target-rich environment." Only one person needs to click on the link to initiate a series of malicious actions. Because the adversary left no hint of a problem on your computer, he now has unfettered access to that unclassified but useful information.

How does the Air Force combat such intrusions? Actually, the best defense for phishing attacks is user education. However, these attacks are becoming more sophisticated and sometimes almost impossible to identify. All of the services have cyberspace units responsible for network defense. In this case, network traffic monitoring tips off the Air Force to the intrusion on your desktop computer. A network operations unit identifies an unusual amount of traffic leaving your base directed to addresses in another country. The unit notifies the 624th Operations Center, including Air Force Office of Special Investigations personnel, and the center begins command and control (C2) and law enforcement efforts to address the event. Cyberspace forensics experts are dispatched to review the situation, not only locating the "infected" equipment but also determining how the adversary accessed the Air Force

system. Cyberspace C2 dispatches cyber operations risk-assessment personnel to survey the situation, determine the exact data exfiltrated, and assess the damage. The Air Force computer emergency response team (AFCERT) examines your base's computers and other hardware to footprint exact infiltration methods, using them to develop (and share) defensive actions specific to the threat and glean any new tactics, techniques, and procedures. The AFCERT pushes patches to all Air Force desktop computers to combat future attempts to employ this technique; it will support your base on further network cleanup and hardening. Now that we have described an attack from 50,000 feet, let us delve deeper into the weapon systems and units that carry out these missions.

Air Force Cyberspace Defense Weapon System

The Air Force Cyberspace Defense (ACD) weapon system prevents, detects, responds to, and provides forensics of intrusions into unclassified and classified networks. Operated by the 33d Network Warfare Squadron (NWS), located at Joint Base San Antonio–Lackland, Texas, and the Air National Guard's 102d NWS, located at Quonset Air National Guard Base, Rhode Island, the ACD weapon system supports the AFCERT in fulfilling its responsibilities. The crews for this weapon system consist of one cyberspace crew commander, one deputy crew commander, one cyberspace operations controller, and 33 cyberspace analysts, all of them supported by additional mission personnel.

The ACD weapon system evolved from the AFCERT, which has primary responsibility for coordinating the former Air Force Information Warfare Center's technical resources to assess, analyze, and mitigate computer security incidents and vulnerabilities. The weapon system offers continuous monitoring and defense of the Air Force's unclassified and classified networks, operating in four subdiscipline areas:

1. incident prevention: protects Air Force networks (AFNet) against new and existing malicious logic; assesses and mitigates known software and hardware vulnerabilities.
2. incident detection: conducts monitoring of classified and unclassified AFNets; identifies and researches anomalous activity to determine problems and threats to networks; monitors real-time alerts generated from network sensors; performs in-depth research of historical traffic reported through sensors.
3. incident response: determines the extent of intrusions; develops courses of action required to mitigate threat(s); determines and executes response actions.
4. computer forensics: conducts in-depth analysis to determine threats from identified incidents and suspicious activities; assesses damage; supports the incident response process, capturing the full impact of various exploits; reverse-engineers code to determine the effect on the network/system.

Cyberspace Defense Analysis Weapon System

The Air Force Cyberspace Defense Analysis (CDA) weapon system conducts defensive cyberspace operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, e-mail, and US Air Force websites. CDA is vital to identifying operations security disclosures. The weapon system is operated by three active duty units (68 NWS; 352 NWS; and 352 NWS, Detachment 1) and two Air Force Reserve units (860th Network Warfare Flight and 960th Network Warfare Flight) located at Joint Base San Antonio–Lackland, Texas; Joint Base Pearl Harbor–Hickam Field, Hawaii; Ramstein Air Base, Germany; and Offutt AFB, Nebraska. The crews for this weapon system consist of one cyberspace operations controller and three cyberspace defense analysts. All mission crews receive support from additional mission personnel.

The CDA weapon system's two variants are designed to monitor, collect, analyze, and report on official Air Force information transmitted via unsecured telecommunications systems to determine whether any of it is sensitive or classified. The system reports compromises to field commanders, operations security monitors, or others, as required, to determine potential effects and operational adjustments. The second variant provides additional functionality to conduct information damage assessment based on network intrusions, coupled with an assessment of Air Force unclassified websites. Only the 68 NWS operates the second variant.

The CDA weapon system supplies monitoring and/or assessment in six subdiscipline areas:

1. telephony: monitors and assesses Air Force unclassified voice networks.
2. radio frequency: monitors and assesses Air Force communications within the VHF, UHF, FM, HF, and SHF frequency bands (mobile phones, land mobile radios, and wireless local area networks).
3. e-mail: monitors and assesses unclassified Air Force e-mail traffic traversing the AFNet.
4. Internet-based capabilities: monitor and assess information that originates within the AFNet that is posted to publicly accessible Internet-based capabilities not owned, operated, or controlled by the Department of Defense (DOD) or the federal government.
5. cyberspace operational risk assessment (found within the second variant operated by the 68 NWS): assesses data compromised through intrusions of AFNets with the objective of determining the associated effect on operations resulting from that data loss.
6. web risk assessment (found within the second variant operated by the 68 NWS): assesses information posted on unclassified public and private websites owned, leased, or operated by the Air Force in order to minimize its exploitation by an adversary, diminishing any adverse affect on Air Force and joint operations.

Cyberspace Vulnerability Assessment / Hunter Weapon System

The Air Force Cyberspace Vulnerability Assessment (CVA) / Hunter weapon system executes vulnerability, compliance, defense, and non-technical assessments, best-practice reviews, penetration testing, and hunter missions on Air Force and DOD networks and systems. Hunter operations characterize and then eliminate threats for the purpose of mission assurance. This weapon system can perform defensive sorties worldwide via remote or on-site access. The CVA/Hunter weapon system is operated by one active duty unit, the 92d Information Operations Squadron, located at Joint Base San Antonio–Lackland, Texas, and one Guard unit, the 262 NWS, located at Joint Base Lewis-McChord, Washington. Additionally, two Guard units are in the process of converting to this mission: the 143d Information Operations Squadron located at Camp Murray, Washington, and the 261 NWS located at Sepulveda Air National Guard Station, California. The crews for this weapon system consist of one cyberspace crew commander, one to four cyberspace operators, and one to four cyberspace analysts. Additional mission personnel support all of the mission crews. Developed by the former Air Force Information Operations Center, the CVA/Hunter weapon system was fielded to the 688th Information Operations Wing in 2009.

Historically, vulnerability assessments proved instrumental to mission assurance during Operations Enduring Freedom and Iraqi Freedom. CVAs continue to provide this vital capability. Additionally, they now serve as the first phase of hunting operations. The hunter mission grew out of the change in defensive cyber strategy from "attempt to defend the whole network" to "mission assurance on the network," offering an enabling capability to implement a robust defense-in-depth strategy. CVA/Hunter weapon system prototypes have participated in real-world operations since November 2010. The weapon system attained initial operational capability in June 2013.

Designed to identify vulnerabilities, the CVA/Hunter gives commanders a comprehensive assessment of the risk of existing vulnerabilities on critical mission networks. It is functionally divided into a mobile platform used by operators to conduct missions either on site or remotely, a deployable sensor platform to gather and analyze data, and a garrison platform that provides needed connectivity for remote operations as well as advanced analysis, testing, training, and archiving capabilities. Specifically, the hunter mission focuses on finding, fixing, tracking, targeting, engaging, and assessing the advanced, persistent threat.

During active engagements, the CVA/Hunter weapon system, in concert with other friendly network defense forces, provides Twenty-Fourth Air Force / Air Forces Cyber and combatant commanders a mobile precision-protection capability to identify, pursue, and mitigate cyberspace threats. It can be armed with a variety of modular capability payloads optimized for specific defensive missions and designed to produce specific effects in cyberspace. Each CVA/Hunter crew can conduct a range of assessments, including vulnerability, compliance, and penetration testing, along with analysis and characterization of data derived from these assessments. The weapon system's payloads consist of commercial-off-the-shelf and government-off-the-shelf hardware and software, including Linux and Windows operating systems loaded with customized vulnerability-assessment tools.

Air Force Intranet Control Weapon System

The Air Force Intranet Control (AFINC) weapon system is the top-level boundary and entry point into the Air Force Information Network, controlling the flow of all external and interbase traffic through standard, centrally managed gateways. The AFINC weapon system consists of 16 gateway suites and two integrated management suites. Operated by the 26th Network Operations Squadron (NOS) located at Gunter Annex, Montgomery, Alabama, AFINC has crews consisting of one crew commander, one deputy crew commander, one cyberspace

operations crew chief, two operations controllers, two cyberspace operators, and three event controllers, all of them supported by additional mission personnel.

The AFINC weapon system replaces and consolidates regionally managed, disparate AFNets into a centrally managed point of access for traffic through the Air Force Information Network. It delivers network-centric services, enables core services, and offers greater agility to take defensive actions across the network. AFINC integrates network operations and defense via four subdiscipline areas:

1. defense-in-depth: delivers an enterprise-wide layered approach by integrating the gateway and boundary devices to provide increased network resiliency and mission assurance.
2. proactive defense: conducts continuous monitoring of AFNet traffic for response time, throughput, and performance to ensure timely delivery of critical information.
3. network standardization: creates and maintains standards and policies to protect networks, systems, and databases; reduces maintenance complexity, downtime, costs, and training requirements.
4. situational awareness: delivers network data flow, traffic patterns, utilization rates, and in-depth research of historical traffic for anomaly resolution.

Air Force Cyber Security and Control System Weapon System

The Air Force Cyber Security and Control System (CSCS) weapon system provides network operations and management functions around the clock, enabling key enterprise services within the Air Force's unclassified and classified networks. It also supports defensive operations within those AFNets. CSCS is operated by two active duty NOSs, one Air National Guard Network Operations Security Squadron,

and two Air Force Reserve Command Associate NOSs aligned with the active duty squadrons. The 83 NOS and 860 NOS are located at Langley AFB, Virginia; the 561 NOS and 960 NOS at Peterson AFB, Colorado; and the 299th Network Operations Security Squadron at McConnell AFB, Kansas. Crews for this weapon system consist of one cyberspace crew commander, one cyberspace operations controller, an operations flight crew (conducting boundary, infrastructure, network defense, network focal point, and vulnerability-management functions), and an Enterprise Service Unit (supplying messaging and collaboration, directory and authentication services, storage and virtualization management, and monitoring management). Additional mission personnel support all of the mission crews.

The CSCS resulted from an operational initiative to consolidate numerous major command–specific networks into a centrally managed and controlled network under three integrated network operations and security centers. In 2007 the Air Force established two active duty NOSs to provide these functions. The Air National Guard Network Operations Security Squadron does the same for the Guard's bases and units.

The CSCS weapon system performs network operations and fault-resolution activities designed to maintain operational networks. Its crews monitor, assess, and respond to real-time network events; identify and characterize anomalous activity; and take appropriate responses when directed by higher headquarters. The system supports real-time filtering of network traffic into and out of Air Force base-level enclaves and blocks suspicious software. CSCS crews continuously coordinate with base-level network control centers and communications focal points to resolve network issues. Additional key capabilities include vulnerability identification and remediation as well as control and security of network traffic entering and exiting Air Force base-level network enclaves. CSCS also offers Air Force enterprise services, including messaging and collaboration, storage, and

controlled environments for hosting network-based systems that support the service's missions.

Cyber Command and Control Mission System Weapon System

The Cyber Command and Control Mission System (C3MS) weapon system enables the Air Force mission by synchronizing the service's other cyber weapon systems to produce operational-level effects in support of combatant commanders worldwide. It provides operational-level C2 and situational awareness of Air Force cyber forces, networks, and mission systems, enabling the Twenty-Fourth Air Force commander to develop and disseminate cyber strategies and plans; the commander can then execute and assess these plans in support of Air Force and joint war fighters. Operated by the 624th Operations Center at Joint Base San Antonio–Lackland, Texas, the C3MS weapon system has crews consisting of a senior duty officer, a deputy senior duty officer, a defensive cyberspace watch officer, an offensive cyberspace watch officer, a DOD information network watch officer, three defensive cyber operations controllers, three offensive cyber operations controllers, three DOD information network operations controllers, a cyberspace effects planner, a cyberspace operations strategist, a cyberspace intelligence analyst, a cyberspace operations assessment analyst, and a cyberspace operations reporting cell analyst. All mission crews are supported by additional mission personnel. The C3MS weapon system evolved from the legacy AFNet operations security center's concept, personnel, and equipment. With the activation of US Cyber Command and Twenty-Fourth Air Force, senior leaders recognized the need for an operational-level cyber C2 capability.

The C3MS is the single Air Force weapon system offering perpetual, overarching awareness, management, and control of the service's portion of the cyberspace domain. It ensures unfettered access, mission assurance, and joint war fighters' use of networks and information-

processing systems to conduct worldwide operations. The weapon system has five major subcomponents:

1. situational awareness: produces a common operational picture by fusing data from various sensors, databases, weapon systems, and other sources to gain and maintain awareness of friendly, neutral, and threat activities that affect joint forces and the Air Force.
2. intelligence, surveillance, and reconnaissance (ISR) products: enable the integration of cyberspace indications and warning, analysis, and other actionable intelligence products into overall situational awareness, planning, and execution.
3. planning: leverages situational awareness to develop long- and short-term plans, tailored strategy, courses of action; shapes execution of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.
4. execution: leverages plans to generate and track various cyberspace tasking orders to employ assigned and attached forces in support of offensive cyberspace operations, defensive cyberspace operations, and DOD information network operations.
5. integration with other C2 nodes: integrates Air Force–generated cyber effects with air and space operations centers (AOC), US Cyber Command, and other C2 nodes.

Why Cyber Weapon Systems?

If we truly wish to treat cyberspace as an operational domain no different from air, land, sea, or space, then our thinking must evolve from communications as a supporting function to cyber as an operational war-fighting domain. To fly and fight effectively and to win in cyberspace, the Air Force must properly organize, train, and equip its cyber professionals. For many years, AFNet infrastructure and systems grew as a result of multiple communities adding components to suit their individual needs, often with end-of-year funds. Similarly, the

components that now make up these six systems had no lead major command to articulate operational requirements and ensure standardized training as well as the effective management and resourcing of equipment life cycles. Such an inconsistent approach made mission assurance and the defense of critical Air Force and joint missions in cyberspace nearly impossible. Migration to the AFNet has allowed the service to take great strides towards realizing the vision from nearly two decades ago of operationalizing and professionalizing the network. AFSPC championed the effort to identify these six systems' weapon systems and facilitate this move to a more disciplined approach. Formally designating these systems helps ensure proper management and sustainment of equipment life cycles. It also expedites the evolution of Air Force cyber professionals from a communications or information technology mind-set to an operational one replete with mission-qualification training, crew force-management standards, and standardization and evaluation programs (where appropriate) to normalize cyber operations, as is the case with space and missile operations. Furthermore, formally designated weapon systems should help cyber receive the proper manning and programmatic funding necessary to ensure that the Air Force can fly, fight, and win in cyberspace.

The DOD construct for the management and resourcing of air, space, land, and sea superiority occurs via weapon systems. The best way to create and control effects in the cyber domain involves using the same weapon system construct to manage and resource cyber capabilities. Cyber weapon systems offer a path for the Air Force to operationalize, normalize, and ultimately standardize cyber, just as we have with the other war-fighting domains. The Air Force has been charged with securing, operating, and defending its portion of the DOD information networks and with defending Air Force and joint missions in the cyberspace domain. These cyber weapon systems give the Air Force a path to follow in normalizing operations to realize this goal.

The designation of cyber weapon systems created a separate cyber-sustainment funding line in the overall process of sustaining Air Force

weapon systems. By normalizing the funding process, the service has instituted proper long-term planning and programming of sustainment funding, thus enabling more effective and efficient use of these limited resources, as compared to uncoordinated execution of unreliable end-of-year funds—key tenets to guaranteeing standardized configuration management and servicewide (and, where applicable, joint) interoperability. We are already realizing these benefits through the deployment of AFNet, whereby the Air Force enterprise has become easier to defend and the user experience continues to improve through ongoing standardization.

The benefits of designating cyberspace weapon systems are similar to those gained by weapon systems in other domains—it is the standard Air Force mechanism for organizing, training, equipping, and presenting mission capabilities. The weapon system construct allows the service to manage operational capabilities in a formalized approach and assure their standardization, sustainment, and availability to combatant commanders. When AFSPC personnel compared the air and space domains' normalization processes, they found that only weapon system designation delivered the desired end state. Such systems may not always be ideally resourced, but they certainly receive better support than they would without designations.

Furthermore, designating cyberspace weapon systems directly supports AFSPC's role as cyber core function lead integrator, enabling the command to meet responsibilities listed in Air Force Policy Directive 10-9 and facilitating standardization across cyberspace platforms.[4] Designating these weapon systems is also critical to providing tactical units with the resources and training they need to operate in a normalized capacity. The core of cross-domain integration lies in the ability to leverage capabilities from different domains to create unique and decisive effects—if adequately resourced. Such designations will support proper evolution of the cyberspace domain and its relationship with the other operational domains—a critically important point because in modern warfare, cyberspace interconnects all domains. All of these ef-

forts to normalize and operationalize cyberspace operations and missions drive the Air Force towards the joint information environment (JIE) construct, standards, and processes. As the DOD, US Cyber Command, and services implement the JIE, they are also standing up cyber mission teams to support national, combatant command, and service-specific cyber requirements. Designating these capabilities as weapon systems allows these teams to better support national and joint missions in, through, and from cyberspace.

Unique Challenges of the Cyber Domain

The air, land, sea, and space domains are natural areas—we didn't have to build them, as we did the tools to leverage those domains. Although none of the natural domains demands any maintenance, cyberspace predominantly exists within the equipment and devices designed, built, and configured by humans, requiring constant maintenance as equipment becomes outdated or worn out. Additionally, the way we construct cyberspace has a direct effect on our ability to operate and defend the domain. This aspect makes cyberspace unique in that its operation is just as important as its defense. We must constantly feed and care for the domain as well as innovate to stay ahead of or, preferably, drive the technology curve.

Defending cyber also presents its own challenges since an adversary can launch a cyber attack virtually without warning from any location on the globe. In the case of intercontinental ballistic missiles, we at least have sensors that detect the launch; thus, depending on the location of the launch, our forces have some modicum of warning and can respond. In cyberspace, attacks can occur without warning or time to craft and execute responses. The Air Force must develop capabilities to detect such attacks, prevent them if possible, and respond accordingly if required, just as it does in all other war-fighting domains. We must also develop the tools to leverage cyberspace for our own benefit. In reality, we may never be able to defend our networks completely—to do so would likely require so much security that we lose the force-

multiplying benefits that cyberspace offers to all of our missions. If we keep all adversaries out, most likely we will keep ourselves locked in. The key lies in finding a balance so that we effectively defend our networks and the missions that rely on them from attack yet leverage cyberspace for the benefit it offers those same missions.

Moreover, cyberspace is critical to Air Force and joint operations in the other war-fighting domains. Practically everything we do in warfare these days relies on cyberspace, be it providing telemetry to satellites and missiles or controlling our military forces in Afghanistan—we depend upon the cyber domain to execute operations in all of the other domains.

Designating cyberspace weapon systems calls for a tremendous resource commitment to meet the standards of air and space weapon systems. Operating to this higher benchmark requires corresponding funding and manpower greater than the cyberspace domain received as a simple communications or information technology support function. However, failure to make these commitments could prove devastating to future operations throughout every other domain. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip cyberspace forces—it is the logical evolution of cyberspace to a true war-fighting domain and a critical enabler of all other war-fighting operations.

Air and Space Operating Center Example

In the late 1990s, the Air Force designated the Falconer AOC a weapon system with little or no formal acquisition, sustainment, or requirements rigor to back it up. Basically, the chief of staff just made it a "go do." The operations community found itself backing into the requirements in much the same way we do today with our cyberspace systems. By declaring the AOC a weapon system, the Air Force sought to normalize what was basically a homegrown "county option" collection of equipment and personnel that varied from one numbered air

force to another. This thinking held that a designated weapon system would result in better training for AOC crews, better defense of the program in the program objective memorandum process, and some protection of the numbered air force's staff manpower from poaching to fill AOC billets.

In reality, the AOC funding line has suffered numerous cuts, the equipment baseline has always been problematic in terms of sustainment and modernization, and AOC manpower has remained subject to several efficiency drills, ultimately shrinking the footprint. It stands to reason that many members of the operations community would argue that classification as a weapon system has not necessarily helped the AOC.

In Air Combat Command's opinion, though, in spite of the serious challenges faced during the transition, the AOC is better off today than it was 15 years ago, especially in terms of training its crews. A dedicated formal training unit at Hurlburt Field, Florida, established a program of record, provided a rigorous configuration and change-management process, and ultimately resulted in recognition by the operations community that the AOC is the crown jewel in the joint force air component commander's tactical air control system C2 concept. Additionally, assignment to an AOC tour is no longer considered a career-ending event for rated officers—quite a change from the perception in the 1990s when an assignment to a numbered air force staff or an AOC was widely seen as the kiss of death for promotion in the rated career fields.

AFSPC would not let the initial pains of the AOC experience deter us from pushing the cyberspace weapon system concept forward. Every program (fighters, bombers, and ISR) confronted its fair share of challenges, but without a program—something with a name attached to it—cyberspace systems would always fight for scraps in money and manpower. As we integrate these cyberspace weapon systems into the Air Force construct, perhaps we can learn from the challenges of es-

tablishing the AOC weapon system and avoid the same pitfalls and mistakes.

Final Thoughts

Through the cyberspace domain, the United States exploits other war-fighting domains. Practically all warfare these days relies on cyberspace—everything from communications, precision navigation and timing, attack warning, ISR, and C2. Designating cyberspace weapon systems will help the Air Force guarantee persistent cyberspace access and mission assurance for other critical weapon systems and domains that rely on cyberspace. By doing so, the service has made a commitment that cyberspace will receive the programmatic and budgetary attention necessary to sustain cyberspace operations, support the cyber mission teams, and drive towards the JIE. Furthermore, cyberspace operations supported by core weapon systems offer increased security, performance, flexibility, and overall capability unmatched in a less normalized environment. The operationalization of cyberspace is more than just a way for AFSPC to properly organize, train, and equip the cyberspace domain—it is the logical evolution of cyberspace to a true war-fighting domain and a critical enabler of all other such domains. ✪

Notes

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 June 2013), 303, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

2. Joint Publication 3-13, *Information Operations*, 27 November 2012, II-9, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

3. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* ([Washington, DC: Mandiant, 2013]), 2, 3, 20, 59, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

4. Air Force Policy Directive 10-9, *Lead Command Designation and Responsibilities for Weapon Systems*, 8 March 2007, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-9/afpd10-9.pdf.

Brig Gen Robert J. Skinner, USAF

General Skinner (BS, Park College; MS, Oklahoma City University) is the deputy commander, Air Forces Cyber (AFCYBER). He is the primary liaison and personal representative to US Cyber Command and the National Security Agency; he also supports AFCYBER's operational activities with the Office of the Secretary of Defense, Director of National Intelligence, Central Intelligence Agency, and other National Capitol Region cyber stakeholders. Commissioned in 1989, the general is a graduate of Squadron Officer School, Command and General Staff College, Air War College, and the Industrial College of the Armed Forces. His career highlights include wing and group commands, multiple squadron commands, a variety of tactical and fixed communications assignments as well as staff assignments at the Joint Staff, Air Staff, and a numbered air force. Prior to assuming his current position, General Skinner served as inspector general at Headquarters Air Force Space Command, Peterson AFB, Colorado. In this role, he led a 70-person, three-division directorate consisting of five branches charged with evaluating the readiness of more than 300 Air Force Space Command space and cyber units located at over 100 worldwide locations.

Let us know what you think! Leave a comment!

Ira C. Eaker Award Winners

for the top *Air & Space Power Journal* articles of the past year

First Place

Lt Col Christopher J. Niemi

"The F-22 Acquisition Program: Consequences for the US Air Force's Fighter Fleet"

(November–December 2012)

Second Place

Maj Jason R. Greenleaf

"The Air War in Libya"

(March–April 2013)

Third Place

Lt Col Peter Garretson

"A Range-Balanced Force: An Alternate Force Structure Adapted to New Defense Priorities"

(May–June 2013)

Congratulations to this year's winners! The award honors airpower pioneer Gen Ira C. Eaker and is made possible through the generous support of the Air University Foundation. If you would like to compete for the Ira C. Eaker Award, submit a feature-length article to *Air and Space Power Journal* via e-mail at aspj@maxwell.af.mil. All military personnel below the rank of colonel (O-6) or government civilian employees below GS-15 or equivalent are eligible. If *ASPJ* publishes your article, you will automatically be entered in the competition.

Maintaining Space Situational Awareness and Taking It to the Next Level

Col Mark A. Baird, USAF

Without question, the United States has become increasingly reliant on space. Both economically and militarily, our dependence on space assets is undeniable. Orbiting satellites provide myriad services that we have become dependent on, such as precise position, navigation, and timing (PNT); communications; weather data; missile warning; and intelligence, surveillance, and reconnaissance (ISR). These functions have served not only as the lifeblood of the global economy over the last decade but also as key enablers in conducting the global war on terror. As the strategic focus shifts to the Pacific region, our reliance on space assets will become even more important, and preserving US space capabilities will prove critical to ensuring America's military dominance in any future conflict.[1]

After the Cold War, space became a sanctuary for the United States, which enjoyed almost complete freedom to operate within its vast realm. That situation is certainly changing, however, as many new players enter the space arena and as China begins to emerge as a near peer in space. With China integrating its military and civilian space endeavors and Russia investing in a revival of its space capabilities, both countries present challenges for the United States that we must address.[2] Although Iran and North Korea have less mature space programs, their continued intercontinental ballistic missile (ICBM) development efforts and attempts to launch satellites indicate a desire to establish a larger presence in space.[3] In addition to developing space-based communications platforms, PNT, and ISR systems, Russia, North Korea, and Iran are working to acquire systems that would effectively deny the US military's use of space by jamming Global Positioning System (GPS) satellites and other key communications links.[4] Imagine a conflict in today's high-tech warfare environment without the ability to drop GPS-guided munitions, offer persistent ISR coverage via remotely piloted vehicles over the battlefield, or detect the launch of a Scud missile. How would a conflict change if weather information over the battlefield were not available or if we had neither strategic communications nor missile warning during a hostile ICBM launch? It is vital that we preserve space-based capabilities critical to the projection of both airpower and sea-based power in the contested and congested space environment projected by the latest national threat assessment.[5]

If we wish to maintain our superiority in space, we must first have a clear picture of the environment around our space assets and be able to detect any change or potential threat—in other words, we need space situational awareness (SSA). Historically, our efforts to protect US space-based capabilities have relied upon SSA focused on space-flight safety, a mission that entails the creation and maintenance of a catalog of orbiting satellites, spent rocket bodies, and other debris used to predict and avoid potential collisions in space. This critical mission reduces the risk to our satellite launches and protects orbiting space assets (both manned and unmanned), all in an attempt to avoid a con-

junction between orbiting objects. In addition to destroying the hit satellite (resulting in loss of mission and the significant investment to deploy it), a collision in space—which can occur at speeds up to 17,000 miles per hour—has the potential to produce a large debris field and render an orbit regime unusable. Even though spaceflight safety is vitally important, an SSA concept of operations focused solely on collision avoidance does not do enough to combat the increasingly contentious environment, which includes antisatellite (ASAT) weapons, communications jammers, and sensor dazzlers.[6] The sobering bottom line is that the SSA concept of operations we have relied upon for decades can no longer sufficiently protect our crown jewels in space.[7]

This article stresses the necessity of maintaining robust SSA, arguing that, to do so, we must pivot from the traditional SSA that emphasizes catalog maintenance to a more tactical, predictive, and intelligence-driven SSA directed by an integrated Battle Management Command, Control, and Communications (BMC3) infrastructure. We must build a new space superiority enterprise around SSA sensors that utilize common data models to support rapid tasking, processing, exploitation, and dissemination across multiple classification levels. It must incorporate tactical intelligence to ensure timely characterization and identification of threats and include a robust set of executable space-control BMC3 courses of action that, given enough warning, we could utilize to mitigate a threat.

Space Race Revisited

1950s–1970s: The Dawn of Space

From the earliest days of armed conflict, military forces have endeavored to occupy the high ground of the battlefield, whether a hill, a mountain, the air, or space. Possessing the high ground has always given a military force the advantage over its adversary, regardless of the technologies or strategies of the time. With the advent of the air-

plane at the beginning of the twentieth century, air became the new high ground and air superiority the rallying cry.

Since the mid-to-late 1950s, technology has advanced to the point where space has become the ultimate high ground. As the Cold War ramped up, the American and Soviet militaries—building upon technologies originally developed to deliver ICBM-carried nuclear weaponry—launched both communications and spy satellites at the same time they built stovepiped command and control (C2) systems.[8] Space was an enabler at this point; weather satellites, communications relays, and the earliest spy satellites did not gain further significant utility until the Vietnam War.

1970s–1990: Buildup of Contested Space

During the height of the Cold War, both the United States and USSR developed and tested several ASAT weapons in an effort to gain the ability to hold adversary space assets at risk—to control space. The Soviet Union worked on a co-orbital satellite destroyer or "Istrebitel Sputnikov" throughout much of the cold war.[9] One of the most well known ASAT tests involved the direct-ascent ASAT destruction of an experimental satellite nearing the end of its operational life (the Solwind P78-1) by a US Air Force ASM-135 missile launched from a specially modified F-15 on 13 September 1985. The fighter launched the ASAT missile from a location 200 miles west of Vandenberg AFB, California, to its target 345 miles above in low Earth orbit. The 30-pound miniature homing vehicle successfully destroyed the 2,000-pound satellite, producing minimal debris, thanks to its relatively small size and low orbit. The remaining pieces of the satellite then burned up as they reentered the atmosphere. This would be the last ASAT test conducted for another two decades.[10]

1990s–2007: America's Growing Dependence on Space

> *Our experience in Desert Storm was a watershed for space power. . . . Space is now so integral to joint and combined military operations that were we to remove space assets from our military arsenal . . . we would be relegated to employing warfighting tactics much like those of World War II.*
>
> —Gen Charles A. Horner, USAF, Retired

The United States conducted a massive integration of space into the American way of war during the decade between the 1991 Gulf War and the wars in Afghanistan and Iraq of 2001 and 2003, respectively. During Operation Desert Storm, which some have called the first "space war," the breadth and scale of the utilization of space had increased significantly since the Vietnam War, both militarily and commercially.[11] The Blue Space Order of Battle (assets used in the execution of the operation plan) included 51 military and 12 commercial satellites.[12] Every space mission played a part in Desert Storm (which, by all accounts, involved the greatest deployment of satellite ground stations and pieces of user equipment in history), with each providing a significant edge to the war fighter on the ground. Even so, we had not yet fully integrated space into our concept of operations—we did not yet have GPS-guided precision munitions, robust satellite communication devices, and tactical ISR at the forward edge of the battlespace. Yet, our forces understood the edge that space systems could provide. A good example is the emergency procurement of early commercial GPS receivers, which were "duct-taped" into helicopters to aid in navigation. Just a decade later in Operations Enduring Freedom and Iraqi Freedom, we used B-52s for close air support missions called in via satellite communications by special operations troops on horseback using laser range finders integrated with the ubiquitous GPS receivers to direct munitions to a precise "danger close" point.[13]

The Importance of Space Control

Adm Alfred Thayer Mahan, one of America's foremost naval strategists, viewed Earth's oceans as a medium for force projection and commerce, which, when controlled by the appropriate strategies, policies, and doctrine, could provide a nation an advantage in economic and military terms.[14] In a similar vein, our nation's growing use of and dependence on space necessitated the development of effective policies and doctrine, as well as the tools and resources to ensure our effective and proper use of space. Taking it a step further, Admiral Mahan advocated the principle of "sea control" for the unfettered use of the oceans for a nation's purposes, an idea that directly translates to the concept of "space control." To gain superiority in space, the space control mission needed to address not only the surveillance of space but also the protection of US and friendly space systems used for battle management, communications, and intelligence, and the prevention of an adversary's ability to use space systems and services for purposes hostile to US national security interests. In 1979 the Space Defense Operations Center (SPADOC, later the Space Control Center) was established at Cheyenne Mountain, Colorado, to command and control the space surveillance network, followed by the establishment of Air Force Space Command in 1982 and the unified US Space Command in 1985. For the first time, space was viewed as a theater of operations, and many of the space control systems we are dependent on today had their genesis during those years.[15]

Soon after the first "space war" and with the demise of the Soviet Union, Russia bowed out of the space race, and the United States effectively ceased major upgrades to its space control enterprise. The SPADOC at Cheyenne Mountain received only a few minor upgrades in the years after Desert Storm. The SPADOC computer system, which still operates, will remain in its current state until a modernized replacement—the Joint Space Operations Center (JSpOC) Mission System (JMS)—comes online in 2016.

In the years after Desert Storm, America's reliance on space-based platforms became an ingrained part of our military through the use of precision-guided munitions as well as ship and aircraft navigation. We repurposed satellites originally designed for more basic objectives as global communications relays for commanding remotely piloted vehicles or platforms that relayed ISR data to the war fighter in the air, on the ground, and at sea. This dependence also permeated our civil culture, with space applications becoming part of the shipping, banking, agriculture, and entertainment industries. The loss of GPS alone would have an impact of more than $96 billion per year.[16] The satellite industry flourished as the world found new ways to use space systems—both on the military front and in the commercial sector. Faced with few challenges to our superiority in space, we rested on our laurels and enjoyed the unimpeded benefits of a burgeoning space industry.

2007–Present: Space Control at a Crossroads

On 11 January 2007, China changed the status quo in space warfare by firing an SC-19 direct-ascent ASAT missile at its own weather satellite—the Fengyun-1C.[17] The kinetic-kill vehicle, a modified version of China's DF-21 medium-range ballistic missile, and launcher system engaged the satellite at a closing velocity of approximately 17,000 miles per hour at an altitude of 537 miles—200 miles higher than the US ASAT test in 1985. Unlike the results of the 1985 US test, destruction of the refrigerator-sized Fengyun-1C created a sizable debris field—the largest in history. With that one test, the space catalog grew by over 15,000 debris particles trackable by the space surveillance network (SSN) and the JSpOC and hundreds of thousands of debris particles too small to be tracked by the SSN but still large enough to be a safety concern for human space activites in low Earth orbit.[18] Figure 1 illustrates the extent of the debris field created by destruction of the Fengyun-1C.

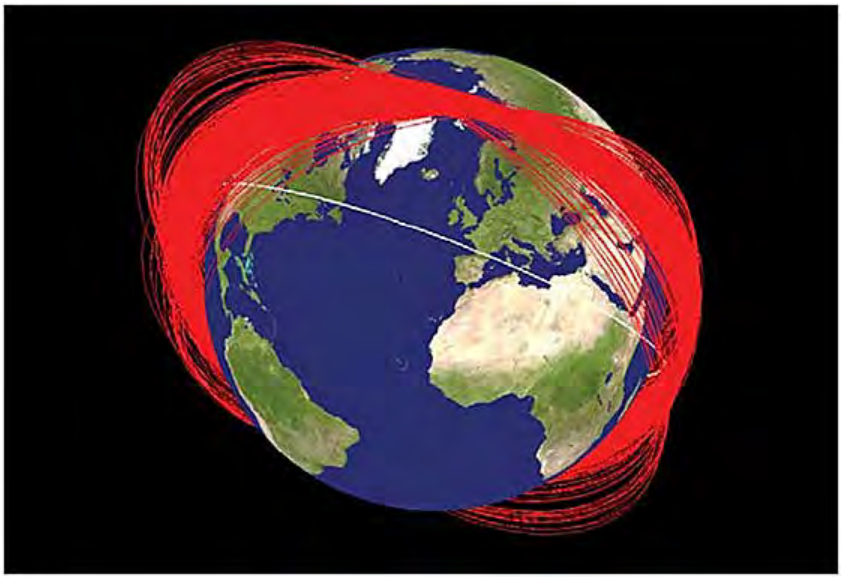


Figure 1. Representation of debris from the Fengyun-1C Chinese weather satellite. (From National Aeronautics and Space Administration, "United Nations Adopts Space Debris Mitigation Guidelines," *Orbital Debris Quarterly News*, April 2007, 2, http://orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv11i2.pdf.)

The satellite collision between the American Iridium 33 and the Russian Kosmos 2251 communications satellites over Siberia in 2009 was the first publicly confirmed hypervelocity accident between two intact artificial satellites in Earth orbit.[19] NASA estimated that the satellite collision created 1,000 pieces of debris, each larger than 10 centimeters (cm) (four inches). The debris field continued to grow, and by July 2011 the SSN had cataloged over 2,000 large fragments of debris. NASA determined that the field presented only a low risk to the International Space Station, which was orbiting approximately 430 kilometers (270 miles) below the collision course, and to the next shuttle launch (STS-119), planned for late February 2009. However, to this day, NASA assesses the potential for a collision with this debris field prior to every space launch. As recently as 22 January 2013, a piece of the Fengyun-1C from the 2007 ASAT test is believed to have hit a Russian experimental Ball Lens in the Space (BLITS) satellite, knocking it out

of its useful orbit.[20] In light of America's unquestioned dependence on its space assets, it is absolutely critical to the nation that we gain and maintain SSA—to detect, track, and identify orbiting assets as well as any other threat to our systems and to perform conjunction assessments within a time frame and with sufficient certainty to take action to avoid any threat, whether accidental or intentional.

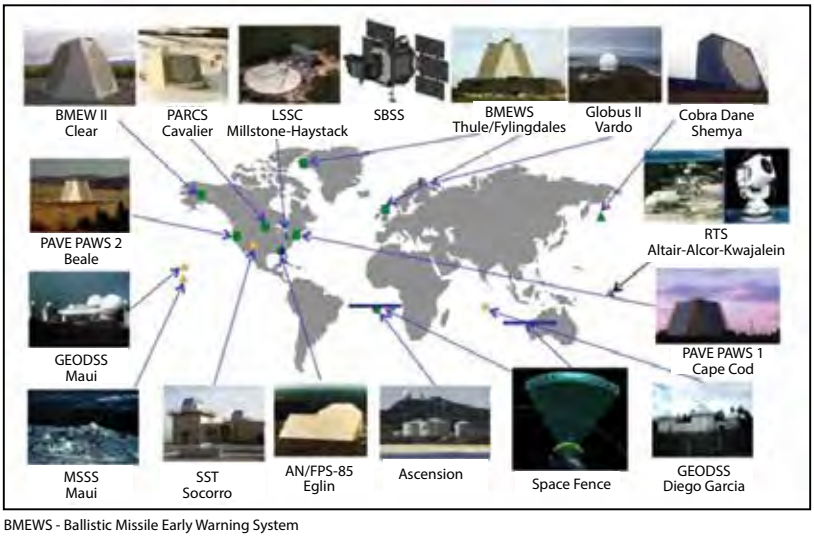
Space Superiority Enterprise

Current SSA Concept of Operations: Routine Catalog Maintenance

At present, the SSA mission focuses on the ability to view, understand, and predict the physical location of natural and man-made objects in orbit around Earth with the objective of avoiding collisions. The Secure World Foundation reports 450 operational satellites and more than 10,000 pieces of trackable debris at low Earth orbit, 55 operational satellites and over 500 pieces of trackable debris at medium Earth orbit, and 400 operational satellites and in excess of 1,000 pieces of trackable debris at geostationary orbit. The JSpOC has the best orbital tracking network in the world with a catalog of more than 21,000 resident space objects greater than 10 cm in size.[21] However, we must also contend with at least 500,000 bits of debris of 1–10 cm and another several hundred million bits smaller than 1 cm. Moving at orbital velocities of thousands of miles per hour, any of these objects could pose a threat as more manned and unmanned spacecraft are launched and exposed to a debris field growing at an alarming rate. This problem affects the United States and all other spacefaring entities—both government and commercial.

We track the location of satellites and space debris with a collection of radars and telescopes (fig. 2), many of which are quite old and were not built with SSA as a primary mission. Ground radars such as Globus II, Millstone/Haystack, ALTAIR/TRADEX, the Ballistic Missile Early Warning System, the Perimeter Acquisition Vehicle Entry Phased Ar-

ray Warning System, and the Perimeter Acquisition Radar Attack Characterization System all have a pedigree in missile warning from the days when the SPADOC was located within Cheyenne Mountain. Originally, the US Army built and operated the ALTAIR radar between 1968 and 1970 at the Reagan Test Site on Kwajalein Atoll to simulate Soviet radar capabilities.[22] Over time, it became apparent that radars could be repurposed or dual-purposed for the SSA mission. Much of our current SSA network is built upon cooperative agreements between government entities in order to fully leverage systems that support multiple missions. Several efforts are in progress to expand this cooperation to global partners, including friendly nations and commercial entities, as a means of increasing our efficiency in monitoring the global space environment. One such example, the new S-Band Space Fence, is scheduled to come online in 2017 and will assume a critical role within the SSA network.[23]



BMEWS - Ballistic Missile Early Warning System
GEODSS - Ground-Based Electro-Optical Deep Space Surveillance
LSSC - Lincoln Space Surveillance Complex
MSSS - Maui Space Surveillance System
PARCS - Perimeter Acquisition Radar Attack Characterization System
PAVE PAWS - Perimeter Acquisition Vehicle Entry Phased Array Warning System
RTS - Remote Tracking Station
SBSS - Space Based Space Surveillance
SST - Space Surveillance Telescope

Figure 2. Space surveillance network (2012) and notional additions

In addition to ground radars, optical systems are essential contributors to the SSA mission. The Ground-Based Electro-Optical Deep Space Surveillance (GEODSS) system, which has operational sites in New Mexico, Hawaii, and Diego Garcia, can track objects as small as a basketball more than 20,000 miles away in space. The GEODSS plays a vital role in tracking space objects, particularly those in deep space. Over 1,200 objects are in deep space in medium Earth orbit, geostationary orbit (GEO), and highly elliptical orbits. At GEO are the vitally important strategic and wideband communications and missile warning satellites. The Space Surveillance Telescope—an advanced ground-based optical instrument—can search an area in space the size of the United States in seconds and can scan the geostationary orbit belt multiple times per night. It has a field of view three times better than that of the most capable GEODSS, and each night the telescope captures more than 1 terabyte (1 billion bytes) of data. Given this large amount, it is important that we have adequate capabilities on the ground to process and use the information. In the very near future, as new radars and optical sensors come online, the JMS will be the glue that binds the new and legacy capabilities, allowing us to best utilize the data they provide.

Ground-based radar and optical systems are the workhorses of the SSN for characterizing objects in space, but they are limited by weather, solar blind spots, and their geographical location on Earth. In order to augment these limitations and exploit the ultimate high ground of space, the United States launched the Space Based Space Surveillance System in 2010. The most capable of the SSN sensors, this system provides high capacity and agility, collecting day or night above the weather and improving revisit rates of objects.

Ground optical, ground radar, and space optical systems provide a critical contribution to achieving SSA, but each has inherent limitations. Thus, the United States must have all three components in order to gain and maintain robust SSA. Given our dependence on space, it is imperative that we effectively resource and utilize our SSA sensor net-

work to provide the knowledge we need to enable the safe operation of our on-orbit fleet.

Future SSA: Rapid Characterization of Emerging Threats

Because of emerging threats, the SSA mission must move beyond routine catalog maintenance towards a predictive, time-critical BMC3 environment. The Defense Intelligence Agency's national threat assessments to the Senate Armed Services Committee in 2012 and 2013 both cited China's growing, increasingly capable military space efforts.[24] In its 2013 *Annual Report to Congress*, which detailed China's military developments, the Office of the Secretary of Defense highlighted that country's "multi-dimensional program to improve its capabilities to limit or prevent the use of space-based assets by adversaries during times of crisis or conflict."[25]

From the counterspace perspective, Russia and China continue to develop systems and technologies that can interfere with or disable vital US space-based navigation, communications, and intelligence-collection satellites. North Korea has mounted Soviet-made jamming devices on vehicles near the North-South demarcation line that can disturb GPS signals within a radius of 50–100 kilometers. Reportedly, it is also developing an indigenous GPS jammer with an extended range of more than 100 kilometers. Other state and nonstate actors rely on denial and deception techniques to defeat space-based imagery collection, conduct electronic warfare or signal jamming, and possibly attack ground sites for space assets.[26] It is critical that the United States ensure the capability to rapidly understand when and where its space systems are compromised.

Today's Command and Control: Modernizing the Space Defense Operations Center

The JMS program, the cornerstone of the space superiority enterprise, will replace the 1980s-era SPADOC system as the C2 system that

focuses on planning and executing US Strategic Command's joint functional component command for the space mission. Unlike other AOC systems, the JSpOC has specialized C2, SSA, and ISR capabilities in support of space control that make inroads into many mission areas.

The JSpOC can be thought of as a combination air traffic control center and AOC but with a span of control extending 22,236 miles outwards into space. For the sake of comparison, an air traffic controller in a tower is responsible for aircraft flying within a 200 nautical mile range of the tower and up to 10,000 feet in altitude—an effective volume of 315,000 cubic miles. Between Earth and the Geostationary Belt, the effective volume of control is 46 trillion cubic miles—about 150 million times as much volume to control! To exacerbate the problem, space offers unique physics limitations, such as a sun-induced blind spot that can render sensitive optics useless for multiple hours per day and vast distances across which electromagnetic waves must travel. Such factors make it difficult to obtain radar returns from which we can glean accurate range measurements and identification of space objects. To undertake the complex and computationally intensive job of integrating data from our sensor platforms and fusing a useful SSA picture, the current JSpOC operator relies on disparate—in most cases, antiquated—technology platforms such as the SPADOC computer system; Astrodynamics Support Workstation; and Command, Analysis, and Verification of Ephemerides Network (CAVENet).[27] Given the growth in the number of spaceborne objects posing a threat to the space systems upon which we so heavily rely, conducting our SSA mission with these legacy systems is not an acceptable way to move forward.

The JMS will replace the legacy SPADOC and ASW processes and capabilities with a modernized, scalable, extensible, and sustainable platform upon which to build the SSA mission set that the United States requires for the twenty-first century. To meet the legacy-replacement goal, the JMS program is developing a government service-oriented architecture (SOA) infrastructure that supports the integration of mission applications while acquiring mature, commercially developed

government mission applications. Building the JMS on a robust, disciplined SOA platform is essential to making sure that the JSpOC can evolve over time with new functionalities replacing outdated services and revised software applications integrating new operator-defined tactics, techniques, and procedures. Future capabilities required by the JSpOC after 2015 will call for the development of new applications and procedures as well as the exploitation of new SSA data sources. Further, we can assume that operators will find innovative ways of using the system's capabilities not imagined when the system was designed—they always do. JMS must enable the JSpOC to exploit this learning.

This is one of the key objectives for the JMS—better, faster, and extensible data integration with a wider variety of data sources. In contrast to the SPADOC system, we expect the JMS to accept and integrate not only traditional SSN tracking data, including information from US missile-warning radars, but also nontraditional formatted observations and ephemerides from a variety of sources, positional data derived from satellite telemetry, and tracking data from foreign sensors. In many cases, the data will be delivered net-centrically, based on work with the Net-Centric Sensors and Data Sources effort, intended to expose such sources.[28]

Pivoting to Space Battle Management Command, Control, and Communications

The Iridium/Kosmos collision in 2009 and the BLITS conjunction of 2013 remind us that poor SSA is not an option. Moreover, in light of the rising number of spacefaring nations (e.g., China, North Korea, and India), clearly space is becoming more crowded. Because some nations have both stated and demonstrated their intent to attack our dependence on space, we must be able to protect our assets.[29] If America intends to maintain its status as the most capable space nation, then—in the face of growing threats—we must evolve our SSA paradigm to do

more than just routine catalog maintenance and monitoring of potential conjunctions. Like its AOC counterpart, the space community needs to develop a BMC3 capability that includes AOC-like analysis, data fusion, and identification of threats.

The routine (peacetime) timelines associated with developing our catalog-maintenance-focused SSA are not sufficient to respond to or even anticipate a would-be adversary's attack in time. Before the joint functional component command for space could start formulating courses of action in response to an on-orbit event—such as a satellite conjunction, debris breakup, or a potential ASAT—decision makers at the satellite operations centers and at the JSpOC would need to develop a timely operational picture of the situation in space. The latter would include all ground assets that can affect objects in space, on sufficient timelines within which to perform observe-orient-decide-act analysis and reach "act" decisions from the appropriate levels in the chain of command—no easy task.

Elements within Air Force Space Command have begun to examine this issue through "kill-chain" analysis—an in-depth examination of technological needs, materiel solutions, procedural changes, ISR requirements, and concepts of operations necessary for a decision maker to execute a course of action that has been planned for, exercised, and refined by space operators. The kill-chain analysis calls for elements of traditional C2; however, now that space is no longer a sanctuary and response timelines are being compressed more than they have been in the history of space control, our C2 must become even more tightly integrated with communications nodes outside the JSpOC—at the National Air and Space Intelligence Center, National Security Agency, National Reconnaissance Operations Center, or any organization with the requisite space control, ISR, or space warfare expertise. This modern C2—or C3 when merged with communications—is essential for effective crisis management. The convolution of battle management and C3—BMC3—is what the space superiority enterprise needs in this era of contested, congested, and competitive space control. Space BMC3

goes beyond a routine, steady-state picture, creating a tactical monitoring posture for high-interest items that can affect space assets. With timely indications-and-warning systems, the enterprise can tailor its prepared responses to tactical events without sacrificing its global commitments to catalog maintenance (fig. 3).

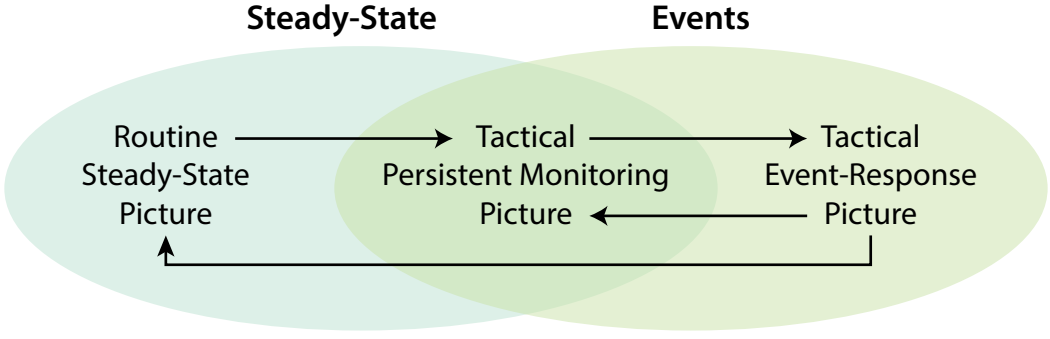


Figure 3. Transitioning the operations tempo of space situational awareness

This new space posture demands much more than upgrades to legacy hardware and software. To enhance current operations, the Space Superiority Systems Directorate has teamed with the JSpOC, US Strategic Command, and other combatant commands in designing and exercising new and evolved tactical scenarios. We use collaborative "scrimmages" to extract and exercise exactly how and which parts of currently operational and prototype systems will support a particular crisis scenario. The exercises make use of test-bed and prototype analyst tools, reducing overall execution risk by buying down technical risk, smoothing out integration schedule risks, providing exercise-quality feedback on potential real-world performance for prioritization purposes, and opening up tactical-response problems for an expanded community of research-and-development problem solvers.

Despite these great strides in evolving the space superiority mission to enhance its flexibility to change, we must take care to ensure that currently static tasking processes become flexible and adaptive to rapidly evolving threats. These processes need to account for the integra-

tion of nontraditional sensors into the JSpOC SOA and the operator's workspace. Data will be delivered to the JSpOC in various formats and classification levels. The JSpOC SOA platform will interpret and fuse the data, feeding them to space operators and intelligence analysts through a user-defined operating picture at the speed of need—not with the hours or even days of delay with which we currently operate. As the volume of data available to the space operator grows, it becomes more important to rapidly collect, process, and exploit the information, using methods not yet refined. This capability exists today, but we need to automate it for execution without intervention by the developer or a cadre of engineers. The data will be compatible with various systems through agreed-upon exchange formats and have outputs that can be readily shared among military and civilian operators. Intelligence operators will have to exploit data on the fly through tactical timelines and rapidly disseminate raw intelligence through net-centric means to operators around the world who can interpret information through their user-defined operating picture.

In this new space posture, the roles of some of our existing capabilities will require adjustment. Intelligence assets already play a critical role in characterizing assets in space and focusing indications and warning resources. Although they already lay the groundwork for planning courses of action in space, they are moving into a new role of tactical corroboration and attribution of space events. Take the air world example of foundational intelligence sources discovering information about a potential adversary's new developmental aircraft. The intelligence community would then use its resources and expertise to determine the capabilities and exquisite features of the new threat. This foundational intelligence collection is critical and long term, but after the aircraft is produced and enters operations, a different type of intelligence is necessary—one that concentrates on rapid and fleeting collection of very sparse data as an adversary actively tries to avoid detection. The ultimate goal of collectors at this point is not high-fidelity pictures but quick fingerprinting (e.g., which of the threats does this match?). We can do this, but we must emphasize timeliness. A pleth-

ora of information systems already makes intelligence assets available. We need to integrate these systems seamlessly into a series of tactics, techniques, and procedures that offer decision-quality information on requisite timeliness.

Future Architecture

To maintain space superiority, we must tightly couple BMC3, SSA, and tactical intelligence in an architecture that enables decision makers to select courses of action in hours rather than days. Today's BMC3, SSA, and space-control architectures are loosely coupled, but future architectures must have tighter integration. A number of materiel solutions could be integrated into a space superiority architecture. Sequestration hinders our ability to upgrade current capabilities and match those of would-be adversaries; consequently, we must be creative in designing a space superiority architecture for 2020 and beyond.

Like C2 systems in the air world, space superiority BMC3 systems should evolve by leveraging ISR data within federated SOAs and data-mining systems. Advances in modern computing make it possible to sort through terabytes of information from many different sources and process these data into actionable information for decision makers. These data must fit within a common data model for exchange among a variety of computing systems. Delivery of the initial SOA in the first increment of JMS, as well as subsequent improvements in future increments, will facilitate cross-domain developments that will allow the JSpOC to connect with AOCs around the world and share BMC3 data at the speed of need.

Air Force and intelligence community agencies have been moving ISR data-fusion centers away from stovepiped systems (e.g., the distributed common ground/surface system [DCGS] and Global Command and Control System [GCCS]) to federated SOAs such as today's DCGS SOA and the GCCS replacement—Joint Command and Control. Moving to interconnected, federated SOAs allows only a limited opportu-

nity to try out new data-fusion techniques between SOAs. To address this, the Space Superiority Systems Directorate and the Air Force Research Laboratory are collaborating in building the Action-Centered Rapid Collaborative Application Development Environment (ARCADE) as the key risk-reduction tool for future JSpOC needs. ARCADE will run the most current JSpOC software edition, which will mimic the operational SOA at multiple levels of security and enable commercial developers, other government entities, universities, and so forth, to test and develop applications (using the common data model and software development tool kit) that we could use in future JMS software releases. This collaborative development environment will reduce risk by allowing new technologies to mature before being inserted into the software integration process and hence into the operational SOA, while still allowing testing in an operationally relevant environment. JSpOC operators will gain insight into the ARCADE, and their feedback on candidate upgrades will be a key input to the Requirements and Planning Council—the requirements-setting body within the JMS enterprise. Through the ARCADE and council process, future JSpOC operators and acquisition leaders in the Space Superiority Systems Directorate can move BMC3 towards a more seamless integration of space and air ISR, giving decision makers the complete, robust, and timely SSA needed in a contested, congested, and competitive space environment.

Conclusion

To maintain space superiority in the face of a changing environment, the United States must find a way to extend the capabilities of current C2, SSA, and ISR systems while investing in new, more capable, but resilient systems to control an increasingly congested environment. More than 1,000 satellites and hundreds of thousands of pieces of debris orbit Earth within an area of 46 trillion cubic miles (fig. 4). With other nations constantly challenging America's status as the leader of the pack in space superiority, maintaining a robust suite of

ground- and space-based sensors from which to gather data to build our SSA picture is a paramount imperative.

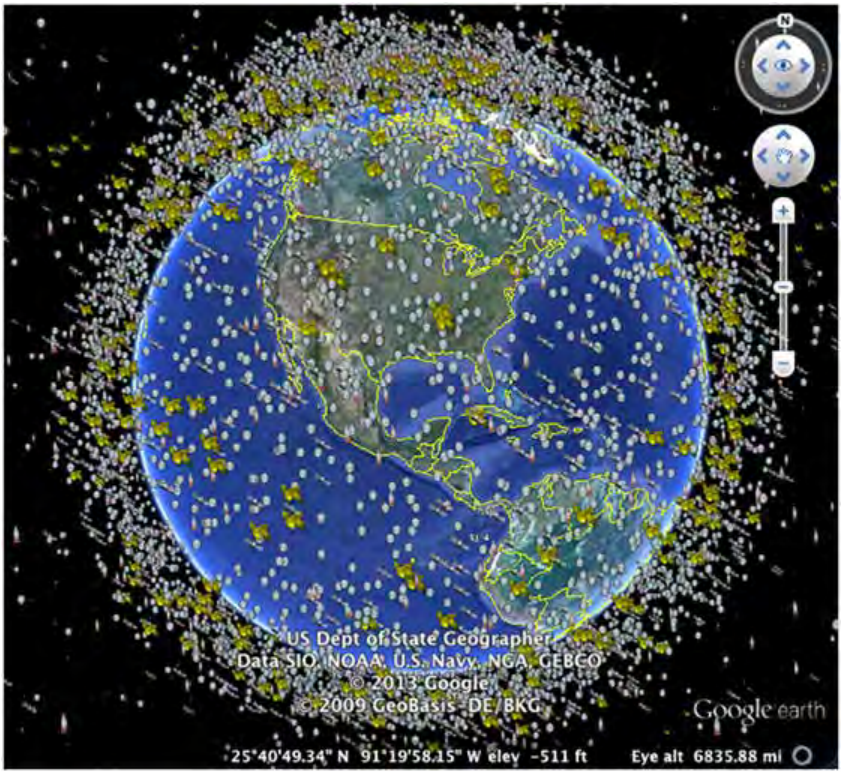


Figure 4. Computer model (not to scale) of man-made debris in low Earth orbit. (From "LEO Images," NASA Orbital Debris Program Office, 2 October 2012, http://orbitaldebris.jsc.nasa.gov/photogallery/beehives.html#leo.)

Better protection of our national interests in space demands that we pivot away from the current metric-track catalog maintenance / forensic analysis focus towards a seamless integration of SSA, BMC3, and air/space ISR. The key difference is that C2 implies a mind-set based on a stable, uncontested space environment with hours or even days of response time while BMC3 requires a mind-set of enabling near-real-time decision making in the face of rapidly changing events that affect national security and America's trillion-dollar space investment.

Thanks to more capable sensors and C3 systems, the space battle-management center of the future will be better at processing future events, more easily upgraded, and able to seamlessly integrate exponential growth in ground, air, and space ISR. Safeguarding US national security satellites depends upon continued support from the entire space community as we work together to operate and counter attempts by China, Russia, Iran, and North Korea to disrupt, deter, and deny our safe and continued access to space—in peacetime and during conflict.[30] ✪

Notes

1. President Barack Obama (remarks before the Australian Parliament, 17 November 2011), http://www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament.

2. Mark A. Stokes with Dean Cheng, *China's Evolving Space Capabilities: Implications for U.S. Interests* (Washington, DC: US-China Economic and Security Review Commission, 26 April 2012), http://project2049.net/documents/uscc_china-space-program-report_april-2012.pdf.

3. Senate, *Annual Threat Assessment, Ronald L. Burgess Jr., Lieutenant General, USA, Director, Defense Intelligence Agency, Statement before the Senate Armed Services Committee*, 112th Cong., 2nd sess., 16 February 2012, http://www.dia.mil/public-affairs/testimonies/2012-02-16.html.

4. Ibid.; Senate, *Annual Threat Assessment, Michael T. Flynn, Lieutenant General, U.S. Army, Director, Defense Intelligence Agency, Statement before the Senate Armed Services Committee*, 113th Cong., 1st sess., 18 April 2013, http://www.armed-services.senate.gov/statemnt/2013/04%20April/Flynn_04-18-13.pdf; "Russia Delivers Radar Jammers to Iran," *Space Mart: Space Industry News*, 25 October 2011, http://www.spacemart.com/reports/Russia_delivers_radar_jammers_to_Iran_999.html; and Patrick Winn, "North Korea's GPS Jammer Brigade," *Global Post*, 16 September 2011, http://www.globalpost.com/dispatch/news/regions/asia-pacific/110916/north-korea%E2%80%99s-gps-jammer-brigade-spy-plane.

5. Senate, *Worldwide Threat Assessment of the US Intelligence Community, James R. Clapper, Director of National Intelligence, Statement for the Record to the Senate Select Committee on Intelligence*, 113th Cong., 1st sess., 12 March 2013, http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.

6. Sensor dazzlers are directed-energy weapons intended to temporarily blind or disorient their target with intense, directed radiation.

7. AU-18, *Space Primer* (Maxwell AFB, AL: Air University Press, September 2009), 68–72, 273–81, http://space.au.af.mil/au-18-2009/au-18-2009.pdf.

8. "Stovepiped" refers to the design and creation of a system in isolation, without regard to future connectivity or integration with other systems.

9. Anatoly Zak, "Spacecraft: Military; IS [Istrebitel Sputnikov] Anti-satellite System," Russianspaceweb.com, 24 December 2012, http://www.russianspaceweb.com/is.html.

10. Dr. Raymond L. Puffer, "The Death of a Satellite," Air Force Flight Test Center Moments in History, 13 September 1985, http://web.archive.org/web/20031218130538/www.edwards.af.mil/moments/docs_html/85-09-13.html; and Craig Covault, "China's Asat Test Will Intensify U.S.-Chinese Faceoff in Space," *Aviation Week and Space Technology*, 21 January 2007, http://web.archive.org/web/20070127122105/http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/aw012207p2.xml.

11. "Desert Storm: The First Space War," in *Gray Space and the Warfighter*, 17 June 1997, http://www.au.af.mil/au/awc/awcgate/grayspc/dstorm/dstorm.htm.

12. Ibid.

13. Maj Michael J. Muolo, *Space Handbook: A War Fighter's Guide to Space*, vol. 1 (Maxwell AFB, AL: Air University Press, 1993), chap. 5.

14. AU-18, *Space Primer*, 137.

15. Benjamin S. Lambeth, "A Short History of Military Space," *Air Force Magazine*, December 2004, http://www.airforcemag.com/MagazineArchive/Pages/2004/December%202004/1204space.aspx.

16. Nam D. Pham, PhD, *The Economic Benefits of Commercial GPS Use in the U.S. and the Costs of Potential Disruption* (Washington, DC: NDP Consulting Group, June 2011), 2, http://www.saveourgps.org/pdf/GPS-Report-June-22-2011.pdf.

17. Shirley Kan, *China's Anti-satellite Weapon Test*, CRS Report for Congress RS22652 (Washington, DC: Congressional Research Service, 23 April 2007), http://fpc.state.gov/documents/organization/84322.pdf.

18. National Aeronautics and Space Administration, "An Update of the FY-1C, Iridium 33, and Cosmos 2251 Fragments," *Orbital Debris Quarterly News* 17, no. 1 (January 2013): 4–5, http://orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv17i1.pdf.

19. National Aeronautics and Space Administration, "Satellite Collision Leaves Significant Debris Clouds," *Orbital Debris Quarterly News* 13, no. 2 (April 2009): 1–2, http://orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv13i2.pdf.

20. Leonard David, "Russian Satellite Hit by Debris from Chinese Anti-satellite Test," Space.com, 8 March 2013, http://www.space.com/20138-russian-satellite-chinese-space-junk.html.

21. Brian Weeden, *Going Blind: Why America Is on the Verge of Losing Its Situational Awareness in Space and What Can Be Done about It* (Broomfield, CO: Secure World Foundation, 10 September 2012), 10, http://swfound.org/media/90775/going_blind_final.pdf.

22. Philip A. Ingwersen and William Z. Lemnios, "Radars for Ballistic Missile Defense Research," *Lincoln Laboratory Journal* 12, no. 2 (2000): 245–66, http://www.ll.mit.edu/publications/journal/pdf/vol12_no2/12_2ballisticmissiledefense.pdf.

23. Senate, *Space Acquisitions: DOD Faces Challenges in Fully Realizing Benefits of Satellite Acquisition Improvements, Statement of Cristina T. Chaplain, Director, Acquisition and Sourcing Management, before the Subcommittee on Strategic Forces, Committee on Armed Services*, 112th Cong., 2nd sess., 21 March 2012, http://www.gao.gov/assets/590/589500.txt.

24. Senate, *Annual Threat Assessment*, 16 February 2012; and Senate, *Annual Threat Assessment*, 18 April 2013.

25. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2013* (Washington, DC: Office of the Secretary of Defense, 2013), 9, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

26. Senate, *Annual Threat Assessment*, 18 April 2013.

27. The heaviest computations are performed on the ASW, a suite of software applications hosted on CAVENet that provides the higher-accuracy satellite catalog needed for a conjunction assessment of spaceflight safety. "Ephemerides" is a table giving the coordinates of a celestial body at a number of specific times during a given period. CAVENet is a legacy system used by the JSpOC consisting of early 1990s-era Silicon Graphics Incorporated workstations and servers. It is an off-line mission support system used for several space surveillance tasks and in-depth analysis.

28. Maj Michael Morton and Mr. Timothy Roberts, "Joint Space Operations Systems (JSpOC) Mission System (JMS)" (presentation, Advanced Maui Optical and Space Surveillance Technologies Conference, 2011), http://www.amostech.com/TechnicalPapers/2011/SSA/MORTON.pdf.

29. Senate, *Annual Threat Assessment*, 18 April 2013.

30. Andrea Shalal-Esa, "Pentagon Cites New Drive to Develop Anti-satellite Weapons," Reuters, 7 May 2013, http://www.reuters.com/article/2013/05/07/us-pentagon-satellites-idUSBRE94614E20130507; and Senate, *Worldwide Threat Assessment*.

Col Mark A. Baird, USAF

Colonel Baird (BS, Florida State University; MS, University of Arkansas) is the director of the Space Superiority Systems Directorate at Los Angeles AFB, California. In this position, he directs the acquisition of space control systems to equip US forces with the capabilities to gain, maintain, and exploit space superiority. He manages a multi-billion-dollar budget, leading a 350-person program office and 1,000-person industry team at multiple locations throughout the country to support operational systems worldwide. Colonel Baird directs the planning, development, testing, deployment, and sustainment of a complex and dynamic portfolio of space superiority capabilities of the highest national priority. He entered active duty in 1989 as a distinguished graduate of the Air Force Reserve Officer Training Corps program at Florida State University. During his career, he has served in a variety of acquisition positions, including contingency contracting officer, procuring contracting officer, program manager, headquarters staff officer, squadron commander, and senior materiel leader. Colonel Baird also has served in fellowships on Capitol Hill and with industry.

Air Force Cyber Warfare

Now and the Future

Col William J. Poirier, USAF
Maj James Lotspeich, PhD, USAF*

I think most people today understand that cyber clearly underpins the full spectrum of military operations, including planning, employment, monitoring, and assessment capabilities. I can't think of a single military operation that is not enabled by cyber. Every major military weapon system, command and control system, communications path, intelligence sensor, processing and dissemination functions—they all have critical cyber components.

—Gen William L. Shelton
Commander, Air Force Space Command

Modern-day cyber warriors are elusive figures. Are they technological ninjas, typing feverishly on a keyboard in a darkened room or perhaps gunslingers throwing cyber bullets

*Additional contributors to this article include Col Douglas Coppinger; Lt Col Michael Birdwell, 91 NWS/CC; Lt Col Brian Denman, 690 NSG/CD; Lt Col Paul Williams, 26 NOS/CC; Lt Col Joseph Zell, 33 NWS/CC; Maj Brian Balazs, 26 0SS/DO; Maj Christopher Corbett, 315 NWS/DO; Mr. Richard DeLeon, 26 NOG/TA; and Mr. Richard White, 67 NWW/TA.

downrange at shadowy foes? There are many images of cyber warfare in popular culture. Most of them focus on the individual's uncanny grasp of technology—the ability to exploit any system with a dizzying flurry of keystrokes or to fend off adversaries with a smartphone, a paper clip, and an ingenious plan. These socially awkward heroes and heroines fill the silver screen with visions of a new kind of warfare.

Contradicting these stereotypes, Air Force cyber operations are carefully planned and controlled by disciplined, rigorously trained operators. Rather than acting alone, these professionals produce effects in support of national interests through teamwork, careful coordination, and deliberate, considered targeting based on established national policy. This article discusses the events and thinking that have resulted in today's cyber forces, describes how they operate in cyberspace today, and presents a vision for how they will continue to provide cyberspace dominance in future wars. Although many of the cyber warfare capabilities of tomorrow are speculative in nature, the enabling technologies and policies for them exist today.

A Brief History of Cyber

> *If we could first know where we are, and whither we are tending, we could then better judge what to do, and how to do it.*
>
> —President Abraham Lincoln

Traditionally associated with the explosive growth of network and computing equipment in the 1990s, cyberspace was commonly used to achieve operational objectives during World War II. For example, in the Battle of the Beams, German bombers navigated from continental Europe to Great Britain by following a radio signal transmitted from the point of origin. The pilots would know they were above their targets when they intercepted a second beam, also transmitted from continental Europe. This system ensured that German night raiders found their targets in the dark and returned home safely. British engineers quickly

discovered the German use of radio frequency and developed countermeasures. By broadcasting similar signals at precise times, British cyber operators fooled the German bombers, causing them to drop their ordnance at a location chosen by the British. Similarly, the British cyber countermeasures made return trips nearly impossible for the Germans, many bombers never finding home base and a few even landing at Royal Air Force fields, their pilots thinking that they had returned home.[1] This use of the frequency spectrum (a critical portion of cyberspace) to create effects illustrates the operational power of cyberspace long before anyone considered it a domain.[2]

Thus, military operations as far back as World War II incorporated aspects of cyberspace into operations, but almost 60 years passed before leaders formally recognized the importance of this domain. In 2003 President George W. Bush released the *National Strategy to Secure Cyberspace*, followed in 2006 by the *National Military Strategy for Cyberspace Operations*.[3] These two documents established the strategic importance of cyberspace to national interests, but they did not form in a vacuum. To understand how cyberspace began to coalesce conceptually and how leaders began to understand its important role in modern military operations, we must first look at how we've arrived at our current perspective on cyberspace and cyber warfare.

Before cyberspace earned recognition as an operational domain of warfare, the military considered information a target and an instrument of war. In 1993 the Air Force established the Air Force Information Warfare Center (AFIWC) as "an information superiority center of excellence, dedicated to offensive and defensive counter information and information operations."[4] Lessons learned from Operation Desert Storm led to the realization that information is vital to modern military operations and, as such, must be defended from adversaries.[5] By the same token, exploitation of enemy information can be a viable option for gaining an operational advantage.

An attack on Air Force networks by unknown adversaries validated this viewpoint. During the "Rome Lab incident" of March 1994, admin-

istrators at Rome Laboratory, New York, found an unauthorized wiretap program—a "sniffer"—on their network that had stolen lab employees' user names and passwords. The attackers—a 16-year-old from the United Kingdom and an unknown person identified only as "Kuji"—successfully obtained information on a number of sensitive defense research projects and used the Rome Lab connection to attack other institutions, stealing all of the data stored on the Korean Atomic Research Institute's computers and depositing it in the Rome Lab computers.[6]

This incident as well other high-profile attacks of the time, such as the theft of data concerning the Strategic Defense Initiative from the Lawrence Berkeley National Laboratory, led to a debate among the Air Force staff regarding whether or not to incorporate the tools and techniques under development at the AFIWC as war-fighter capabilities.[7] On 15 August 1995, the debate ended when the Air Force chief of staff directed development of an information warfare squadron to support Ninth Air Force's combat operations. As a result, the service established the 609th Information Warfare Squadron in October 1995 with a mission to "conceive, develop, and field Information Warfare combat capabilities in support of a Numbered Air Force."[8]

The squadron pioneered defensive counterintelligence operations from 1995 through 1999 and then transferred its mission to the Air Force computer emergency response team, a subdivision of the AFIWC.[9] During this time, a number of events—exercise Eligible Receiver and operations Solar Sunrise and Moonlight Maze—led to an increased interest in information operations at the Department of Defense (DOD) level.[10] Eligible Receiver highlighted critical vulnerabilities in US Pacific Command's systems as well as in 911 and power grids in nine US cities. Analysts were still digesting the results of this exercise when officials discovered attackers stealing tens of thousands of files from systems at the Pentagon, National Aeronautics and Space Administration, and Department of Energy.[11] Detection of additional exploitations of known vulnerabilities in the DOD's unclassified networks further highlighted the need to develop indicators and

warnings of attack as well as organize to address weaknesses in information warfare operations.[12]

To address these shortfalls, the DOD activated Joint Task Force–Computer Network Defense under Maj Gen John "Soup" Campbell in December 1998, reporting directly to the secretary of defense and envisioned as having a war-fighting role.[13] In 2000 the task force took on an additional offensive role and a new name—Joint Task Force–Computer Network Operations—to reflect this change. The DOD adjusted the mission again in 2004, this time adding management as well as defense of the department's networks. The offensive mission moved to a new organization, Joint Forces Component Command–Network Warfare.[14] Finally, in 2009 the establishment of United States Cyber Command (USCYBERCOM) rejoined both organizations under a single subunified command.[15]

Although the history of cyber is full of organizational changes, we have little documentation of why the military chose to organize as it did to address cyberspace challenges. Attacks on military networks such as Moonlight Maze and Solar Sunrise provide insight only into why defensive operations were necessary, but the organizational changes also reflect a shifting concept of the interactions among defensive, offensive, and network management operations in the realm of cyberspace. Additionally, the evolution from information warfare to cyber warfare indicates a subtle shift in mission: from information as a commodity; to attack and defense of the systems used to process, store, and transmit information; and finally to the domain in which those systems and the information they manipulate reside.

Cyber Warfare Today

Reflecting the military's changing understanding of the nature of cyber warfare, today's operations are defined by a mixture of mature and developing capabilities, doctrine, and organizations. As with air and space domains at their inception, the cyberspace domain continues to

mature along a trajectory of increasing capability and capacity; however, many shortfalls exist. Fortunately, military leaders understand them and are sharing their perspective in the national debate. For example, in *Cyber Vision 2025*, Mark Maybury, the former chief scientist of the Air Force, describes the technological, policy, and personnel changes necessary through 2025 to realize future Air Force cyber capabilities.[16] Gen Michael Hayden, USAF, retired, former director of the National Security Agency and Central Intelligence Agency, discusses 10 questions that must be answered before we can truly integrate cyber into national instruments of power.[17] In a recent symposium sponsored by the Armed Forces Communications and Electronics Association, Gen William Shelton, commander of Air Force Space Command, addressed the steps taken by his command to operationalize and integrate cyber forces as well as the issues we face in the near term.[18] Similarly, Maj Gen Suzanne Vautrinot, the former commander of Twenty-Fourth Air Force, now retired, outlined the challenges and strategies for increasing defensive and offensive capabilities in a constrained fiscal environment.[19] The combined efforts of these and many other senior Air Force leaders are driving the maturation of the service's cyber operations by accelerating the pace of innovation.

The Air Force's cyber capability exists on a continuum (see the figure below) ranging from nascent and niche effects to proactive and responsive support of combatant commanders. In today's cyber force, operators occupy the middle of this continuum with niche targets included in operation plans and a mixture of proactive and reactive defensive capabilities. To move combat effectiveness to the right on this chart, the Air Force must implement future initiatives such as USCYBERCOM's cyber mission force structure and the joint information environment architecture, both of which will enhance the ability of cyber forces to provide theater- and campaign-level support. The Air Force also will continue ongoing initiatives, including Air Force Network (AFNet) migration, and the maturation of cyber weapon systems to increase cyber capacity in terms of the number of missions conducted in support of war fighters.

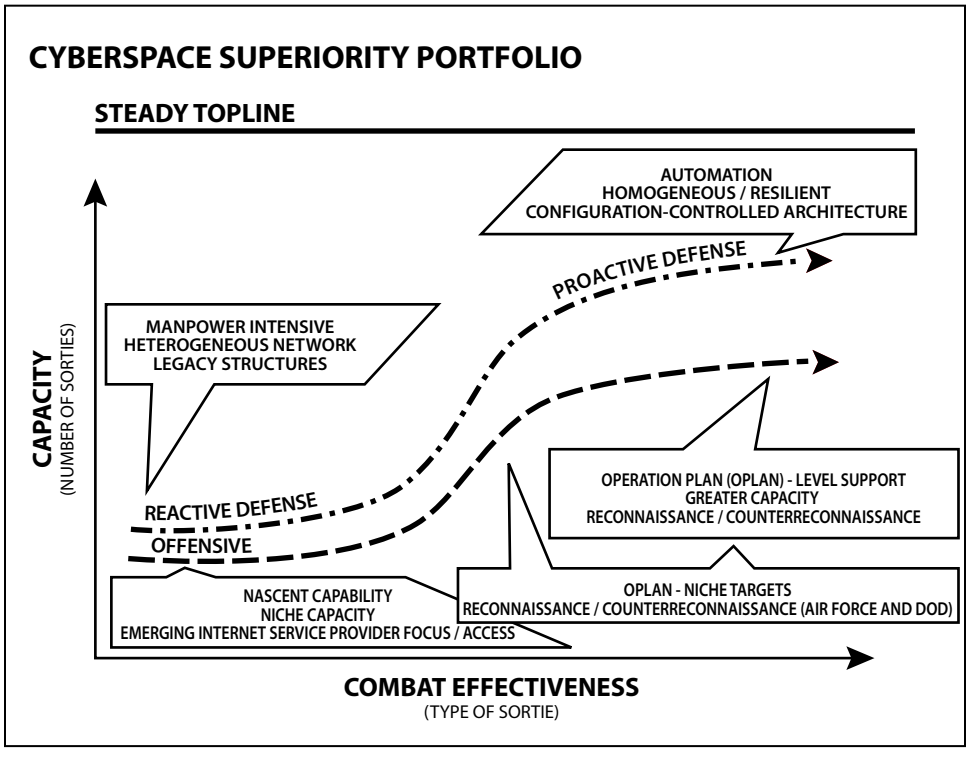


Figure. Cyberspace investment challenge. (Adapted from Maj Gen Suzanne M. Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly* 6, no. 3 [Fall 2012]: 74, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf.)

Even though the capability continuum depicts only offensive and defensive cyber forces, modern cyber warfare is conducted by leveraging three operational mission areas: Department of Defense Information Network (DODIN) operations, defensive cyber operations (DCO), and offensive cyber operations (OCO), each of which independently enables effects for the air, space, sea, and land domains.[20] All three are inextricably linked to generate effects across the spectrum of conflict, from small special operations missions to global conventional warfare.

The rapid rise in weapon systems and command and control (C2) systems that rely on network and wireless connections makes the integration and synchronization of complex operations difficult apart from the cyber domain—and underscores the importance to modern mili-

tary warfare of the DODIN. That network is "the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, sorting, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communication and computer systems and services, software (including applications), data, security services, other associate services, and national security systems."[21] DODIN operations construct, operate, and sustain the cyber domain, offering mission assurance and defense through prioritized network provisioning (dynamic construction), hardening, and configuration management.

Twenty-Fourth Air Force manages the AFNet—the Air Force's portion of the DODIN. With 850,000 total force users and billions of dollars in systems and infrastructure, Twenty-Fourth Air Force's units dynamically construct and operate a global enterprise and provision enterprise services to the Air Force and joint forces worldwide. Additionally, they defend the network through management of both base and AFNet boundaries, sensor placement and management, client configuration, and enterprise-compliance management. The services offered by these units assure that operational planners receive information for missions requiring complex communication topologies, high bandwidth, and high reliability.

Oftentimes people misconstrue DODIN operations as a support or information technology function. For example, Lt Gen Michael Basla, the Air Force's chief information officer, said, "I think we will draw a clearer line and distinction between what is required to build, operate and maintain [Air Force networks] and what is required to operate on the network."[22] Moreover, Gen Mark Welsh, the Air Force chief of staff, has observed that up to 90 percent of Air Force cyber personnel operate Air Force networks and that "they're not what NSA would call a cyber warrior."[23] Although these statements blur the distinction between network maintenance and defense, the DODIN fills an integral role in the conduct of military operations. The obvious benefits include con-

structing and operating the domain that enables all other domains. Additionally, DODIN operations provision access to information sources, harden friendly portions of the domain from unauthorized access, and configure network systems to provide ease of maneuver to friendly forces while constraining the adversary's options. These actions create a cyber high ground resulting in strategic, operational, and tactical advantages by making mission-critical information easier to defend and harder to attack.

To that point, the Air Force advanced the AFNet's defensive posture through two significant DODIN architecture initiatives. First, the deployment of Air Force gateways reduced the number of external network access points from 120 to 16. This architectural change enabled the service to canalize traffic, characterize the domain, and control data flows to significantly reduce the AFNet attack surface exposed to enemy strikes. The second initiative consolidated 850,000 users into a single integrated Air Force network, enabling enterprise-wide collaboration and improved, trusted secure communications. Defensively, this initiative delivers embedded security that substantially reduces an adversary's ability to act on the network by using compromised user credentials. Collectively, these defensive improvements inverted the cost/risk calculus of attack versus defense by forcing the adversary to work harder to find vulnerabilities while making it easier for the defender to guard critical assets.

The DCO mission area provides active defense against opponents. Twenty-Fourth Air Force's units prevent, detect, and respond to enemy actions through both active and passive defensive capabilities. These units conduct defense through a set of layered, overlapping technologies called "defense in depth," an architecture that ensures monitoring and defense of avenues of access as well as end points such as clients and servers. While DODIN operators limit attack vectors and reduce vulnerabilities by strategic placement of defensive capabilities on the network, DCO operators actively engage adversaries inside Air Force

networks to prevent intrusions, detect malicious capabilities and techniques, and respond to system compromises.

DCO operators monitor defenses for signs of attack and configure defenses to foil future attempts. The primary strategy for preventing intrusion calls for detecting known adversary tactics (signatures), limiting visibility into the AFNet, and continuously monitoring intelligence streams for indications of pending attacks. Operators analyze capabilities and methods used by the enemy and develop signatures that match patterns unique to a particular attack and thus provide complete protection from strikes matching the signature. Unfortunately, this method will not block attacks that have been modified from the original salvo. To maneuver around signature-based defenses, cyber attackers must "reengineer" their weapons so that unique signatures compromised in previous attacks are no longer detected. Depending upon the complexity of the developed signature, the adversary may be able to alter his weapons, forcing defenders to develop new signatures. This arms race between attack and defense has traditionally favored the attackers; however, as DODIN forces continue to reduce pathways that opponents can use, and as DCO operators persist in locating and eliminating vulnerabilities, the balance begins to shift in favor of the defense.

When new attacks occur that defenders could not prevent, sensors placed throughout the network supply intrusion indications and point DCO operators to the compromised systems, which they examine (by means of digital forensic analysis) to determine how the intrusion occurred and what tools were used. They then develop countermeasures to prevent future attack. DCO forces remotely access forensic data from all sensor devices to counter future compromises. Defenders use specialized tools to remotely capture the exact state of a computer (e.g., current data in memory, running programs, open network connections, etc.) to determine exactly what is happening at a given moment. This capability takes snapshots of malicious code as it executes, helping defenders understand the exact behavior of implanted soft-

ware. By analyzing this behavior, they can develop signatures and new tactics, techniques, and procedures (TTP) to prevent the same type of compromise in the future. The use of remote forensics capabilities reduces defenders' incident response from days to hours, slashing the amount of time that attackers have to maneuver through the network, perform reconnaissance, or exfiltrate sensitive data.

Additionally, Twenty-Fourth Air Force has both hunting and pursuit capabilities to offer real-time defense and response against adversary actions and regularly analyze enterprise resources for indications of advanced enemy presence or attempted access. Even though boundary defense is an effective means of recognizing and repelling most attacks, a sufficiently sophisticated and dedicated actor will eventually gain a toehold. Highly skilled DCO operators conduct active pursuit operations to rove the enterprise network and find, fix, track, and target such actors. These operators conduct real-time analysis of network devices, looking for anomalies that indicate enemy activity, eradicating the threat, and initiating an incident-response process to determine the root cause and/or TTPs used to gain access. Sometimes an even more comprehensive look is necessary to ensure that critical assets such as weapon systems and C2 nodes are appropriately hardened and cleared of advanced adversary presence. The Air Force uses hunt operations to characterize the cyber environment in these enclaves, complete a comprehensive analysis of mission data flows, standardize and harden the weapon system or critical asset interfaces, determine potential anomalous activity or attack vectors, herd adversary behavior, and eradicate persistent threats from the environment. These operations, which rely heavily on individual experience, knowledge, and training, are intensive and focused to ensure that these critical assets enjoy freedom of action in contested environments. Even as technology progresses, we will rely heavily on both pursuit and hunting capabilities to counter the advanced adversary threat in the future. Additionally, to increase the capacity and capability of this mission area, USCYBERCOM has developed a cyber protection team structure, each team including a mixture of capabilities designed to give combatant

commanders DCO effects. According to Gen Keith Alexander, the commander of USCYBERCOM, the command will stand up 13 teams by the end of 2015, significantly increasing the Air Force's DCO force, strengthening blue networks, and forcing the enemy to divert manpower and attention to counter this new capability.[24]

As with DCO and DODIN operations, OCOs have developed from a nascent to an operational capability well integrated into joint operations. The OCO mission set concentrates on gaining and—more importantly—maintaining access to enemy areas of cyberspace without detection. The nature of OCOs requires operators to carefully plan missions to characterize and exploit enemy networks. Further, the tools used to perform OCOs are sensitive because of the nature of the cyber domain (i.e., the ease of copying bits and bytes). Consequently, tool development and deployment are an important aspect of this mission area.

Although OCO operators provide a very real set of strategic alternatives to combatant commanders, the effects are specific and limited in scope. To exploit an adversary's system, offensive operations demand detailed knowledge of the target network, obtaining such information by performing network reconnaissance with sophisticated TTPs. Once operators have identified vulnerabilities, they must then develop either a technique or a weapon or select one from an existing repository prior to choosing the specific delivery mechanism. After they have accessed their target, operators establish a permanent presence on the machine while cloaking indications of the incursion, allowing them to maintain access indefinitely. Such persistent presence lets them effectively exploit information on the target in support of war fighters' objectives. In light of the long lead time necessary to perform target reconnaissance and establish persistent access, offensive operations typically require advanced planning and a lengthy time horizon to offer effective options.

The weapons used by operators are similar to the ordnance that a pilot employs to carry out a given mission. Certain weapons are bet-

ter for a desired purpose than others, and some work against a particular set of targets while others are ineffective against that objective. One major difference, however, is their fragility. Since defenders can block a weapon using a signature once they have detected it, use of a given technique or weapon to gain or maintain access carries a risk that the attacker will discover and counter it, rendering the technique or weapon useless for future operations. As a result, operational planners must assess the technical gain/loss associated with the employment of OCOs. If the desired effect is not substantial enough to justify the potential loss of an OCO weapon, then they should consider other methods.

Today's OCO force is a high-demand, low-density asset. As it did with DCOs, to increase the capacity and capability of this mission area, USCYBERCOM will develop a cyber mission force structure for OCOs, including teams composed of a mixture of capabilities designed to provide a broad spectrum of OCO effects to combatant commanders. General Alexander expects the command to stand up several of these teams by the end of 2015, significantly augmenting the Air Force's OCO force.[25] The increased capacity for OCO operations will put enemy strongholds at risk, forcing adversaries to divert manpower and attention to defenses and reducing the defensive burden on US networks.

The shortfalls of current cyber warfare operations are not readily captured by the dimensions of the capability continuum in the figure depicting the cyberspace investment challenge (see above). Fully illustrating where the cyber domain rests in this continuum requires extending into a third dimension—domain coverage. Contemporary cyber warfare is characterized by largely network-based capabilities in conjunction with traditional electronic warfare. During peacetime, the bulk of the effort focuses on shaping the cyber battlefield, defending critical assets, and collecting intelligence. Should the United States enter a full-scale cyber war today, offensive and defensive capability would be limited to subsets of the full cyberspace domain. These subsets are critical to the projection of power, but they do not fully en-

compass the overall domain. Such current capabilities, though effective, present limited cyber options to our combatant commanders.

Cyber Warfare in the Future

> *Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.*
>
> —Air Marshal Giulio Douhet

Although cyber warfare is currently limited to information networks and network-attached systems, it will drastically expand in the future. Rather than decide between kinetic and nonkinetic effects, planners will choose the effect that will best produce the desired outcome. Cyber-based effects will not be limited to networks of computers; rather, they will encompass all electronic information processing systems across land, air, sea, space, and cyberspace domains. This full-domain dominance will permit freedom of maneuver in all war-fighting domains by holding the enemy's electronic information-processing systems at risk while defending friendly systems from attack.

The future of cyber warfare is predicated on policy, technology, and threat. New technology can have disproportionate effects, not only on the weapons used in cyberspace but also on the makeup of the domain itself. National policy on cyberspace dictates the objectives and rules of engagement for cyber capabilities as well as the organization and execution of operations. The rapidly evolving threat posed by peer actors in the cyber domain will dictate how cyber forces are trained and deployed in the future battlefield. Despite these wildcard influences, the future of cyber warfare can be broadly extrapolated from current experience and application of fundamental tenets of warfare. To remain grounded in today's realities, we limit the vision of cyber warfare discussed here to a decade into the future, allowing us to assume that technological changes will follow the course laid out in *Cyber Vision 2025*.[26]

Future cyber warfare will not be relegated solely to network-based resources. According to Major General Vautrinot, "Cyberspace is not simply the Internet; rather, it is a network of interdependent information technologies including the Internet, telecommunications networks, computer systems, and embedded processors."[27] Although much of the present effort focuses on Internet-connected networks, this is only a subset of the total cyber domain, which also includes non-Internet-connected networks such as tactical data links, satellite-control networks, launch-control networks, and other networks not traditionally based on Internet data-transfer protocols and technologies. Future warfare will see DODIN operations as well as DCO and OCO forces expanding their mission areas to these nontraditional networks and the systems that connect through them, such as satellites, avionics, targeting pods, digital radios, and remotely piloted aircraft. Effects produced on and through these systems will include disruption, distraction, distortion, distrust, confusion, and chaos of both a virtual and physical nature, with consequences that can be assessed and measured on the battlefield.

In this future war, many of the services currently supplied by DODIN operations will be decoupled from the hardening, defense, and mission-assurance roles. Services such as e-mail, data storage, web, and transport will be provided as commodity services/utilities, much like electricity or water. Through the joint information environment, the DOD will leverage economies of scale and cloud technologies to improve the resiliency of services and expand their reach so the war fighter can safely assume availability and reliability. This roll-up of commodity services will free DODIN operators to concentrate on defensive hardening and attack recovery while expanding their scope to nontraditional networks. As with AFNet, consolidation and standardization of tactical and C2 networks will result in a reduced attack surface, higher reliability, and more responsive disaster recovery. Rather than rely on weapon system designers to take responsibility for the security of their systems, DOD professionals will manage and enforce formalized security standards and interoperable interfaces. The stan-

dards will ensure that weapon systems have a "baked-in security" capability while the interoperable interfaces will reduce the "one-off" systems and capabilities that drive increased enterprise vulnerabilities and cost. Sensors, reporting mechanisms, and configuration-management tools will be designed into the system from the beginning, allowing DODIN operators to enforce a rigorous and standard security posture across all combat systems.

Future DCO capabilities will tackle one of the greatest costs associated with defense: the man-in-the-loop sensor, which offers alerts that require human intuition and experience to interpret and identify the occurrence of a compromise. This reliance on human intuition forces defenders to maintain large, well-trained manpower pools to defend relatively small areas of cyber terrain. The human limitation prevents analysis of these alerts at the speed of data passing through the network, forcing defenders to react to threats rather than proactively defeat them. As technology advances, the infusion of human intuition into automated sensors will allow for man-on-the-loop defense, which will reduce manpower requirements but increase overall effectiveness.

Building upon a standardized security framework, future DCO capabilities and sensors—deployed across all combat platforms—will be designed to supply man-on-the-loop rather than man-in-the-loop detection. These sensors will leverage machine-learning techniques and predictive-behavior modeling to recognize and separate attacks from normal operational data flows. Rather than rely on a human to view and interpret results, defenders will mitigate attacks on the fly and ignore false positives, with human intervention driven by triggers and confidence thresholds.[28] Using ubiquitous network sensors, they will also perform data correlation and analysis across platforms and networks to discover trends of attacks, using them to further characterize current and emerging adversary tactics and give some perspective on both persistent and fleeting targets of enemy interest.

Armed with information on targets under attack in cyberspace, defenders will perform critical asset protection. Expansion outside tradi-

tional networks will require that defenders focus on prioritized assets, a process enabled by situational awareness tools that tie missions to systems and physical locations to network locations. Defenders need not protect every workstation equally; instead, they can focus their efforts on systems supporting a high-priority operation or on data links critical to attaining a war fighter's objective. This prioritization of effort will allow them to utilize both mass and maneuver to best counter enemy actions in a timely and effective manner.

Improved sensors and prioritized defenses will allow defenders to push enemy actors outside blue cyberspace. Today's defense in depth catches many attacks inside the boundaries of our networks. In the future, improved sensor capabilities, combined with automated responses, will frustrate most attacks at the boundary of blue space, letting defenders focus on identifying threats before they reach friendly cyber systems and reporting the threats to offensive forces early enough for OCO operators to conduct operations, if necessary. By increasing the engagement distance, defenders will ensure system and data integrity and force attackers to battle through offensive interception before they can attempt to attack friendly systems.

Building on the capabilities of DCOs, future OCO capabilities will split into two types of missions: interception and attack. The former will engage enemy actors as they prepare to strike friendly forces whereas attack missions will hold enemy assets at risk in their own areas of cyberspace. Each mission will engage enemies on both traditional and nontraditional networks in the cyber domain.

Interceptor missions act in conjunction with DCO sensor targeting to attack enemies before they reach friendly systems. These missions will harass the enemy by capturing tools before he can launch them, changing attack targets so that his tools attack the wrong system or commit fratricide, and manipulating the data presented to the enemy operator, forcing him to react to forged threats. Rapid forensic capabilities let defenders reverse-engineer tools captured by interceptors and apply defenses against those tools in real time, foiling any further at-

tempts. These interceptor missions will represent a close air support function in cyber that keeps friendly cyberspace safe by attacking the threat before it arrives.

Attack missions, on the other hand, represent the strategic strike capability of OCOs and will create both virtual and physical effects across all domains through application of offensive capabilities in the cyber domain. Virtual effects will include manipulating data on enemy C2, intelligence, surveillance, and reconnaissance systems; injecting false data into C2 networks and tactical data links; removing data from those links; and isolating systems from their associated networks. Physical effects might include destruction through manipulation of digital control systems or remote system control of platforms such as satellites, remotely piloted aircraft, and fly-by-wire systems. In addition to these effects, attack will provide intelligence collection, data exfiltration, and other more traditional capabilities, but these will be employed across the cyber domain to include satellite systems, aircraft, and C2 systems.

In support of the full-domain competencies discussed above, cyber operators will have comprehensive situational awareness of the cyber domain. Although traditional sensors permit monitoring of the avenues of ingress and egress and small subsets of endpoint behavior, it will be necessary to develop new sensors that alert defenders to behavioral anomalies or statistically significant departures from the expected baseline. Sensors will supply these alerts in an actionable form so that operators can quickly determine whether or not a large-scale attack is occurring or a single node is compromised. Additionally, it will be possible to visualize the cyber domain in terms of logical connections, such as network and radio frequency circuits supporting a given mission, or data flows supporting a desired mission area to provide mission assurance.

Current cyber sensors utilize priorities associated with specific alerts to warn operators of possible malicious action. To determine whether or not those alerts represent a true threat or merely a false positive,

DCO operators must review detailed information such as the actual data passing between computers, the machines involved in the suspect transaction, and the basis of the original alert. This time-intensive process requires highly skilled operators and is prone to human error. Additionally, the alerts signify singular events that occur in a stream of data and may occur ambiguously under normal operating conditions as well as during an attack.

Future situational awareness tools, though, will capitalize on advanced threat indicators such as divergence from expected behaviors. These sensors will use a known baseline of user activity on a given node to determine whether or not a node is deviating from its expected behavior. Using a defense-in-depth methodology, sensors will automatically correlate similar behavioral alerts across multiple clients. With this type of automation, DCO operators can validate alerts at a higher level, in less time, and with reduced manpower. Moreover, behavioral alerting will decrease the number of false positives produced by sensors, allowing operators to spend more time responding to real incidents rather than analyzing nonevents.

Operators will receive alerts in an actionable form. For example, if a sensor alerts them to possible data exfiltration, it will automatically store the data stream in a temporary buffer pending operator action. If the operator confirms the alert, then the act of confirmation will delete the data in question before it is delivered; if the operator determines that the alert is a false positive, then the transmission will be resumed with no data loss. Similarly, attempts to compromise an aircraft or a satellite data link will result in an operator alert indicating the source of the attempt, methods used, and possible attribution based on known TTPs. This level of situational awareness enables the operator to alert the component commander in a timely manner so that he or she can take appropriate kinetic or nonkinetic action in response to the attack.

Finally, situational awareness tools will offer both physical and logical mapping of data and nodes. Since the cyber domain contains both

data and the nodes that process it, many parts of the domain possess both a physical and a logical location. For example, systems used to perform space launch may reside at an Air Force base thousands of miles from the actual launch location. A cyber situational awareness tool must be able to depict the systems both as a physical device associated with a given location and as a logical portion of the space launch network. It is also necessary to visualize data flow so that operators can see where spikes in data flow occur, where data is diverted for unknown reasons, and where it has stopped flowing. The increased visualization of data traversing cyberspace will permit operators to better understand and react to changes in both the physical and virtual battlespace.

To conduct cyber operations across the entire domain, we will develop Airmen with the foundational knowledge to comprehend traditional Internet-protocol-based networks as well as radio-frequency and proprietary-communications networks. Further, these warriors must understand not only how devices that operate in the cyber domain are designed but also how they operate. Just as a pilot must have knowledge of aerodynamic fundamentals to understand the performance and limitations of his weapon system, so must cyber warriors possess a foundational grasp of the cyber domain to employ cyber weapon systems properly.

As in the air and space domains, successful deployment of weapon systems in a combat environment demands that cyber crews develop competency in these weapons over the course of a career. Doing so requires a career-field-management strategy that emphasizes the development of experience and expertise tied to weapon system employment. Much like pilots, cyber warriors will be assigned to a mission track (e.g., DODIN operations, DCOs, or OCOs) and a weapon system. During initial qualification training, operators will become proficient in the configuration, components, design, and operation of their system. Over the course of one or more operation tours, they will continue to build expertise and competence in the deployment of that

weapon system. Like members of the flying community, those operators will have opportunities to transition to different systems as well as serve on staff or career-broadening tours. Each career path will remain generally distinct in technical development yet emphasize leadership, supervision, and cooperative action that translates to broader Air Force and joint operational expertise over time. The necessary skills and experience will be normalized with the joint community to ensure that forces presented to combatant commanders provide reliable capabilities consistent with those of the other services.

The Air Force will train cyber operators in a rigorous, deliberate fashion to ensure that they possess the foundational skills to perform their specific mission. This training will encompass networking and computing fundamentals as well as knowledge of data transmission across the electromagnetic spectrum, operating systems, computer design fundamentals, and electronic circuit theory. Training specific to mission areas will encompass not only particular toolsets but also defensive and offensive techniques. Both DCO and OCO personnel will routinely rotate into DODIN positions to guarantee current knowledge of system configuration, defensive posture, and terrain familiarization.

Conclusion

Just as the air and space domains took time to grow from their inceptions to fully capable war-fighting domains, so is the cyber domain poised to follow the same arc. That domain has developed at a rapid pace from a novelty and mission-enhanced commodity to a mission-critical capability in just a few decades. As it continues to progress, the level of capability offered by dedicated operators to the war fighter will also increase exponentially.

We can compare today's cyber power to airpower sometime during the interwar years. Operators have developed capabilities and demonstrated their effectiveness to combatant commanders; however, warfare in and through cyberspace remains underdeveloped. Even though

professionals in the cyber field have become more proficient at creating effects in the domain via DODIN as well as DCO and OCO operations, these effects are still not well integrated into a combat environment. As was the case with airpower before the beginning of World War II, operational planners are not sufficiently versed in this domain to intuitively envision cyber's contribution to decisive battlefield effects in modern form. Partly because of occasional doubt regarding the proficiency of cyber capabilities, their effects are currently considered "nonkinetic" while more traditional military capabilities produce "kinetic" effects. In the future, cyber warfare will prove its effectiveness on par with more traditional capabilities, blurring the line between kinetic/nonkinetic effects. By then, cyber capabilities will have become well-deliberated strategic alternatives for our national leaders and combatant commanders—recall World War II's Battle of the Beam, mentioned above, when cyber capabilities were the first and best option to defend Great Britain against German bombing raids.

The explosive growth in cyber today and the bold vision articulated by senior leaders throughout the DOD promise a bright future for this domain. As cyber warriors continue to develop competence and effectiveness in their weapon systems, the capabilities they bring to the joint fight will begin to show their true potential. As we plan and employ such capabilities with greater frequency and effectiveness, commanders will fully understand how best to utilize these forces to fulfill mission objectives. Advances in technology, organization, and operator expertise will continue to translate into unprecedented battlefield effects. ✪

Notes

1. Alfred Price, *Instruments of Darkness: The History of Electronic Warfare* (London: Panther, 1979), 55–58.
2. Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 15 July 2010, 2–3, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf.

3. Department of Homeland Security, *The National Strategy to Secure Cyberspace* (Washington, DC: Department of Homeland Security, February 2003), http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberspace_strategy[1].pdf; and Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (U) (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

4. Joseph A. Ruffini, "609 IWS Chronological History," 609 Air Operations Squadron, June 1999, 8; and "Air Force Information Warfare Center," in *Air Intelligence Agency Almanac*, Federation of American Scientists, accessed 21 June 2013, http://www.fas.org/irp/agency/aia/cyberspokesman/97aug/afiwc.htm.

5. Armed Forces Communications and Electronics Association, *The Evolution of U.S. Cyberpower* (Fairfax, VA: Armed Forces Communications and Electronics Association, n.d.), 11–17, http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf.

6. Senate, *Committee on Governmental Affairs, Permanent Subcommittee on Investigations (Minority Staff Statement), Hearing on "Security in Cyberspace,"* 104th Cong., 2nd sess., 5 June 1996, app. B.

7. Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989), 180–86; and Ruffini, "609 IWS Chronological History," 3.

8. Ruffini, "609 IWS Chronological History," 4.

9. Ibid., 4–30.

10. "Cyberwar!," *Frontline* (Public Broadcasting Service), 24 April 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/; and "Solar Sunrise," GlobalSecurity.org, accessed 21 June 2013, http://www.globalsecurity.org/military/ops/solar-sunrise.htm.

11. "Cyberwar!"

12. "Solar Sunrise."

13. Jason Healy, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 12–13, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf; and History, Defense Information Systems Agency, Department of Defense, 2000s, accessed 5 August 2013, http://www.disa.mil/About/Our-History/2000s.

14. History, Defense Information Systems Agency.

15. Jason Healy and Karl Grindal, "Lessons from the First Cyber Commanders," *New Atlanticist*, Atlantic Council, March 2012, http://www.acus.org/trackback/65665.

16. Mark T. Maybury, PhD, *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision, 2012–2025*, AF/ST TR 12-01 (Washington, DC: Office of the Chief Scientist, United States Air Force, 2012), http://www.af.mil/shared/media/document/AFD-130327-306.pdf.

17. Gen Michael V. Hayden, "The Future of Things 'Cyber,' " *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3–7, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf.

18. Gen William L. Shelton, commander, Air Force Space Command (remarks, Armed Forces Communications and Electronics Association Cyberspace Symposium, Colorado Springs, CO, 6 February 2013), http://www.afspc.af.mil/library/speeches/speech.asp?id=728.

19. Maj Gen Suzanne M. Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 71–87, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf.

20. Cheryl Pellerin, "Cyber Command Adapts to Understand Cyber Battlespace," Department of Defense, 7 March 2013, http://www.defense.gov/news/newsarticle.aspx?id=119470.

21. Joint Publication 3-12, *Cyberspace Operations*, 5 February 2012, 18.

22. John Reed, "What Does Cyber Even Mean?," *Killer Apps* (blog), 5 December 2012, http://killerapps.foreignpolicy.com/posts/2012/12/05/what_does_cyber_even_mean.

23. Ibid.

24. Ellen Nakashima, "Pentagon Creating Teams to Launch Cyberattacks As Threat Grows," *Washington Post*, 12 March 2013, http://articles.washingtonpost.com/2013-03-12/world/37645469_1_new-teams-national-security-threat-attacks.

25. Aliya Sternstein, "Military Cyber Strike Teams Will Soon Guard Private Networks," Nextgov, 21 March 2013, http://www.nextgov.com/cybersecurity/cybersecurity-report/2013/03/military-cyber-strike-teams-will-soon-guard-private-networks/62010/.

26. Maybury, *Cyber Vision 2025*.

27. Vautrinot, "Sharing the Cyber Journey," 75.

28. Recent advances in support vector machines specifically and machine learning / classification tasks in general support this assertion. See "Unsupervised Learning and Clustering," in Richard O. Duda, Peter E. Hart, and David G. Stork, *Pattern Classification and Scene Analysis: Part I, Pattern Classification*, 2nd ed. (New York: John Wiley & Sons, 1995).

Col William J. Poirier, USAF

Colonel Poirier (BS, University of Massachusetts–Amherst; MS, Strayer University; MS, National War College) commands the Air Force's newest combat wing, the 67th Network Warfare Wing, Joint Base San Antonio–Lackland AFB, Texas. His wing presents trained and ready cyber forces through Air Forces Cyber to US Cyber Command and other joint task force and combatant commanders to execute global network operations, defense, and full-spectrum network warfare capabilities. The 67th Network Warfare Wing also performs electronic systems security assessments to improve operational security for the Air Force and joint partners. During his career, he has commanded a squadron and has completed assignments at the Air Staff, two unified combatant commands, a binational command, and a defense agency. He has also led two divisions on the staff of a combined force air component commander; served as the chief command, control, communications, computers, and intelligence (C4I) engineer in Operations Southern Watch, Enduring Freedom, and Iraqi Freedom; enabled launch and maintenance operations for strategic and tactical nuclear weapon systems; and was a member of the start-up team for United States Northern Command. Colonel Poirier is a graduate of the Army Command and General Staff College and National War College.

Maj James Lotspeich, PhD, USAF

Major Lotspeich (USAFA; MS, Air Force Institute of Technology; PhD, Naval Postgraduate School) serves as director of operations for the 33d Network Warfare Squadron. He trains and readies cyber forces for presentation through Air Forces Cyber to US Cyber Command and other joint task force and combatant commanders to execute defense of the Air Force portion of the Department of Defense's global enterprise network. He is responsible for directing all Air Force network defense operations in support of the Air Force Network Operations commander and US Cyber Command. Major Lotspeich has held a variety of leadership positions at the base and major command levels, both in-garrison and deployed, serving as leader of postal operations for Air Combat Command and as mission systems flight commander during Operation Iraqi Freedom. Additionally, Major Lotspeich served as assistant professor of computer science at the US Air Force Academy where he directed the core computer science course for 1,400 cadets each year.

Let us know what you think! Leave a comment!

Space Superiority, Down to the Nanosecond

Why the Global Positioning System Remains Essential to Modern Warfare

Col Bernard J. Gruber, USAF
Col Jon M. Anderson, USAF, Retired

To maintain our superiority in space, the Air Force continues to modernize the GPS program.

—Secretary of Defense Chuck Hagel

Reel back to the year 2008 when Michael Phelps swam into the history books with an astonishing finish to win his seventh gold medal by one one-hundredth of a second against Milorad Cavic. By any stretch of the imagination, the time differential in this historic race was imperceptible, but for the Global Positioning System

(GPS) an error of one one-hundredth of a second would be a disaster.[1] Why? For the GPS, one nanosecond (0.000000001 second) would result in the equivalent of approximately a one-foot error on Earth. Translated, Phelps's razor-thin margin of victory would have produced an incredible error of almost 10,000,000 feet or approximately 1,894 miles. Although the GPS provides so much more than just timing accuracy, this measurand has become one of its key hallmarks, as have its space superiority and force-multiplying capabilities. Joint Publication 3-14, *Space Operations*, defines "space superiority," a primary focus of this article, as "the degree of dominance in space of one force over any others that permits the conduct of operations at a given time and place *without prohibitive interference from space-based threats*" (emphasis added).[2] Although not yet fully operational at the time, the GPS was first used for combat in Operation Desert Storm, often called "the first space war."[3] From initial air strikes by Pave Low helicopters to Gen Norman Schwarzkopf's famous "left hook," the GPS served as a key force enabler, even with a very limited deployment of receivers.[4] Furthermore, the GPS has been a crown jewel of the American military's superior space capabilities for decades, through Operation Enduring Freedom. Yet, emerging threats and increasingly sophisticated foreign capabilities present new challenges to maintaining US technical and operational advantages.

Provided free of charge by the US Air Force and acquired and operated by Air Force Space Command, the GPS is a critical national asset. A tangible symbol of US economic and military might and a system unmatched in performance, cost, and availability, the GPS is now utilized by well over 1 billion people and has been integrated into more than 2 billion devices, both commercial and military.[5] Its applications are wide ranging and diverse, from aircraft navigation to network synchronization (see the table below).

Application	*GPS Enabler*	*Effect*	*Military Counterpart*
Agriculture	Precision Farming	Demonstrated increases in annual crop yields of 10%	Minelaying, unmanned ground vehicle positioning
		Reduction in fuel costs of 52%	
		Reduction in labor costs of 67%	
Aviation	Next Generation Air Traffic Management System	Single large aircraft descent: 1,600 lb. of fuel with a corresponding reduction of two metric tons of carbon dioxide	Military aircraft navigation
Maritime	Automatic Identification System	Vessel traffic control around busy seaways	Minesweeping, maritime navigation
Surveying	Control survey points	Cost reduced from $10,000 to $250/point	Target location
Precise Time	Worldwide distribution	Cellular networks, satellite communications, ATM machines as well as many other "consumer" services, and the underlying banking, data handling, and public utilities	Tactical network synchronization
		Time order of battle	
Environmental	Optimization of fleet-management systems	Reduction of fuel consumption by 5.4 billion gallons	Aircraft fuel reduction
		Reduction of CO_2 emissions by 54 million metric tons/year	
Disaster Relief	Rescue teams	Instant beacon location	Combat search and rescue
	Emergency response	Optimized routing	
Humanitarian	Airdrops (e.g., Joint Precision Airdrop System)	260 acres of space required (1999) to five acres (2012)	
Military	Precision-munition guidance	Joint Direct Attack Munition, joint standoff weapon, small-diameter bomb, Tomahawk cruise missile, Excalibur projectile	
	Combat search and rescue	Combat Survivor Evader Locator radios, Motorola XPR6550—multiple examples	

Table. Applications of the Global Positioning System. (Data extracted from the nomination of the Global Positioning System for the International Astronautical Federation's 60th Anniversary Award, 2011.)

Although the law guarantees availability of the GPS to users worldwide, the system also serves as a critical fiber in our nation's defense, clearly enabling space superiority as defined by Department of Defense (DOD) policy. This article highlights how the GPS has become an integral part of our nation's war-fighting and commercial capabilities, why it will remain essential to both national economic power and US military superiority, and how it will get better in the future. The article offers unique analogies, examples, and the firsthand experiences of two senior leaders of the GPS Directorate who have worked GPS strategy, policy, technology, and acquisition for more than 20 years combined.

The Importance of the Global Positioning System

Positioning, navigation, and timing (PNT), a term rarely heard outside the US government, usefully consolidates under a single banner the various systems, policies, and activities concerned with providing critical positioning information, navigation capabilities, and time dissemination. By most measures, PNT is a thriving, healthy, global enterprise, largely due to the ubiquity of the GPS, which the United States has offered as a free global utility since the inception of the GPS program office in 1973.

Today, more than 3.3 million jobs rely on GPS technology, including approximately 130,000 in GPS manufacturing industries and 3.2 million in the downstream commercial, GPS-intensive industries. In light of high financial returns, we expect the commercial GPS adoption rate to continue to grow across industries. Consequently, the system's technology will create $122.4 billion in benefits per year and will directly affect more than 5.8 million jobs in downstream commercial, GPS-intensive industries when penetration of the system's technology reaches 100 percent in those industries.[6]

The GPS has proven brilliantly successful and so universally adopted that Russia, the European Union, and China have all developed imita-

tions and are in various stages of deploying them. Additionally, more than 50 nations have developed GPS augmentations. In many ways, the GPS was the first truly global utility—one that is only now realizing its potential as new commercial applications emerge every year. The system has also become a symbol of military interoperability, boasting agreements with 55 US allies as authorized users of the military's precise positioning service.

The GPS largely owes its success to the fact that no other system or technology can match its performance, cost, and availability. Traditional radio navigation aids are far less accurate and do not provide global coverage. Inertial systems are capable of very precise short-term accuracy, but physics dictates that their accuracy will diminish over time unless synchronized periodically with the GPS or a similar system. Atomic clocks keep accurate time but are costly, requiring significant power and thermal control. Promising new technologies such as Chip-Scale Atomic Clocks, Cold Atom Inertial Systems, and Wi-Fi Navigation all reduce dependencies on the GPS alone; however, they probably will not deliver similar accuracy and pervasive availability for the foreseeable future. Instead, these technologies work best when integrated with other sensors—especially the GPS. As such, the US military continues to rely on the GPS, even as new technologies are integrated into weapon systems.[7]

Background

Like cell phones, computers, and the Internet, the GPS is used worldwide by ordinary citizens and the military forces of both allies and adversaries. Since the launch of its first satellite more than 30 years ago, the system has transformed navigation and precise timing. From the first GPS satellite launch on 22 February 1978, any user—military or civilian—could access the unencrypted coarse/acquisition (C/A) code on the primary GPS frequency L1 (1575.42 megahertz [MHz]).

From the system's inception, military leaders have been concerned about universal access to the precise PNT offered by the GPS to friend and foe alike; thus, its "dual-use" phenomenology has at times caused friction between the military and civil user communities. As the commercial use of and reliance on the GPS increased, the effects of the "selective availability" methodology—the original means of limiting universal capability—proved too hard to bear for the US government. The concept behind selective availability involved the employment of positioning and timing accuracy as a discriminator between military and civil users. The signal was intentionally degraded to 100-meter accuracy, a condition that authorized users with a valid decryption key could remove. This practice not only was enormously unpopular with the civil GPS community but also was eventually circumvented by differential techniques. In fact, the Department of Transportation funded and developed differential GPS, leading to the untenable situation in which one arm of the federal government undermined another.

The downing of Korean Airlines Flight 007 by an aircraft of the former Soviet Union over the Sea of Japan on 1 September 1983 emphasized the critical need for a global civil-navigation system. A series of US policy initiatives promoting adoption of the GPS by civilian and commercial users followed, including Presidential Decision Directive no. 6 in March 1996, and culminated with the elimination of selective availability in May 2000.[8] Its removal offered civilian GPS users the reliable accuracy previously delivered only to the US military and spawned explosive growth in the development of high-precision civilian applications in such fields as surveying, agriculture, and earth science. On 27 September 2007, the White House announced that selective availability would no longer be included in future procurements of GPS satellites. Today, there is little difference in the accuracy available to US forces, civil users, or adversaries.

The Air Force took the additional step of committing to specific levels of civilian performance and backed up that commitment with US law. The GPS Standard Positioning System Performance Standard (SPS PS),

first published in 1993, established minimum levels of GPS service in terms of constellation coverage, signal accuracy, and integrity for C/A code users. These GPS performance commitments—particularly important for safety-of-life applications—have allowed certification of the system for commercial aviation by both the Federal Aviation Administration and the International Civil Aviation Organization. The SPS PS has been updated multiple times over the years, most recently in 2008, and will continue to undergo updates to account for the deployment of new civil signals. The US government's commitment to GPS standards for civilian users has allowed receiver manufacturers and other commercial developers to commit resources to developing products and services based upon accurate, reliable, and globally available GPS signals. As new, developing service providers of the global navigation satellite system—such as the European Galileo system and Chinese BeiDou (Compass) system—begin operations, users will also demand similar commitments, particularly for safety-of-life applications.

During more than 30 years of operation, the GPS has made continuous improvements to its operational control segment, which monitors the health and status of the constellation. This segment produces data on GPS satellite orbits and the atomic clocks on board each GPS spacecraft that all receivers use to compute their position and timing solutions. In the last decade alone, these improvements have led to 50 percent reductions in the signal-in-space user-range error. In fact on 21 April 2013, the GPS system recorded a user-range error of 51.4 centimeters, setting an all-time-record low.[9] Considering that the minimum standard guaranteed by the US government is six meters, this accomplishment is quite spectacular.[10] Moreover, the GPS tripled the number of monitor stations with the addition of 10 from the National Geospatial-Intelligence Agency, starting in 2005. These extra stations supply more data, which improves the control segment's estimates of the satellite orbits and atomic-clock time offsets, leading to improved accuracy for the user. In fact, the GPS time scale now typically differs from the time standard maintained by the US Naval Observatory in Washington, DC, by fewer than five nanoseconds.

These improvements ensure that the GPS system's importance to space superiority will continue. Further, the approximately $32 billion already invested in the system and the ongoing improvements envisioned within it assure war fighters that they can rely on the attributes of the GPS. However, the removal of selective availability, coupled with the continuous and significant accuracy improvements to the globally available civil GPS service, magnifies the challenges presented by the system's dual-use nature, offering potential adversaries precise PNT at low cost.

The Global Positioning System in the Navigation Warfare Era

In 1996, Presidential Decision Directive NSTC [National Science and Technology Council]-6, *US Global Positioning System Policy*, instructed the DOD to protect the US military's use of the GPS in the presence of jamming, develop the means to prevent its employment by adversaries, and ensure that civil users outside the area of military operations would remain unaffected.[11] Although elements of this initiative, commonly known as navigation warfare, already existed, the three tenets (protection, prevention, and preservation) embodied the notion that the GPS was outgrowing the earlier security features embedded in its design and that a different approach was needed—one that did not include selective availability. The navigation warfare tenets were further codified by direction from Congress in Title 10, *United States Code*, and in the White House's policy on space-based PNT in 2004. Given the ubiquitous nature of the GPS and the growing prevalence of both sophisticated and brute-force jamming threats, military leaders and US policy concerns identified a need for strategic alternatives.

The 2006 *Joint Capabilities Document for Position, Navigation, and Timing*, developed by US Strategic Command, states that "no other capability permeates the fiber of joint operations like PNT."[12] Although the GPS is not the sole source of PNT for the US military, it is the primary one for most users. Compared to the next-best alternatives, GPS is simple, inexpensive, reliable, and highly accurate. It has changed

not only how US forces navigate but also how they fight. Like their civilian counterparts, the Soldiers, Sailors, Marines, and Airmen of the US armed forces take the availability of the GPS for granted; experience has taught them that it works nearly everywhere and nearly all of the time.

Although eminently functional in most environments, the GPS has limitations. Its signals are very weak, well below the ambient noise level in GPS receivers, and easily blocked by obstructions such as buildings and terrain; further, unlike some signals, they do not penetrate under water, under ground, or through thick foliage. Additionally, GPS signals are vulnerable to radio frequency interference, both intentional and unintentional. The accuracy of the time or position obtained by the GPS user is directly related to the geometric relationships between the user and the visible satellites, resulting in degraded performance whenever a portion of the sky is obscured. Consequently, the *Joint Capabilities Document* identified several primary PNT gaps, including access to PNT in the presence of "geospatial impediments," which include environments such as indoors, underwater and underground locations, and both natural and urban canyons.

Unlike individuals who employ inertial navigation systems and local timing sources, PNT users dependent on GPS must rely on external radio signals. As is the case with radar and radio communications, adversaries can jam these signals in a variety of ways—a situation that led the original GPS developers to incorporate secure encryption and antijamming features into the design. The secure military signal, known as P(Y) code, is used by the US military, some federal agencies, and the military services of several allied nations. In addition to providing an element of assurance to the military user, this code signal is more resistant to jamming than the civil (C/A code) signal, and military users have access to two frequencies rather than the single frequency available to civil users today. Encryption also creates a form of military exclusivity, which gives authorized users a uniquely available signal, although many high-precision commercial receivers utilize techniques

that exploit general characteristics of the military signal while ignoring the encryption. Growth in applications based on these techniques has led to a commitment by the US government to maintain the signal characteristics until a second coded civil signal becomes fully operational and available from the GPS constellation.

Antijamming for GPS users exists in several forms, from natural body masking on aircraft and terrain masking for ground users to technical innovations such as adaptive antenna arrays, narrowband frequency filters, and "tight" integration with inertial sensors. Unlike commercial receivers, military GPS receivers are designed to operate under jamming conditions and are generally more robust. They also typically utilize older technology than modern, commercial GPS receivers primarily because of the much faster commercial-product lifecycle time, additional unique requirements levied upon military electronic equipment, and the acquisition process to procure military receivers. High-end systems used on military aircraft, ships, and some missiles and munitions are typically part of an integrated navigation system. Oftentimes they operate outside the range of the most likely threat—ground-based jamming. In recent years, attention has mainly focused on low-end users, especially military handheld GPS receivers—also widely used in vehicles. For these users, size, weight, and cost are critical factors, so aircraft antijamming techniques offer limited benefits. Toward that end, Air Force Space Command has made GPS modernization and the protection of military signals a priority.

Modernization of the Global Positioning System

The only practical method of denying the use of GPS to an enemy while limiting the effects to a geographical region involves the employment of local electronic warfare. Unfortunately, GPS civil and military signals share the same frequency range. Although the military originally enjoyed access to a second frequency unencumbered by a civil signal, pressure from civil agencies led to this frequency becoming dual use as well. After searching for a tractable solution that would en-

able military use of the GPS in the presence of "friendly" jamming of the civil GPS signal, the Air Force developed a new military signal—military code (M code)—which shares the current GPS frequency bands yet is sufficiently separated from the civil signal to provide secure GPS to military users in the presence of friendly jamming operations against the civil signal. To meet the direction from the White House and Congress to prevent adversaries from using the GPS, modernized receivers must be robust in the presence of friendly jamming. Spectral separation of the M code signal from civil GPS signals (see the figure below), combined with modern signal processing, will enable war fighters to navigate securely while aggressively jamming enemy use of satellite-based navigation systems. Thus we can ensure space superiority well into the future.

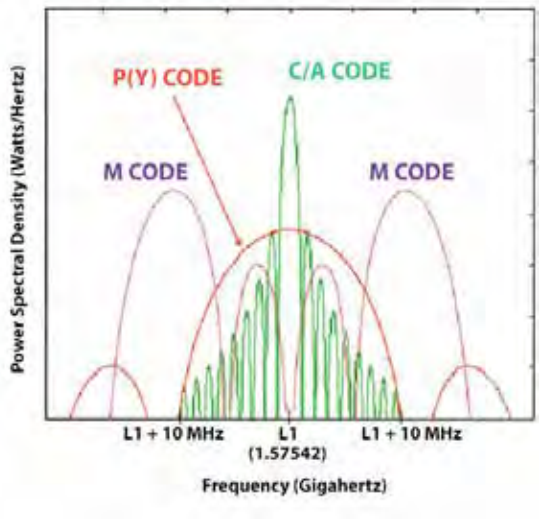


Figure. GPS spectrum on L1 (primary GPS frequency)

The first satellite with M code launched in 2005, and the 12th one in 2013. By 2017, 24 modernized M-code-capable GPS satellites will supply global coverage and capability to US military and allied users. M code offers several advantages in addition to "spectral separation" (i.e., the frequency allocation of M code does not directly overlay the civil-

ian signals). Its inherent design improves the accuracy and jamming resistance of the military signal, and it includes several enhanced security features. Increased transmitter power aboard the satellite—one of the key attributes of jamming resistance—bolsters the jamming power necessary to defeat friendly receivers, making higher-power jammers easier to detect, locate, and target. The GPS III satellite program, currently approved for eight modernized satellites, will provide M code signal power up to eight times stronger than legacy military signals supplied by GPS II satellites.[13] Although this extra power will not in itself defeat known threats, more power complements every other antijamming technique. More power adds more "bars" to the signal meter, providing a signal under tree canopies and possibly in buildings; moreover, it overcomes many annoying, interfering sources that occur regularly in the field. Additional power will come from advanced beam-shaping antennas on future GPS satellites, further improving performance in both impeded and highly jammed conditions.

The GPS has matured in a manner analogous to radar's development. From the early days of World War II to the present day, an unrelenting pursuit of technologies has yielded tremendous improvements in radar performance. Radar evolved from early continuous-wave radars to monopulse radars, followed by pulse-Doppler radars, phased-array radars, and, finally, today's state-of-the-art synthetic aperture radars. Further, the US military, civilians, and users worldwide rely upon "identification, friend or foe" radar frequencies to distinguish themselves from enemy forces.

Similarly, the original GPS signals were designed in the 1970s, around the same time that Steve Jobs and Steve Wozniak worked on the Apple 1 computer. M code incorporates a modern signal design that enables sophisticated signal-processing techniques which, when combined with the higher signal power on GPS III, will decrease the effective range of enemy military jammers against GPS receivers. Just as radar has continued to evolve since its inception, so will GPS antijamming technologies continue to mature and offer distinct advan-

tages for the US military and allies. In addition to jamming, the GPS has proven vulnerable to "spoofing," a deception technique using electronic warfare to fool a GPS receiver into locking onto false signals rather than GPS satellite signals. Prof. Todd Humphries of the University of Texas recently testified to Congress that his team of graduate students used a spoofing transmitter to take control of a GPS-guided remotely piloted vehicle, causing it to dive toward the ground.[14] The DOD has long known of this threat and has taken measures to prevent it. Antispoofing has always been a feature of military GPS, using encrypted signals as the first line of defense. Moreover, M code cryptography is far more advanced than its older sister, the P(Y) code. Codesigned by the GPS Directorate and the National Security Agency, M code is comparable to modern systems that protect much more critical data, and it will protect war fighters from spoofing for decades. Additional measures include smart algorithms incorporated into the Military GPS User Equipment Program, whose receivers can sort out false signals from the satellite signals and reject them, giving the user high assurance.

In the early 2000s, the DOD began employing the Selective Availability Anti-Spoof Module, which introduced over-the-air rekey, over-the-air distribution, and contingency recovery—a technique that resets GPS receivers from possible compromise of the GPS key, thus improving positive control and resiliency. GPS modernization takes this even further. Working with the National Security Agency to leverage its key-management infrastructure, US Strategic Command will have even more tools to ensure that only authorized users have access to M code, that the user is protected from spoofing, that keys are readily available to US and coalition partners, and that the drivers of security expenses for user equipment remain minimal.

The recent launch of the fourth GPS IIF satellite on 15 May 2013 once again has demonstrated Air Force Space Command's commitment to mission success. Because of the current limitations of the ground-control segment, the launch of this latest satellite will "max

out" the constellation with 31 operating satellites at 11,047 nautical miles above the earth in an inclination of 55 degrees to the equator. To ensure continued service, the GPS Program Directorate at the Space and Missile Systems Center, Los Angeles AFB, California, has already delivered five additional GPS IIF satellites to storage, a precedent not attained in well over a decade. These satellites now allow tremendous flexibility to launch on demand when the operational need arises, should a significant series of failures occur.

The GPS Directorate is also investing in the future capability of both the satellite constellation and the ground segment to provide improved command and control of GPS signals. Next-generation GPS IIF and III satellites are in various states of assembly, integration, test, and production in an effort to improve the average user-range error from 0.9 meters—established and maintained for the last three years—to a root-mean-squared user-range error of 0.5 meters by 2016. Clearly, space superiority is based as much upon PNT accuracy as upon the ability to conduct land, sea, or air operations at a given time and place without prohibitive interference by an opposing force. Toward that end, the GPS III satellite system, with its first launch scheduled for 2015, employs up to eight times the amount of M code power; a designed 15-year lifespan; a new, internationally compatible civil signal (L1C); and greater accuracy. To maintain a competitive edge over other global navigation satellite systems and to reduce costs, the GPS Directorate is also funding technologies that will provide a return on investment. For example, lithium ion batteries greatly reduce the weight of the satellite, and improved solar cells produce more power at reduced cost, as does the combining of star trackers and inertial measurements into a single component on the spacecraft. Furthermore, digital waveform generation (the ability to change on-orbit signals in space via software commands instead of hardware upgrades, necessarily requiring the launching of new satellites) could become an integral part of the future enterprise architecture.

In addition, the Next Generation Operational Control System (OCX) is designed to command and control our modernized secondary civil signal L2C (1227.60 MHz), safety-of-life signal L5 (1176.45 MHz), and the internationally compatible L1C (1575.42 gigahertz) signal. These additional civil signals include the ability to correct for ionospheric effects and achieve a resulting improvement in accuracy currently enjoyed by military receivers. Importantly, the OCX will no longer be limited to the command or control of only 31 satellites since the system is being designed to accommodate up to 64 GPS satellites. The OCX's expandability and service-oriented architecture will give users and operators the security, information assurance, and flexibility they simply do not have today.

Affordability and Innovation

Even with all of these improvements, affordability demands innovative ways to deliver the GPS to war fighters. More than 165,000 precision lightweight GPS receivers (PLGR) have been procured worldwide and over 478,000 defense advanced GPS receivers (DAGR) have been ordered (the PLGR and DAGR are the most common military receivers in the DOD).[15] The initial DAGR was a marvel, weighing just one pound versus the PLGR's 2.7 pounds and adding dual-frequency GPS as well as a map display. Both the PLGR and DAGR have become the standard GPS receivers for ground forces. Today, however, most of them (60–70 percent) are used in vehicles, often with three or more DAGRs mounted in an Army vehicle, all operating independently. The functionality and user interface of the DAGR, a handheld device, don't compare well with those of the lightweight, user-friendly commercial devices to which Soldiers have become accustomed. If the DOD designed something equivalent today, it would not keep pace with the innovation and life cycles typical of commercial technology.

The Army recognized this challenge and established a policy in 2009 that called for procurement of embedded receivers, initiating the development of two devices known as the "HUB" and the "PUCK." In

many cases, these new devices will enable the Army to replace up to five DAGRs in a vehicle such as a tank with a single embedded ground card. Embedded devices will also replace the concept of GPS handhelds; instead, systems for dismounted Soldiers will be developed with GPS embedded to support an evolving human interface. In March of 2012, the Army introduced the Army Marketplace, with 12 initial apps available for iOS devices. Most of these concentrated on training needs and handbooks, but in other research activities, the service has developed and tested other apps for combat support, including augmented reality and navigation.[16]

Given the ready availability of devices such as smartphones and iPads, it no longer makes sense for the DOD to invest in stand-alone devices with archaic user interfaces. The GPS Directorate is working with Aberdeen Proving Ground to marry commercial off-the-shelf technology, which changes quickly, with secure, enhanced, and robust GPS. A key cornerstone in our overall strategy entails production of the Common GPS Module. Explicitly designed with a small, minimalist package to support diverse applications, it will prove suitable for integration in a wide range of devices, from smartphones to secure radios. The module will be indistinguishable from the human-machine interface, delivering performance in an electronic warfare environment. Further, it will be a key element of munitions programs such as the small-diameter-bomb direct-attack munition and the precision guidance kit for mortars.

As affordability becomes more important, procurement strategies can adapt according to the mission need. In some cases, situational awareness of an enemy jamming or spoofing in the area may be sufficient. For example, the Rifleman Radio, carried by individual platoon members, is used primarily for voice communications, but it has an inexpensive C/A code chip that reports location to the platoon leader, who has a display. An affordable upgrade may involve providing a secure, lightweight Selective Availability Anti-Spoof Module or M code capability to the platoon leader using the Common GPS Module. Oper-

ating procedures could produce the same effect as giving every Soldier the antijamming/antispoofing capability of M code but at a fraction of the cost. Many systems may not need M code at all. Consider, for example, the T-6 Texan II, the T-38 Talon, and T1A Jayhawk aircraft, flown primarily at bases in the continental United States for undergraduate pilot training. In such a basic training environment, spoofing and/or jamming is highly unlikely, obviating the need for such code.

As the GPS has become more sophisticated, delivering more capability to both civil and military users, the cost of the spacecraft, including launch, has increased tremendously. The expenditure necessary to put a GPS III in orbit now approaches half a billion dollars. Furthermore, national policy and worldwide expectations are driving the minimum constellation size to 30 satellites on orbit even though a 24-plus-three (on-orbit spares) satellite constellation is considered nominal.[17] As aging Block II satellites reach the end of their life span during the next decade, this higher expectation will become burdensome for the DOD. To explore alternatives, Air Force Space Command has initiated an architecture study to define an augmentation strategy with GPS III to reduce the total ownership cost while meeting performance expectations. This strategy, known as "Navsat," calls for producing and launching simpler, lighter, and cheaper satellites two or three at a time. Navsat will ensure that the Air Force delivers on the White House's objective that GPS remain the premiere satellite navigation system in the world. Moreover, by augmenting the GPS III satellite system with eight to 12 cheaper satellites, we can retain competition, bolster the defense industrial base, and reduce total life-cycle costs.

The Global Positioning System as a Cornerstone of Space Superiority

In many ways, today's satellite navigation technology resembles automobile technology in the 1960s. For example, consider some models of the Chevy Vega, whose aluminum engine block warped, or the 1960

Corvair, called by many the most dangerous car ever put on the road.[18] Or consider any automobile before the 1964 Mustang, which marketed seat belts as an option until they became mandatory in 1968.

Since the 1960s, cars have incorporated system safety and efficiency features that did not change the fundamental nature of the car but arguably saved lives and reduced costs. According to the National Highway and Traffic Administration's estimates, child restraints, seat belts, and airbags saved over 90,000 lives from 2003 through 2007.[19] Power steering, power brakes, and fuel injection have improved control and comfort. Fuel emission standards have reduced air pollution in major cities—easily confirmed by observing the thick smog in television shows filmed in Los Angeles in the 1970s. Many of these auto safety initiatives were expensive, premium features when introduced, and resistance to safety legislation from consumers and legislators was intense. Yet, the evolution of the automobile has improved millions of lives.

Similarly, the GPS must evolve, and the delivery of GPS modernization is critical for US battlefield superiority in the future. The GPS was conceived in the late 1960s and early 1970s, deployed in the 1980s, and widely adopted in the 1990s. Antijamming and antispoofing are like seat belts and air bags insofar as they improve the reliability and availability of precision PNT to aircraft, bombs, ships, vehicles, communications systems, and personnel. Enhanced signal and key management are like power steering and power brakes insofar as they make the system more effective and efficient. Just as Congress specified requirements for seat belts, so does Title 10 *United States Code*, section 2281, demand that all military GPS receivers be M-code capable. And just as the seat belt met resistance, so is there reluctance to program M code receivers into the Future Years Defense Program even though, like the automobile, M code receivers—in terms of safety—will be superior to commercial receivers.

The GPS has its competitors, the most formidable of which have the backing of their national sponsors. The Russians have reinvigorated

their Global Navigation Satellite System (GLONASS) and since October 2011 have provided a full 24-satellite constellation for the first time since late 1995. The Chinese are rapidly populating the satellite constellation of their BeiDou system but actually rely on the GPS constellation to operate fully. The Japanese Quasi-Zenith Satellite System augments the GPS through highly inclined satellites with long dwell times over the home islands. The European Union has recently committed to buying what will become a full-complement system with 30 satellite vehicles.

The GPS is—and for the foreseeable future will remain—the best global satellite navigation system in the world, and the United States has the ability to retain the space superiority enabled by the GPS. Like a high-performing NASCAR team, America must continue to rely on engineering excellence, innovative management, and sustained operational excellence to maintain the leadership position that the GPS now enjoys. The United States and the Airmen who provide this vital global utility free of charge for the world should be justifiably proud of its history and capabilities. The GPS must continue to evolve as warfare evolves. As Gen Giulio Douhet aptly observed, "Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."[20] ✪

Notes

1. The GPS is a space-based positioning, navigation, and timing system. With a constellation of at least 24 satellites (currently more than 30) in medium Earth orbit, it provides global positioning and timing by broadcasting radio frequency signals at three frequencies in the L-Band: L1 (1575.42 megahertz [MHz]), L2 (1227.6 MHz), and L5 (1176.45 MHz). The user's GPS receiver obtains position and time by tracking four or more satellites and determining the time of arrival of each radio signal, which propagates at the speed of light. For more information on GPS, see "The Global Positioning System," GPS.gov, 17 January 2013, http://www.gps.gov/systems/gps/.

2. Joint Publication 3-14, *Space Operations*, 29 May 2013, GL-8, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

3. "Desert Storm: The First Space War," in *Gray Space and the Warfighter*, 17 June 1997, http://www.au.af.mil/au/awc/awcgate/grayspc/dstorm/dstorm.htm.

4. Ibid.

5. The GPS is integral to nearly all smartphones today. According to CNET, "During the third quarter [of 2012], the total installed base for smartphones worldwide hit 1.04 billion, jumping from the 959 million smartphones in use during the second quarter, research firm Strategy Analytics announced today." Don Reisinger, "Worldwide Smartphone User Base Hits 1 Billion," CNET, 17 October 2012, http://news.cnet.com/8301-1035_3-57534132-94/worldwide-smartphone-user-base-hits-1-billion/.

6. Nam D. Pham, PhD, *The Economic Benefits of Commercial GPS Use in the U.S. and the Costs of Potential Disruption* (Washington, DC: NDP Consulting Group, June 2011), 1, http://www.saveourgps.org/pdf/GPS-Report-June-22-2011.pdf.

7. "Because the Global Positioning System (GPS) was so accurate (although not as accurate as laser-guided bombs) and could be used in all weather, the Joint Direct Attack Munition was the favorite. While designed to be used against high-value, fixed targets, JDAMs were heavily used against relatively low-value targets and in close air support missions flown by bombers at relatively high altitudes. The extensive use of precision-guided munitions greatly improved the Air Force's ability to hit targets, in any weather." Kristin F. Lynch et al., *Lessons from Operation Iraqi Freedom* (Santa Monica, CA: RAND Corporation, 2005), 95, http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG193.pdf.

8. "Selective Availability (SA). Protection technique employed by DoD to deny full system accuracy. On May 1, 2000, President Clinton announced the discontinuance of SA effective midnight 1 May 2000. The effects of SA went to zero at 0400 UTC on 2 May 2000." Department of Defense, *Global Positioning System Standard Positioning Service Performance Standard*, 4th ed. (Washington, DC: Department of Defense, September 2008), C-4, http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

9. "Instantaneous User Range Error (URE). An instantaneous URE is the difference between the pseudorange measured at a given location assuming a receiver clock that is perfectly calibrated to GPS time and the expected pseudorange as derived from the NAV [navigation] message data for the given location and the assumed receiver clock. The instantaneous SIS URE [signal-in-space user-range error] includes only those pseudorange data set error budget components assigned to the GPS Space and Control Segments (i.e., not including the error budget components assigned to the GPS User Segment such as the troposphere delay compensation error, multipath, and receiver noise)." Ibid., C-2.

10. Ibid., 22.

11. Presidential Decision Directive NSTC-6, *US Global Positioning System Policy*, 28 March 1996, http://www.fas.org/spp/military/docops/national/gps.htm.

12. United States Strategic Command, *Joint Capabilities Document for Position, Navigation, and Timing* (Offutt AFB, NE: United States Strategic Command, 28 September 2006), 4. FOUO. Information extracted is unclassified.

13. GPS II refers to the second generation of GPS satellites although Block II was actually the first series of operational GPS satellites. The designators IIA (advanced), IIR (replenishment), and IIF (follow-on) represent the versions of Block II satellites. To date, four of 12 IIF satellites have been launched.

14. House, *Professor Tom Humphreys, Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to GPS Spoofing, Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security*, 112th Cong., 2nd sess., 19 July 2012, http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg80848/html/CHRG-112hhrg80848.htm.

15. Data obtained from GPS User Equipment Division contracts.

16. "Another app, called 'SoldierEyes,' turns a smartphone into a sort of battlefield navigation device. In addition to displaying a digital map, it features an 'augmented reality' mode that enables the user to flip on the camera and scan the horizon. Digital markers pop up on the screen, displaying the direction and distance to objectives on the battlefield." Nathan Hodge, "Killer App: Army Tests Smartphones for Combat," *Wall Street Journal*, 3 June 2011, http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html.

17. "According to Dr. Sheila E. Widnall, Secretary of the Air Force, the Air Force recognizes the tremendous civil and military aspects of GPS, and fully intends to maintain a 24-satellite constellation for the duration of the program." "President Opens Door to Commercial GPS Markets: Move Could Add 100,000 New Jobs to Economy by Year 2000," press release (Washington, DC: White House, Office of the Press Secretary, 29 March 1996), http://clinton3.nara.gov/WH/EOP/OSTP/html/gps-pressrel.html.

18. "The Most Dangerous Cars of All Time," CarsDirect.com, 24 February 2012, http://www.carsdirect.com/automotive-news/the-most-dangerous-cars-of-all-time.

19. National Highway Traffic Safety Administration, *Lives Saved FAQs* (Washington, DC: National Highway Traffic Safety Administration, December 2009), 4, http://www-nrd.nhtsa.dot.gov/Pubs/811105.PDF.

20. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of the Air Force History, 1983), 30.

Col Bernard J. Gruber, USAF

Colonel Gruber (BSME, North Dakota State University; MSBA, Central Michigan University) is the director of the Global Positioning Systems Directorate. He is responsible for a multiservice, multinational systems directorate that conducts development, acquisition, fielding, and sustainment of all Global Positioning System (GPS) space segment, satellite command and control (ground), and military user equipment. The $32 billion GPS program, with a $1 billion annual budget, maintains the largest satellite constellation and the largest avionics integration and installation program in the Department of Defense. Commissioned in 1986, Colonel Gruber is a graduate of Squadron Officer School, Air Command and Staff College, Air War College, Defense Systems Management College, and Joint Forces Staff College, and has commanded at the squadron, group, and wing levels. A member of the Acquisition Corps, he is a certified joint specialty officer and National Defense Fellow alumnus. Colonel Gruber has distinguished himself in a variety of leadership positions within the operations, intelligence, launch, engineering, and acquisition disciplines. He has served in key positions at major command, Air Staff, Joint Staff, and Defense Agency levels. Prior to assuming his current position, Colonel Gruber served as one of four mission panel chiefs on the Air Staff, responsible for future budgeting for all space and intelligence, surveillance, and reconnaissance programs across the Air Force.

Col Jon M. Anderson, USAF, Retired

Colonel Anderson (BSEE, University of Kansas; MSEE, South Dakota State University; PhD, Air Force Institute of Technology) is the former chief of the Global Positioning System (GPS) User Equipment Division. He was responsible for leading over 299 military, civilian, and contractor personnel executing multiple development and production contracts valued at more than $2 billion and delivering secure GPS capabilities to Department of Defense and allied users. Commissioned in 1988, Colonel Anderson is a graduate of Squadron Officer School, Air Command and Staff College, and Naval War College. He has commanded at the squadron and group levels and has a broad Air Force background, with experience in missile operations, technical intelligence analysis, systems engineering, operational test support, national and international space policy, and program management. Colonel Anderson was recently recognized by the Institution of Navigation as the recipient of the 2012 Captain P. V. H. Weems Award for sustained contributions to modernized military GPS, leading enhanced capabilities for US and allied military operations in a navigation warfare environment.