AIR FORCE SPACE COMMAND

Volume 2, Number 3

HIGH FRONTIER

THE JOURNAL FOR SPACE & MISSILE PROFESSIONALS

SPACE COMMAND & CONTROL

U.S. AIR FORCE

HIGH FRONTIER

The Journal for Space & Missile Professionals

April 2006 Volume 2, Number 3

Headquarters
Air Force
Space Command
Peterson Air Force Base, Colorado

Vice Commander
Lt Gen Frank G. Klotz

Director of Public Affairs
Lt Col Marcella Adams

Creative Editor
Ms. Nadine Sage

High Frontier Staff

Lt Col Michael Pierson
Lt Col Kent Dalton
Maj Corvin Connolly
Mr. Masao Doi
Capt Karim Ratey
1Lt Jennifer Whitaker
TSgt Kate Rust
TSgt Jennifer Thibault

Published by a private firm in no way connected with the US Air Force, under exclusive written contract with Air Force Space Command. This command funded Air Force journal is an authorized publication for members of the United States military Services. Contents of *High Frontier* are not necessarily the official views of, or endorsed by, the US Government, the Department of Defense, or the Department of the Air Force.

Editorial content is edited, prepared, and provided by the Public Affairs Office of Air Force Space Command. All photographs are Air Force photographs unless otherwise indicated.

High Frontier, Air Force Space Command's premier space professional journal, will be published quarterly. The journal provides a scholarly forum for professionals to exchange knowledge and ideas on space-related issues throughout the space community. The journal focuses primarily on Air Force and DoD space programs; however, the *High Frontier* staff welcomes submissions from within the space community. Comments, inquiries and article submissions should be sent to AFSPC.PAI@peterson.af.mil. They can also be mailed to:

AFSPC/PAI
150 Vandenberg St. Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3978
Fax: (719) 554-6013

For more information on space professional development visit:
http://www.peterson.af.mil/spacepro

To subscribe: nsage@colsa.com

DISCLAIMER: The views and opinions expressed in this journal are those of the authors alone and do not necessarily reflect those of the United States Department of Defense, the United States Air Force, or any other government agency.

COVER: At its HI-Vision laboratory in Colorado Springs, Lockheed Martin is engaged in developing integrated network-enabled solutions for Space command and control to conceive, plan, and execute vital national operations and deliver real-time information to decision makers around the world.

Photo credits: Lockheed Martin
Back cover: Photo/illustration by Erik Simonsen, The Boeing Company

Contents

Introduction

Senior Level Perspective

Industry Perspective

Space Command and Control

Future Forecasts

Book Review

Next Issue: ***The Future of Strategic Deterrence and the ICBM***

Introduction

Space Command and Control: The Lynchpin to Our Success

Lt Gen Frank G. Klotz
Vice Commander, Air Force Space Command

"Once the command of the air [and space] is obtained by one of the contended armies, the war must become a conflict between a seeing host and one that is blind."

- H. G. Wells

There are many imperatives within the National Security Space (NSS) enterprise. However, as we drive to further operationalize space, the lynchpin to our success is Space Command and Control (C2). The goal of this issue of the "High Frontier" is to examine where our Space C2 efforts are succeeding and where we are missing the mark. Up to this point, we have been able to meet joint warfighter needs through sheer brute strength. If an answer or a solution was not available, we simply engineered one. This ad hoc approach will not be adequate as we continue to transform military operations and fight the "Long War."

From an Air Force Space Command perspective, we must understand a few key characteristics about the environment in which we operate. First, we must establish a warfighter perspective in everything we do. It is this perspective that will enable us to deliver tailored space combat effects to joint warfighters. Second, the legacy era of operating space systems in isolation is quickly coming to an end. As systems such as the Transformational Satellite, Space-Based Infrared, and Space Radar come on line we will realize the importance of dynamic tasking and the need for interdependency across our military. Finally, speed of action is central to every new innovation. To effectively fight in the information age we need the right data before the adversary has the opportunity to react.

Space is an inherently joint activity. One hundred percent of everything we do and the money we spend goes toward fielding joint capabilities. Space C2 is not about checking a box and accomplishing something we promised to deliver. It is about meeting warfighter needs. Warfighters do not want excuses about artificial boundaries between black and white space. Warfighters do not want explanations of the differences between Military Satellite Communications and commercially provided services. Warfighters want to know that when they need space combat effects they will be there. They want space capabilities to be as automatic as flipping on a light switch.

> *"To conquer the command of the air [and space] means victory; to be beaten in the air [and space] means defeat and acceptance of whatever terms the enemy may be pleased to impose."*
>
> - Giulio Douhet

So, the first essential ingredient in our Space C2 architecture must be the warfighter. At its heart it is about providing tailored space combat effects. Accomplishing this feat requires us to be connected at the hip and horizontally integrated across the NSS enterprise, the Department of Defense, and with federal, state and local agencies. As we saw after Hurricane Katrina, sometimes the warfighter is not a warfighter at all. The tailored space effects we provide could be in support of various agencies right here at home. Our Space C2 architecture absolutely must be capable of fully integrated operations across this wide spectrum of space customers.

One of the key hurdles to delivering tailored space effects is without question our organizational construct. Once again, any changes we make to our organizational construct must take the warfighter into account. All of us have been confused by the myriad of complicated wiring diagrams trying to explain the future of Space C2. The first test for an effective organizational construct should be simple. If we cannot understand it, it is probably not the correct answer. Furthermore, the right organizational structure may lie outside of anything we presently know. It is essential for us to look at this issue with a clean slate and not attempt to fit it into current models just because they exist and we have always done it that way.

The second imperative driving change is the development of "Third Generation" space systems. Transformational Satellite Communications, Space-Based Infrared, and Space Radar are as different from our legacy systems as the F-15 and F16 are from our "Fifth Generation" fighters, the F-22 and F-35. We will operate these systems in a dynamic tasking environment where we must be interconnected with the joint warfighter and C4ISR as well as other space systems. Our objective is to remain one step ahead of any adversary, at all times. Success in this endeavor will first require a different type of space warrior. Radical adjustments to our training processes may need to be considered to eliminate the current stovepipe constructs. In addition, leaders must make a concerted effort to educate space warriors beyond their particular system or area of expertise.

We need space warriors that understand the full spectrum of combat operations. Our Secretary of the Air Force, The Honorable Michael Wynne, has laid out his vision and it can be seen in our new mission statement—"The mission of the United States Air Force is to deliver sovereign options for the defense of America and its global interests—to fly and fight in air, space and cyberspace." As space warriors we need to fully understand the "space" part of our mission, but we also need to internalize and understand air and cyberspace operations. Our Space Professional Development Program is leading us in that direction, but it is still up to each leader and individual to take it the next step.

There are additional ways in which we can leverage our people to enhance Space C2. Specifically, we are examining ways to bring more joint participation into the space team. The challenges in securing funding for key capabilities are well documented. What is not so well documented is our inability to bring enough members of our sister services into inherently joint organizations such as the Joint Space Operations Center (JSpOC) and the Space and Missile Systems Center (SMC).

Few positions within the command carry a joint billet designation. To continue making tremendous strides in bringing space to joint operations, we must encourage our sister services to provide high quality people to places like joint program offices in the SMC, the JSpOC, and the National Security Space Institute. We may want to consider joint duty credit for the appropriate positions as one way to achieve our goal.

The final piece of the puzzle involves speed. We have been criticized for relying on "PowerPoint Integration." Instead of a seamless operating environment with machine-to-machine interfaces, we have relied on our people and their ingenuity. Our space warriors are amazing, but we should not ask them to continue to engineer tedious operational workarounds. Information should flow across operations centers, from system to system, and ultimately to the user that needs it with minimal manual interaction.

There are also pitfalls we must be careful to avoid. Converting the current processes from a manual process to an automated process is not innovation. That is automation, which may or may not be an improvement. We have all seen examples of organizations that have attempted to do this. Invariably leaders of these organizations are surprised when the automation of existing processes fails to deliver the groundbreaking results promised. We cannot say it enough—the joint warfighter must be our central focus. We encourage our space warriors to break apart the existing paradigms and engineer the right solution, not the easy solution.

The challenges we face are sizable, but we can and will be successful. Our Intercontinental Ballistic Missile (ICBM) warriors have shown us the way for more than four decades. There are many positive lessons we can learn from ICBM C2. Our air-breathing warriors, as well as our sister services have also learned many lessons. As we build a global Space C2 architecture, we must incorporate best practices and devise solutions all of us can live with…air, land, sea, space, and cyberspace.

As you read through this issue of the "High Frontier," I encourage you to think critically about the challenges we face in Space C2. Not all of the view points will be complimentary, and we do not expect them to be. This is an incredibly complex topic and there are many different approaches. However, the one constant still remains the joint warfighter. Any path we choose must first tailor our solution to the needs of the joint warfighter and our ability to meet their needs. We must engineer solutions that go beyond today's operational models and answers the questions of tomorrow's dynamic environment. Finally, now more than ever, it is speed that will save the lives of our soldiers, sailors, Airmen, Marines, and coastguardsmen …our most valuable resource.

Lt Gen Frank G. Klotz (BS International Affairs, USAFA; MPhil, International Relations, Oxford University; PhD Politics, Oxford University) is Vice Commander, Air Force Space Command, Peterson Air Force Base, Colorado. He assists the Commander in the development, acquisition and operation of the Air Force's space and missile systems. The command oversees a global network of satellite command and control, communications, missile warning and launch facilities, and ensures the combat readiness of America's intercontinental ballistic missile force. The command comprises more than 39,700 space professionals who provide combat forces and capabilities to North American Aerospace Defense Command and US Strategic Command. General Klotz also directs and coordinates the activities of the headquarters staff.

He has commanded a Minuteman missile squadron, a missile launch task force, an operations group, a missile wing and a numbered air force. The general's staff assignments include tours on the Air Staff, in the Office of the Secretary of Defense and at the State Department as a White House Fellow. He has also served on the faculty of the Air Force Academy, at NATO headquarters in Brussels, at the American Embassy in Moscow, Russia, and as the Director for Nuclear Policy and Arms Control with the National Security Council at the White House.

General Klotz is a graduate of Squadron Officer School, National War College, and the Senior Officials in National Security Program at Syracuse University, New York.

SATCOM: A Critical Enabler for Our Joint Warfighters

LtGen Robert M. Shea, USMC
Director, C4 Systems, J6

In the continuing Global War on Terror, joint warfighting forces are more mobile, more precise and more lethal than ever before. To this end, we have become increasingly reliant upon networked capabilities. Given the austere environments, rugged terrain and greater distances at which our deployed forces operate, satellite communication (SATCOM) is the mainstay for networking forces with warfighting capabilities. The timely delivery of decision-quality information to ground, air, space, and maritime forces provides us a warfighting advantage against evolving adversaries across the entire continuum of warfare. As our Joint Force capabilities grow, we must confront SATCOM-related challenges now, so we can depend on this critical joint warfighting enabler in the future. These challenges are not mutually exclusive, but the solutions have synergistic effects. Proactively working the challenges is imperative so that we are less reactive in mitigating future threats. Countering threats to our space dominance with thoughtfully defined capabilities, as well as sound investment, acquisition, and information assurance strategies are paramount to sustaining our competitive edge.

> *Countering threats to our space dominance with thoughtfully defined capabilities, as well as sound investment, acquisition, and information assurance strategies are paramount to sustaining our competitive edge.*

Global threats are asymmetric and diverse. They have caused the Department of Defense (DoD) to reexamine the organization and capabilities of our forces. The days of massed forces along linear borders with similarly echeloned antagonists are rapidly becoming a design of the past. Today's joint and combined warfare occurs over a non-contiguous battlespace of varying terrain and under demanding, stressful conditions. SATCOM networks connect disparate capabilities and truly puts the "Global" into the Global Information Grid (GIG), the military's strategic, operational, and tactical equivalent of the Internet.

The GIG is the information backbone for delivering net-centric warfighting capabilities for joint forces. Net-centricity is the interlinking of information technology, weapons platforms and personnel, along with doctrine, tactics, techniques, and procedures (TTPs), that permits near instantaneous information exchange. Research indicates and experience supports that networked forces bring increased capability and are dramatically more effective than their non-networked counterparts.[1] SATCOM is increasingly providing the connectivity necessary to link dispersed forces across the continuum of operations. SATCOM's ability to bridge the "first tactical mile" of forward-deployed forces and reachback through the GIG to key sources of information provides dispersed joint warfighters with a critical enabler for actionable decisions.

SATCOM Support to Current Ops

SATCOM is a key force multiplier in supporting networked expeditionary operations. Its beyond line-of-sight capability, broad coverage and large bandwidth capacity allows critical information exchange between and across all echelons of command and control, logistics, and intelligence, surveillance, and reconnaissance (ISR) activities.

We have seen glimpses of the power of this capability. In the very early stages of Operation ENDURING FREEDOM, the Afghan Northern Alliance forces were impressed with our ability to use man-packed tactical SATCOM to rapidly share time sensitive targeting data with B-52s in near-real time, in order to drop bombs on the Taliban forces. During the initial phases of Operation IRAQI FREEDOM, a wide variety of SATCOM assets provided Naval Strike Groups with mission updates, allowing precision Tomahawk missile strikes. Nearly every aspect of the Naval campaign used SATCOM for its networking needs. Without SATCOM, alternative communication means would have dramatically slowed the execution of the campaign and support of ground forces.

Today, ISR information is routinely downlinked from satellites to commanders in order to rapidly support key decisions. As an example, inside the Air Operations Center (AOC), whether Joint or Combined, there is a communication support team in charge of command, control, communications, and computers (C4) requirements and activities. It acts as a conduit in working with operational users. SATCOM enables the AOC to swiftly process, manage, and fuse intelligence from across a variety of sources in order to reduce information cycle timelines and thus shorten the sensor to shooter loop.

SATCOM facilitates synchronization of our mobile and distributed forces. Its reachback capability not only supports mission success, but also provides access to information sources that improve the quality of life of forward deployed personnel. SATCOM also allows us to deploy with a smaller footprint and facilitates faster and improved decisions in order to better direct actions in the battlespace. Furthermore, it enables morale programs such as video teleconferencing and e-mail between military personnel and their families. The bottom line is SATCOM can be used to strengthen all aspects of joint warfighting. That stated, we have more work to do.

SATCOM Investments

Continued investment in SATCOM systems is crucial to achieving net-centricity. Today's military SATCOM systems are aging, especially when compared to new capabilities available in the commercial market. Consequently, we must continue to invest institutional energy and work with the services, Combatant Commands (COCOMs) and agencies to advocate and defend the funding for new space capabilities. Key initiatives such as the Advanced EHF System, the Mobile User Objective System, and the Transformational Communications System represent the foundation of new networking capabilities. In addition to providing increased bandwidth and greater coverage, it's essential that we capture advancements in new information technologies. These advancements will help bring us closer to true net-centricity and transform the way our forces operate. We are advancing to a point where future weapon platforms will become a node on the network. Our networks and associated nodes will form a robust information enterprise that will reliably provide information where it is needed, when it is needed, and to those who need it.

Having sound procedures and methods that enable us to quickly react to threats to our satellites and ground control segments is instrumental in keeping our satellites fully mission capable.

The DoD is investing time, intellectual capital, and resources in transformational communications in anticipation of significantly improved warfighting capability. In order to reach this goal, we must more proactively integrate the capabilities offered by SATCOM technologies into our concept of operations. Improved SATCOM technology offers significant potential, but it will be limited if we do not develop sound concepts supported by appropriate TTPs.

SATCOM Acquisition

The transformation course we are embarked on is challenging. Anticipating future SATCOM system capabilities requires multi-dimensional insight and understanding of both the technical aspects of SATCOM and possible ways of employing it. Dynamically changing technologies, emerging threats and an increasing desire for additional capability demands that developers and users alike work closely together to evaluate trade-space in design, protection, and capability. We need to re-double our efforts in defining our most desired SATCOM capabilities and then support consistent funding of the developmental efforts if we are to deliver network-enabled forces in the required timeframe.

The Senior Warfighter Forum (SWarF) promotes a corporate SATCOM users perspective. It is chaired by and comprised of the COCOMs and other key stakeholders. It is an excellent venue to address capability shortfalls. The SWarF analyzes and prioritizes complex warfighting capabilities for the Joint Requirements Oversight Council, the adjudicator of joint warfighting capabilities.

Commercial SATCOM

Using military SATCOM first, then surging to commercial SATCOM has driven DoD investments in the past. We now understand that we need to carefully consider commercial SATCOM as part of an integral mix in the DoD's warfighting architecture. To better accomplish this, we are changing our commercial SATCOM provisioning paradigm. As part of this maturing partnership with commercial industry, we have identified several desirable SATCOM joint warfighting attributes that we want built into our contracts such as responsiveness, coverage, network operations, flexibility, capacity, and protection.

Further, we need to improve our methods of constructing leasing agreements in order to promote bandwidth bundling and provide flexibility for expanded capabilities. We need to take full advantage of discount rates that will be a natural outgrowth of purchasing commercial bandwidth in bulk. Ultimately we need to determine how to best structure lease agreements that are competitive and flexible enough to meet DoD's growing demands. We see this as mutually benefiting for commercial satellite providers and DoD.

Protection

With our ever-increasing reliance on SATCOM and the GIG, comes a higher expectation that our networks must operate all of the time; uninterrupted. Therefore, protecting the space segment as well as the terrestrial control segments must be a major focus. We must consider end-to-end capability protection.

In defending our networks, we must build and implement a comprehensive and well thought out information assurance (IA) strategy. IA is not just cryptography. It includes policy, integrated systems and processes that continuously monitor, detect, avoid, and prevent all forms of cyber threats from impacting operations. Embedding IA early into the SATCOM design is important so that it is not overlaid as a secondary and overly expensive feature. IA must be part of a sound life cycle management plan to reduce the instability and vulnerability of our networks.

Protecting our satellites is just as important as protecting our terrestrial networks. Having sound procedures and methods that enable us to quickly react to threats to our satellites and ground control segments is instrumental in keeping our satellites fully mission capable. Working with our industry partners and creating better situation awareness tools across the entire satellite network infrastructure will enhance our ability to mitigate threats.

Enhancement Opportunities

We also need to bolster and nurture the highly skilled and educated workforce that has supported our MILSATCOM programs over previous decades. Space acquisition is "rocket science," and is a tough and an unforgiving business. AFSPC's

While satellite communication initiatives continue to be a Joint Staff priority, we are supporting the pursuit of other capabilities that can provide space-like effects such as near-space platforms.

Space Professional Development Program is an example of how we, as a department, must aggressively identify, acknowledge, promote, and develop our current and future space professionals. Additionally, the development of a skilled pool of scientists and engineers in the private sector directly correlates to our military and national security needs. To that end, we must continue to collaborate with our industry partners to recruit and retain highly qualified personnel to support our aerospace programs.

While satellite communication initiatives continue to be a Joint Staff priority, we are supporting the pursuit of other capabilities that can provide space-like effects such as near-space platforms. Near space exhibits potential for a revolutionary 4th layer of coverage (ground, air, near space, and space), and we are researching and developing platforms to operate in this environment. This region shows promise to provide more capabilities for the warfighter, especially at the tactical and operational levels of war where commanders are unable to use high-demand strategic SATCOM resources due to limited availability. The bottom line is that near space has the potential to fill capability gaps in our space segment as an additional tool for the warfighter, not a replacement.

Conclusion

The way in which war is waged has changed dramatically over the past decade. Our joint forces have adapted to this new environment by becoming more dispersed, mobile, and skilled at directing the effects on targets. SATCOM has helped joint operations throughout the battlespace by providing a reliable method for information and decision transport. While we are addressing several issues for the future, we have a solid foundation for growth. The military will remain flexible and committed in its use of SATCOM. We have made significant progress toward net-centricity enabled by SATCOM. I am confident that through the combined efforts of space professionals, joint forces, academia, and industry we will be able to take combat capabilities enabled by SATCOM to the next level.

Notes:

[1] Maryann Lawlor, "War Validates Netcentricity Concept," *Signal,* November 2005, 17-22.

LtGen Robert M. Shea (MA, Central Michigan University) serves as the Director, Command, Control, Communications and Computer Systems (C4 Systems), The Joint Staff. He is the principle advisor to the Chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense.

His service spans 35 years. Prior to his current assignment, Lieutenant General Shea was the Deputy Commander, United States Forces, Japan. His command positions include Commander of the Marine Component to the Joint Task Force Computer Network Defense, Director of the Marine Corps Command and Control Systems School, Commanding Officer, 9th Communications Battalion, I Marine Expeditionary Force during DESERT SHIELD and DESERT STORM. Other assignments include Commanding Officer of two communications companies and the Battalion Communications Officer for 1st Amphibian Tractor Battalion, 3d Marine Division.

Lieutenant General Shea's previous staff assignments include serving as the Director for Command, Control, Communications and Computers (C4) for the Marine Corps, the Chief Information Officer of the Marine Corps, Director of Intelligence for the Marine Corps, the Director for Command, Control and Communications (J6), for the United States Pacific Command, Head, Command and Control Telecommunications Systems Branch and Head, Resources Branch, C4 Department, Headquarters United States Marine Corps, Assistant Chief of Staff, G6 Operations, 3rd Marine Division, Head, Plans Division and Systems Control Officer for the Defense Communications Agency Pacific Area, the Assistant Inspector-Instructor, 6th Communications Battalion.

Lieutenant General Shea also attended The Basic School, Advanced Communications Officers' Course, the Marine Corps Command and Staff College and the Industrial College of the Armed Forces, National Defense University.

Joint Space Command and Control

RADM Melvin G. Williams, Jr., USN
USSTRATCOM Director, Global Operations

Space Command and Control (C2) provides for the exercise of authority over assigned and attached space forces/assets and resources to monitor, assess, plan, and direct space operations at all echelons of command. Department of Defense (DoD) and the Intelligence Community require space C2 capabilities, providing commanders, decision makers, and leaders at any echelon the ability to obtain the required information to make informed decisions in a timely manner. Consequently, Space C2 provides the Joint Force Commander (JFC) the required capability to employ space systems to produce desired effects across the battlespace.

Background

In October of 2002, United States Strategic Command (USSTRATCOM) merged with United States Space Command forming the new US Strategic Command. That merger signified the DoD's commitment to addressing the unconventional challenges and strategic uncertainties we are confronting today. Because the security threats of the 21st century possess the key dimensions of "globalization and the potential proliferation of weapons of mass destruction," the Unified Command Plan added to that portfolio several previously unassigned missions. One of these missions is developing the desired characteristics and capabilities of, advocating and planning for, and conducting space operations.

Realizing the "new" USSTRATCOM was not optimally organized to handle its new mission sets, especially considering today's and tomorrow's security environment, General James E. Cartwright needed a more efficient and effective way to accomplish the Command's missions. The solution involved macro-level integration and "strategic partnerships" combined with decentralization and multiple, crosscutting connections between individuals and organizations. The resulting net-centric operations dispersed power, capitalizing on the creativity and productive capability of the experts in each area. It also involved a fundamental culture change in the Command to improve innovation in several areas instead of concentrating on just the legacy missions. The desired end state is that anyone should be able to get the information they need, anywhere they need it, at the time they need it to provide integrated solutions to the Nation's defense issues. USSTRATCOM and our Service components are embracing Net-Centric Warfare. All of the Service and Joint Transformational Roadmaps are based on a central principle. This is a means to develop and maintain a decisive warfighting advantage for our joint forces. When discussing the Four Pillars of Force Transformation, the number one pillar is strengthening joint operations through the development of joint operations concepts and architectures. Effective collaboration and coordination are required from each of the services to achieve this goal.

To realize the above vision, USSTRATCOM flattened the Headquarters organization and horizontally integrated Effects Based Operations and Network Centric Operations. Additionally, it created Joint Functional Component Commands (JFCCs) and Centers to handle operational level tasks. This construct allowed the Headquarters to maintain strategic level integration "up and out" while pushing operational level tasks to the JFCCs who had the expertise to handle day to day and crisis activities. One of the JFCCs to begin operations was JFCC Space and Global Strike (SGS).

The new organizational structure has now transitioned from theory to practice as USSTRATCOM is operationalizing its eight mission sets by aligning and updating its processes to be consistent with the new decentralized organizational construct. Improving USSTRATCOM Global Operations primarily entails supporting the JFCCs and all Combatant Commands. This includes performing integration with the Joint Staff, Office of the Secretary of Defense, and other non-DoD agencies and external organizations. As we will see this integration is especially important in the field of joint command and control of space operations.

Unity of Effort

On 18 January 2005, Commander, US Strategic Command (CDRUSSTRATCOM) directed the JFCC SGS Commander to optimize continuous planning, execution and force management of space operations. To focus on operational speed and cut across the boundaries that sometimes separate the four services, Commander (CDR) JFCC SGS designated the Commander, 14th Air Force as Commander, Joint Space Operations (CDRJSO). The CDRJSO is the primary USSTRATCOM interface for joint space effects to the supported commander under the authorities of the CDR JFCC SGS. The CDRJSO exercises tactical control (TACON) of designated space forces through the Joint Space Operations Center (JSpOC). This 24/7 node executes CDRJSO missions for joint space command and control.

The "Joint" in Joint Space Command and Control — the services are embracing Joint space command and control through providing additional Service representation to the JSpOC. Efforts are underway within the Navy and Army to increase the number of billets assigned to the JSpOC to make it a truly joint organization. This jointness will positively contribute to the overall mission of space C2.

The C2 of global space operations is complicated by fragmented authorities and organizational structures. Global space operations must support national security objectives and military operations across several theaters, including commercial and civil users. Multiple military organizations control space forces and deliver space effects. Intelligence and civil agencies, and many commercial companies also provide space force enhancement capabilities to support military and other national security operations. Moreover, US warfighters may depend on space services from foreign and international providers. Clearly, the inherently decentralized nature of space operations, and the different interests involved, requires some form of central command and control to integrate effects.

To maximize their efficiency and effectiveness, global space operations should be commanded, controlled, and coordinated to support a common set of objectives. Identifying operational and functional chains of command and establishing appropriate command relationships, such as operational control (OPCON), TACON, or support, helps ensure unity of action for military space forces. However, establishing command relationships for national, civil, and commercial space assets is extremely problematical, since their complex lines of authority extend beyond the DoD. In that case, designating a coordinating authority to facilitate unity of effort among those disparate organizations becomes crucial to ensure space superiority and joint warfighting effectiveness for US military forces.

CDRJSO has the command authority to compel unity of effort for the global military space forces CDRUSSTRATCOM controls. However, intelligence, civil, and commercial space assets are outside his span of control. To facilitate coordination and achieve unity of effort, the Command has established agreements and working relationships with several non-military space support organizations. These agreements create an avenue towards synergy, but work remains to be done to ensure a fully integrated effort. On a related note, the Secretary of Defense may direct CDRUSSTRATCOM to transfer control of specified space forces to another JFC. For example, a Joint Tactical Ground Station unit could be deployed and attached to a JFC for theater missile warning. This does not take the CDRJSO out of the loop. To the extent such forces may provide extra-theater effects or support USSTRATCOM's global missions, CDRJSO must harmonize, integrate, and/or synchronize their operations and effects.

In order to facilitate synchronization, CDRUSSTRATCOM established CDR JFCC SGS as the Global Space Coordinating Authority (GSCA) to enable unity of effort in global space operations. JFCC SGS further delegated GSCA responsibilities to CDRJSO, as he provides space operations expertise and C2 capabilities through the JSpOC. The GSCA is the single authority in USSTRATCOM to coordinate global space operations and integrate space capabilities CDRUSSTRATCOM does not control.

GSCA is not an authority by which C2 may be exercised. Rather, it is a specific consultation relationship between military commanders and other agencies. As such, the GSCA can require consultation between the agencies involved, but does not have the authority to compel agreement. Here's how it works: CDR USSTRATCOM will generate an establishing directive specifying the common tasks to be coordinated while not disturbing normal organizational relationships in other matters. Then, he grants the GSCA direct liaison authorized (DIRLAUTH) with USSTRATCOM's functional and service components; appropriate DoD, intelligence, and civil agencies; and with commercial space service providers, in accordance with established agreements, procedures, and relationships. In this manner, the GSCA can gain more inclusive results than each agency can working alone or with interests at odds with each other.

The CDRJSO's role as Global SCA is very different from the theater SCA's job. The theater SCA is primarily a space user. He is the JFC's single authority that requests support and theater space effects from CDRJSO. Since the JFC/JFACC (or other theater component commander) controls few if any space forces, he needs coordinating authority – thus SCA. Conversely, CDRJSO is primarily a provider of space forces and effects. He ensures unity of effort by prioritizing space requirements and directing the delivery of space effects across multiple theaters. The difference is also a matter of perspective. While the SCA wants to optimize satellite performance over his area of responsibility (AOR), the GSCA is concerned with how that will affect performance on the "other side of the world," including impacts to other AORs' users.

To accomplish the GSCA role, the CDRJSO has several wide-ranging coordinating responsibilities:

1. Establish, deconflict, prioritize, and integrate military, intelligence, civil, and commercial space requirements for CDRUSSTRATCOM and other combatant commanders.
2. Recommend guidelines for employing non-military space capabilities in global space operations.
3. Monitor the status of all military, intelligence, civil, and commercial space systems that affect global space operations.
4. Ensure interoperability among military and non-military space assets.
5. Recommend appropriate command relationships for space forces to CDR JFCC SGS.

CDRJSO's GSCA duties are vital to ensure integrated, synchronized space effects using all our space power capabilities. The following example shows how a single event involving one space asset affects several users having different interests. It also illustrates how the solution requires input from various communities; inputs the CDRJSO must synthesize and coordinate to produce effective action.

Joint Space Command and Control Exemplified

Fictitious Situation: In the not-too-distant future, the United States is engaged in combat operations in Central Command's (CENTCOM) AOR. Supporting CDRCENTCOM, the Combined Force Air Component Commander is planning to strike Time-Sensitive Targets and is relying on in-theater intelligence, surveillance, and reconnaissance (ISR) assets for targeting information. A commercial communications satellite, owned by an international consortium whose business headquarters is in the US, is relaying some of the ISR information to the Combined Air Operations Center (CAOC).

Threat: The adversary begins to reposition his forces and wants to hide the movement as much as possible. He talks to some people in another country outside the AOR. This country is sympathetic to his cause, and our adversary convinces them to employ commercial TV transmitters to overpower the commercial satellite signal supporting the CAOC. The jamming effectively impedes timely delivery of ISR data to the CAOC. As a further impact, the jamming "bleeds over" into an adjacent signal and interferes with the transactions of a Pacific Rim financial institution.

Problem: Who is responsible for leading the US response to this action?

Most answers involve numerous players. Clearly, the situation immediately impacts CENTCOM's mission. However, there is an impact in Pacific Command's AOR as well, and the adversary weapon system is physically located in, say, European Command. The commercial owner/operator under attack is based in Continental US and therefore is a Northern Command concern. The Department of State, the Director of National Intelligence, DoD, and Department of Commerce are all engaged. Finally, there are international actors including the governments of the impacted nations and the United Nations agencies governing telecommunications.

The scenario raises numerous legal, policy and C2 questions, but the central point of the event is the adversary is purposefully interfering with a US space asset. US policy considers this a space attack, and it requires remediation. CDRUSSTRATCOM has the Unified Command Plan mission of Space Defense. He has delegated authority for this mission to his Joint Functional Component Commander for Space and SGS. The CDR for JFCC SGS has in turn appointed a CDR for Joint Space Operations (JSO) to execute this mission for him.

In the example above, CENTCOM would do everything it could with in-theater assets to mitigate the effects of the attack while reporting the outage to the Global SATCOM Support Center (GSSC). The GSSC would immediately call the JSpOC, which would initiate a Space Operations Conference to share all available information on the threat system and task the subordinate organizations and intelligence agencies to gather more information. Simultaneously, Joint Task Force-Global Network Operations would work closely with the JSpOC to reroute the desired ISR data through another communications path to the CAOC. This is a temporary solution that provides some capability until the full long-term resolution is in place.

Next, CDRJSO would employ his space situation awareness capabilities to detect, characterize and geolocate the interfering signals, analyze the data, fuse with all-source intelligence, and provide the information to CDRUSSTRATCOM. Then, CDRUSSTRATCOM makes a formal assessment confirming the US is under a space attack and CDRJSO prepares Courses of Action (COA) to deal with the situation. The entire process requires the close collaboration and cooperation of numerous DoD and non-DoD agencies. He must take into account impacts to all parties involved (although some will have higher priority than others). He must also consider each one's contribution to the overall answer to develop comprehensive COAs that restore our capability.

Once CDRUSSTRATCOM selects a COA, CDRJSO will coordinate COA execution via his command, control, and coordination relationships to provide the most effective countermeasures and restore space capability. The execution includes monitoring the effects of the solution to ensure it is having the desired result, and to adapt to any further adversary action. Further, the AOR may take direct action to silence the jammer. In that case, CDRJSO would coordinate specific space support to theater missions to in effect "help them help us." Thus, the CDRJSO's GSCA duties take the event from "cradle to grave." Notification, plan formulation, coordination, and execution all run though a single entity, providing unity of effort among all parties.

Does the scenario sound far-fetched? It's not. In 2003, a nation jammed incoming Voice of America broadcasts originating from the US, and they did it from a third country's soil. The situation was ultimately resolved peacefully through the State Department, but highlighted organizational weaknesses within the US government for dealing with this type of threat. The new USSTRATCOM construct and way of doing business via coordinated action is working to overcome these weaknesses.

The threats to our Nation are continuously evolving. It is up to the military as one of the Nation's instruments of power to adapt to and overcome these new threats. USSTRATCOM and its components play a vital role in defending our nation, including global and regional space effects. The CDRJSO's JSpOC is the single "center of excellence" for C2 of joint space forces. As such, it enables the unmatched space effects we and our allies have come to rely on to conduct operations. The resulting rapid adaptability gives the US crucial decision superiority to defeat threats to space assets with full spectrum, integrated, and synchronized action.

RADM Melvin G. Williams (BS, Mathematics, US Naval Academy; MS, Engineering, Catholic University) is Director of Global Operations, US Strategic Command (STRATCOM), Offutt Air Force Base, Nebraska. He is responsible for maintaining full-spectrum global operations capabilities to meet both deterrent and decisive national security objectives. His duties encompass the traditional J3 role, as well as the J2, J4, J6, and J7 areas.

His previous assignments include Commanding Officer of the Trident Submarine USS Nebraska (SSBN 739)(Gold), Commander of six fast attack submarines at Submarine Squadron Four, Chief of Staff – Kitty Hawk Battle Group, Command of twelve submarines at Submarine Group 9, and Deputy Commander Joint Functional Component Command Space and Global Strike at STRATCOM. His tours include initial combat strikes during Operation DESERT STORM and Operation ENDURING FREEDOM.

Senior Level Perspective

Space Command and Control

Maj Gen Tommy F. Crawford, USAF
Commander, AFC2ISRC

As Maj Gen John T. "Tom" Sheridan stated in the previous edition of *High Frontier*, "the United States has become increasingly reliant on space systems for communications, signals and imagery intelligence, early warning, tracking, navigation, and weather forecasting".[1] Key to ensuring these capabilities are available to commanders when and where needed is how the command and control (C2) of Space is accomplished. In this article I will describe Space C2 needs and a way ahead regarding Air and Space C2 integration.

The Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC) is chartered to integrate AF C2 and intelligence, surveillance, and reconnaissance capabilities in support of warfighters. Many of the benefits of dedicating an organization to this mission are now coming to fruition. The Air and Space Operations Center (AOC) now has a defined baseline and configuration control, and five Falconer AOCs will be baselined this year. The Distributed Common Ground Station (DCGS) is currently undergoing testing and DCGS sites will begin receiving a common intelligence exploitation and distribution baseline later this year. Tremendous progress has been made in getting our various platforms on a common data link path and ensuring this real-time information is available to support C2 decisions in a timely manner. While significant progress has been made, there is plenty of work remaining. As the AFC2ISRC shifts gears to increase attention on AOCs aligned to specific functions (i.e., AFTRANS, AFSOF, and AFSTRAT – to include Joint Space Operations Center [JSpOC]), lessons learned associated with integrating the AOC, DCGS, and Tactical Datalinks will be applied to the functional domains. Space C2 will be a key focus as the AFC2ISRC builds on several previous and current efforts.

The AOC, DCGS, and Datalink successes mentioned above were not done to the exclusion of Space C2. In the first Expeditionary Force Experiment (EFX 98), the Air Force experimented with Space Support Teams in the CAOC. This led to increased Space support (i.e., Director of Space Forces [DIRSPACEFOR]) during Operations ALLIED FORCE, ENDURING FREEDOM, and IRAQI FREEDOM.

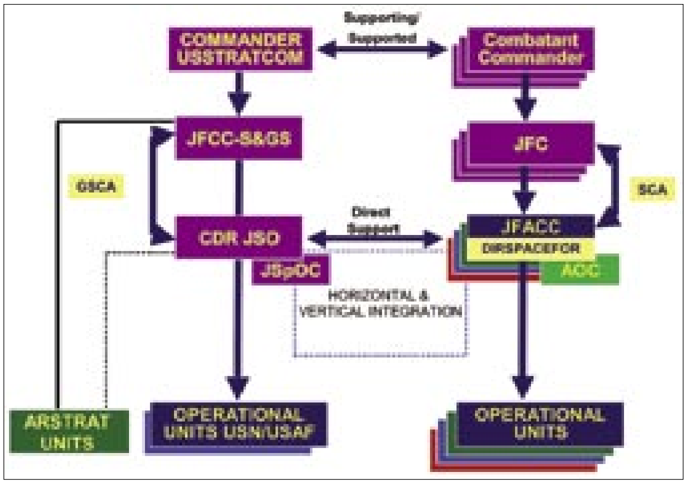
During Joint Expeditionary Force Experiment 2004 (JEFX 04), Air Force Space Command (AFSPC) sponsored two key initiatives, SATCOM Interference Response System (SIRS) and the Initial Single Integrated Space Picture (ISISP). SIRS is a readily deployable defensive counterspace capability providing rapid detection, characterization, and geolocation of SATCOM interference. In short, SIRS-generated data supports Time Critical Targeting processes for engagement of hostile jammers. The AFC2ISRC advocated proving JEFX transition dollars to SIRS and it is undergoing transition right now.

The ISISP initiative was designed to enhance Space Situation Awareness (SSA) and improve the ability of operators to collaborate across the air and space domains. The increased collaboration helps optimize space capabilities and effects, thus improving space support to warfighting commanders. Numerous lessons were learned from the JEFX 04 initiative and are helping to improve SSA and the C2 of global and theater space assets. The full SISP capability is envisioned to provide planning and execution visibility of military, national, civil, and commercial space assets in support of combatant commanders. This single coherent view of all space forces capabilities, threats, and effects will be a tremendous enabler for future operations as Space is further integrated into operations interdependent with other forces—air, land, and sea.

There are certainly Air and Space C2 similarities, but there is also critical domain specific capabilities requiring attention to detail as Air and Space C2 capabilities are integrated. Air C2 is typically accomplished in a specific theater, or area of responsibility, such as Central Command (CENTCOM), European Command (EUCOM), Pacific Command (PACOM). This is accomplished by the Coalition/Joint Force Air Component Commander (C/JFACC). As the world changes and the military is increasingly called upon to support global operations, a regional AOC must not only have the ability to command and control air operations within their theater, but also to collaborate and coordinate with organizations external to their theater. Thus all AOCs will require the ability to plan, coordinate, integrate, and direct execution in coordination with other command centers worldwide.

Unlike Air C2, Space C2 is conducted on a global scale via distributed operations centers. It is based on theater commander and national needs. The main hub of activity for accomplishing this is the JSpOC. On behalf of US Strategic Command (USSTRATCOM), the JSpOC provides all combatant commands (COCOMs) with Space support. In addition, the JSpOC is a key element of USSTRATCOM's Joint Functional Component Command Space and Global Strike (JFCC SGS). In this role, JSpOC collaborates with AFSTRAT in supporting JFCC SGS shared SSA, operational planning efforts and course of action development. The Commander, Joint Space Operations (CDR JSO) has responsibility for Global Space Coordination Authority (SCA) and works with theater SCAs on behalf of Commander, USSTRATCOM (CDRUSSTRATCOM) and Commander, JFCC SGS (CDR JFCC SGS).[2] Regardless of supporting/supported and Operational Control/Tactical Control relationships, the goal is to enable integrated planning, direction, control, execution, and assessment of global and theater space operations. The supported/supporting relationships are depicted in figure 1.

With the above basic understanding, I would like to cover a few key information exchanges between Air and Space. These



Lt Gen Michael A. Hamel, JSpOC Briefing, 1 Mar 05

Figure 1. Space Supporting/Supported Relationships.

are areas the AFC2ISRC has started analyzing for increased Air and Space C2 collaboration, automation and/or machine-to-machine interfaces.

The JSpOC processes and organization construct is modeled after Falconer AOCs. At the top-level, this consists of four divisions—Strategy, Combat Plans, Combat Operations, and ISR. In producing the Space Tasking Order (S-T-O), the JSpOC is seeking to institutionalize a disciplined, yet flexible and timely, planning and execution cycle similar to what is used in production of the Air Tasking Order (ATO). With these similarities in mind, here are key Air and Space C2 information exchanges.[3] These exchanges are listed in their "as-is" state—primarily sequential in nature and lacking automation. I believe they are prime candidates for increased collaboration and/or integration.

- AOC providing the Air Operations Directive to JSpOC
- JSpOC providing Target Nomination List to AOC
- AOC providing the Joint Integrated Prioritized Target List to JSpOC
- JSpOC providing Master Air & Space Attack Plan (MAAP) input to AOC
- AOC providing MAAP to JSpOC
- AOC providing ATO to JSpOC
- JSpOC providing S-T-O to AOC
- Units providing reports to both AOC and JSpOC in support of a Combined Assessment Report

The idea behind this increased, distributed collaboration and coordination is reducing the number of handoffs and serial processes where possible, thus reducing the time to produce a synchronized S-T-O and ATO while increasing operational effectiveness. In addition, moving to a service oriented architecture to support increased data availability and discovery will provide a framework for making information available in a timely manner.

One piece of good news is that many of the systems used in ATO and S-T-O production today are the same. The below list are systems currently common to both the AOC and JSpOC baselines.[4]

- Global Command and Control System (GCCS)
- GPS Interference & Navigation Tool (GIANT)
- Information Warfare Planning Capability (IWPC)
- Space Battle Management Core System (SBMCS)
- Integrated Broadcast System (IBS)
- Satellite Interference Response System (SIRS)
- InfoWorkSpace (IWS)
- Multimedia Message Manager (M3)
- Theater Battle Management Core System (TBMCS)
- Generic Area Limitation Environment (GALE)
- Joint Deployable Intelligence Support System (JDISS)
- Target Prioritization Tool (TPT)
- Defense Collaboration Tool Suite (DCTS)

Leveraging this commonality provides a great baseline in providing commanders and users at all echelons an Air and Space C2 tailorable picture (i.e., User Defined Operational Picture [UDOP]). I will cover this in more detail later in this article, but first I would like to discuss some specific Space C2 needs.

At a general level, command and control of space forces requires the ability to plan, task, direct, and integrate assigned forces—not unlike air C2. AFSPC has created the following Operational View—1 (OV-1) as macro view of how the various pieces fit together to accomplish this. These complementary capabilities include: (a) Space Superiority, (b) Global Information Services, (c) Global Surveillance, Tracking, and Targeting, and (d) Assured Access.

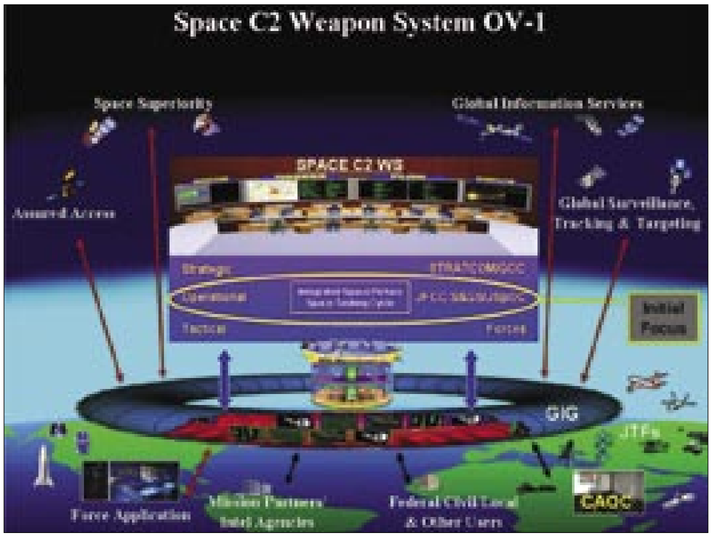

Space C2 Weapon System OV-1
Space Superiority
Global Information Services
SPACE C2 WS
Assured Access
Global Surveillance, Tracking & Targeting
Strategic
STRATCOM/GCC
Operational
JFCC-S&GS/JSpOC
Tactical
Forces
Initial Focus
GIG
JTFs
Force Application
Mission Partners Intel Agencies
Federal Civil Local & Other Users
CAOC

Figure 2. Space C2 OV-1.

Space Superiority includes SSA, Defensive Counterspace, and Offensive Counterspace. As defined by JP 1-02, Space Superiority seeks to achieve a degree of dominance in space that permits the conduct of space operations at a given time and place without prohibitive interference by the opposing force. General capabilities include detect, monitor, track, exploit, protect, deny, assess, and respond. Space Superiority is ongoing, with heightened readiness and operations as required. The information is a key input to the S-T-O process and the desired Space C2 UDOP.

Global Information Services consist of the ability to command, operate, observe, gather, move, and link data and information. Key systems enabling these capabilities include

MILSATCOM, Navigation/Timing, Broadcast, Weather, and Blue Force Tracking.

Global surveillance, targeting, and tracking is basically find, fix, track, target, and assess. Contributing systems include space based infrared radar, nuclear detonation, and others.

Assured Access & Operations includes the ability to launch, operate, maneuver, and control launch systems and Air Force Satellite Control Network provide key contributions to these capabilities.[5]

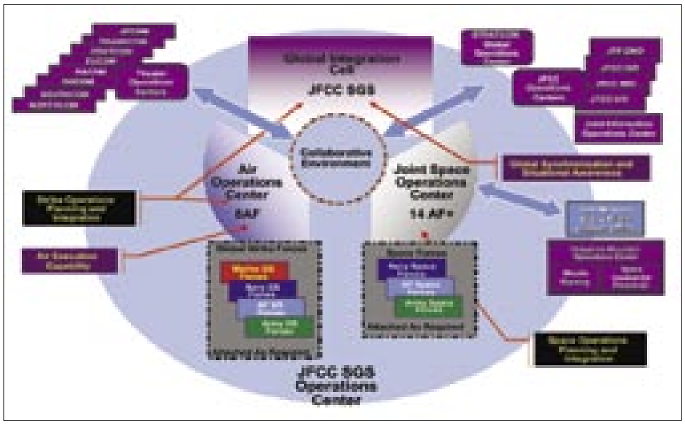
The above information should come together in an integrated Air and Space UDOP. Possible space-related information for inclusion includes the health and status of the space constellation and systems, maintenance and launch schedules, capability prediction by time and/or region, in-space events such as conjunctions, New Foreign Launches, maneuvers, re-entries, and feedback and assessment related information to support the Commanders intent and COA development.

As people and processes are energized to deliver the above capabilities, the use of a service oriented approach seems likely and will ensure consistency with other domains. This entails defining and implementing common Space C2 Services supporting system effects, counterspace tasking, collision avoidance maneuvers, maintenance schedule direction, and Space Control Center priorities. In response to the need for Air and Space integration, the AFC2ISRC has started several space-related initiatives to provide enhanced air and space collaboration capabilities. The Space Battlelab (Lead) and C2 Battlelab have teamed to integrate Geo-Positioning System (GPS) Interference and Navigation Tool (GIANT) and SCOPES with Theater Battle Operations Net-centric Environment. GIANT will provide navigational accuracy and SCOPES will provide red, blue, and grey overhead information to air planners. The machine-to-machine integration will further reduce the targeting timeline (i.e., time-sensitive target kill chain) and allow for increased efficiency of air tasking. The initiative is being demonstrated in JEFX 06 and AFC2ISRC has received outstanding feedback from JEFX 06 Spiral 2 in mid-January.

In addition to the C2 and Space Battlelab efforts mentioned above, the AF is focusing JEFX 08 on Joint Command Control in support SGS. There are six JEFX 08 focus areas:

1. Joint Functional Component Command – Space & Global Strike (JFCC SGS)
2. Joint Functional Component Command – Intelligence, Surveillance, and Reconnaissance (JFCC ISR)
3. Global Force Management
4. Networked Warfighting Headquarters (WFHQs)
5. Integrated Air, Ground, Space Network
6. Unit-level Integration

These focus areas provide significant integration and interdependency challenges, especially regarding Air and Space integration. As part of the JFCC SGS focus area, JEFX participants will mature and test the collaborative processes and tools required for JFCC SGS to accomplish their mission. Contributing to this is the Networked WFHQs focus area where AFSTRAT, JSpOC, and USSTRATCOM's Global Integration Cell will be connected to provide a single, virtual operations center capability. An additional focus area will look at the definition and standardization of a Space Friendly Order of Battle, and this should be part of the Global Force Management focus area.


Global Integration Cell
JFCC SGS
Collaborative Environment
Air Operations Center
8AF
Joint Space Operations Center
14 AF
JFCC SGS Operations Center

USSTRATCOM JFCC SGS CONOPS (Draft), 3 May 05

Figure 3. JFCC SGS Concept of Operations.

Work has begun with USSTRATCOM, AFSPC, ACC, AFSTRAT, JSpOC, and others in ensuring space is fully represented and integrated in JEFX 08. While the details of each of the focus areas are a work in progress, space integration will occur on a scale far beyond any of our previous efforts to date.

Due to the risk associated with the large, complex JEFX 08 focus areas—several smaller events prior to JEFX 08 are being planned. One of these is a Global Strike Pilot in direct support of CDR USSTRATCOM. The AFC2ISRC is partnered with ESC in providing USSTRATCOM, AFSTRAT, and JSpOC a truly integrated Air and Space C2 capability.

The Global Strike Pilot will be our initial Limited Objective Experiment (LOE) leading to a fieldable and supportable capability following JEFX 08. This LOE will be our first demonstrate of capabilities in a distributed and interdependent environment. The system information and participants will be geographically distributed and use collaborative tools in working through a Time Sensitive Planning scenario. The Global Strike Pilot and JEFX 08 JFCC SGS focus area are intended to support the following USSTRATCOM goals.[6]

- Further evolve the JFCC SGS processes and requirements
- Streamline and integrate complementing applications.
- Create a common core information framework for the common core C2 processes.
- Allow rapid customization of framework to support specific scenarios.
- Allow distributed participants to assume roles of other participants.

This rapid prototype of net-centric capabilities and services will move Air and Space C2 capabilities toward a more open architecture permitting access to authoritative data and services. It will involve an integration of "best of breed" legacy and current data, applications, and enterprise services through an interoperable portal/portlet architecture.

As part of the LOEs leading up to JEFX 08, the AFC2ISRC will assist in developing activities, systems, services, and data taxonomies in support of USSTRATCOM's Global Operations

Center (GOC). The experiment will demonstrate dynamic Community of Interest (COI) activities and collaboration tools. The AFC2ISRC is currently leading a Time Sensitive Targeting COI effort in support of US Joint Forces Command (USJFCOM) and making progress in integrating key portions of the SSA C2 COI with TBMCS.

The LOEs and JEFX 08 will allow USSTRATCOM to formalize and exercise roles and responsibilities of JFCC SGS, AFSTRAT, JSpOC, and other Operations Centers to provide S&GS effects to Combatant Commanders. The synchronization and integration of AFSTRAT and JSpOC will enable the delivery of S&GS effects to support theater crisis and contingency operations

From a governance perspective, the AFC2ISRC provides critical support to a C2 general officer steering group chaired by AF/XO and SAF/XC. Via this forum, all MAJCOMs and WFHQs participate in defining and implementing future AF C2 capabilities. Space representation and participation will become even more critical to this forum as the focus is expanded to include a more encompassing integrated Air and Space C2 capability. Space is a critical capability the Air Force provides to the fight and must be integrated with our other domains to fully meet the challenges ahead.

In conclusion, as the Air Force moves forward—it must provide commanders and customers at multiple echelons an adaptable, flexible, and responsive C2 capability spanning air and space. It must be horizontally and vertically integrated. This capability must support and enable interdependence with national, coalition, and multi-service stakeholders. The AFC2ISRC is well postured and leaning forward to address key gaps in capabilities. The AFC2ISRC looks forward to working these challenges and delivering an integrated, interdependent Air and Space command and control capability to execute operations in every theater across the globe.

Notes:

[1] Maj Gen John T. "Tom" Sheridan, "Today's National Security Space Acquisition Environment: Learning From the Past - A Path Forward," *High Frontier* 2, no. 2 (2006): 18.

[2] Maj Gen Michael A. Hamel, "Joint Space Operations Center" (briefing, 1 Mar 2005).

[3] ibid.

[4] Lt Col Nevin J. Taylor and Maj Russ Rowland, "AFSTRAT Operations Center Integration" (briefing, 1 November 2005).

[5] Maj Gen Douglas Fraser and Maj Gen Micahel A. Hamel, "Welcome to the Space C2 Focus Day" (briefing, 2005).

[6] Col Mark Lorenz, "GOC Net-centric Initiative" (briefing, 22 November 2005).

Maj Gen Tommy F. Crawford (BA, New Mexico State University, MS, Boston University) is the Commander of the Air Force Command and Control, and Intelligence, Surveillance and Reconnaissance Center, Langley AFB, Virginia. General Crawford is responsible for integrating command and control, and intelligence, surveillance and reconnaissance for the Air Force to reduce duplication of effort, increase commonality and enable the Expeditionary Air Force. He is also the implementing agent for Air Force experimentation. The center comprises 780 people, and defines C2 and ISR requirements and operational concepts, develops open architectures, and manages C2 and ISR systems and budgets. General Crawford was commissioned a second lieutenant through the Air Force ROTC program at New Mexico State University in May 1972. He has staff experience in Air Force plans, special weapons, and as Assistant to the Supreme Allied Commander Europe. The general has served as an instructor pilot, squadron weapons officer, F-111A flight commander, A-7D and F-117A Nighthawk weapons and tactics officer, wing weapons and tactics chief, assistant operations director and major command inspector general. He has commanded at squadron, air operations group and wing levels. General Crawford is a command pilot and DESERT STORM veteran with more than 3,000 hours in fighter aircraft. Prior to assuming his current position, the general served as the Deputy Chief of the Central Security Service, National Security Agency, Fort George G. Meade, Maryland.

Senior Level Perspective

Dominance in Space is Dominance in Command and Control

RDML Gerald R. Beaman, USN
Commander, Naval Network and Space Operations Command
Director of Operations,
Naval Network Warfare Command

What exactly does it mean to a Navy unit when one speaks of Space command and control? One might be tempted to respond to this question by saying that it means navigation, timing, satellite communications, email, web services, imagery, targeting information, battlespace awareness, coordination, information, shared data, and business processes that travel via our satellite links to and from our Navy ships at sea. But I submit that the response is much simpler. In my mind, it is not the question, "What is Space command and control?" but rather a statement that "Dominance in Space is dominance in command and control."

It was not all that long ago when warships went to sea and it might be years, months, or weeks before word sent from them could reach a headquarters. While this operational environment built within the Navy service gave us a laudable sense of independence and provided us the ability to function without links to home, it also made it very difficult to quickly respond to changing events, and it made it nearly impossible to command or control any forces outside visual range. While the introduction of radio communications made things better, the low bandwidth communications did not support anything but the simplest of forms of communications and even those were encumbered by a slow, difficult, and error prone process. Furthermore, when a ship initiated the communication with these omni directional devices, the mere act of doing so then entailed a risk of detection that was often not operationally acceptable. Given these limitations, one can only wonder how many opportunities to inflict damage upon our enemies were missed as a result. Practically speaking, it was not until the advent of satellite communications that we could even hope to network our maritime units in a manner that allowed us to use them to their fullest potential. With space based assets providing communications and other links to the headquarters, we could finally command and control our forces, in near real time, anywhere on the globe.

US Navy

Without the navigation, timing, satellite communications, email, web services, imagery, targeting information, battlespace awareness, collaborative target development, coordination, information, shared data, and business processes available via our links to our sea going forces, what sort of command and control is possible without assets in orbit? Not much! I doubt that any Navy Commander, nor for that matter a Commander from any service, would relish armed conflict without the secure, robust, and high bandwidth links provided by our space assets. For without them, it is impossible to deliver the world the voice, video, and data in the immense quantities necessary to be successful on the modern battlefield. In fact, our fundamental awareness of the battlespace depends upon the information we get from or via our space command and control assets. Consider for example the current operations in Iraq and Afghanistan. Just a few short years ago, the thought of remotely piloted vehicles launching armed strikes against targets thousands of miles away was not much more than a dream; yet today it is common. Consider that just a few short years ago we transported air tasking orders in hardcopy format from the ground headquarters out to the carriers, and today they travel effortlessly and reliably via pure electronic means. Consider that just a few short years ago, we coordinated real time movements and retargeting of assets with voice communications over secure circuits, today we do it much more quickly in collaborative workspaces and chat rooms, all while watching a real time video feed from an unmanned aerial vehicle half a world away. It is these tools that enable the command and control of units on the modern battlefield, and Navy units are as dependent upon them as is everyone else. The command and control made possible by our space assets enables our netted Naval forces to bring combat power to bear with speed and agility unmatched by our rivals and unheard of just a few short years ago. However, with these capabilities come a number of challenges that we in the Navy, along with the other services, must resolve. Foremost among them are the challenges of interoperability, demand, and security.

If we are to achieve the goals of FORCENet and of the larger network-centric operations concept, then we must ensure that all of our space command and control capability is seamlessly integrated with the systems of the several services. Products, services, and command and control information must quickly and seamlessly traverse the Global Information Grid (GIG),

US Navy

including those orbital assets, so that all the users on the network have access to the right information at the right time. We must be able, depending upon the situation, to extend all or part of this command and control information to other Federal agencies, state and local authorities, and even to coalition partners and allies. The lessons of Hurricanes Katrina and Rita, and our operations in the Global War on Terror serve as stark reminders that this information sharing is essential in any number of unforeseen circumstances.

Secondly, the demands we place on these systems are immense…and growing rapidly. Real time streaming video, high resolution photography, video teleconferencing, and high bandwidth collection devices put immense pressure on us to expand the amount of available bandwidth. Certainly, we must make every effort to increase our bandwidth wherever possible, but we cannot do so forever. The simple reality is that there is not an unlimited source of funds to purchase more bandwidth any more than there is an unlimited amount of bandwidth available for purchase. Therefore, it is important that we start looking at ways to limit our appetite or, at a minimum, to conserve where possible so that we can shallow the slope of the ever growing demand curve. I suspect we are our own worst enemy; one only need look in their respective inbox to see room for improvement. How many multi-megabyte presentations are needlessly copied to large groups of users? How many web pages are needlessly complex or filled with bandwidth draining images or graphics that are necessary to the mission? In each of these examples, we expend precious bandwidth and burden our command and control network. Is this really necessary? Disciplined use of bandwidth and greater emphasis on collaborative workspaces stand to reduce this burden on the system and yet still permit everyone who truly needs that ten megabyte presentation to still have a copy, yet at the same time not using up ten megabyte chunks of bandwidth to send it to those who do not need it. Consider for a moment how much savings one might harvest across the entire domain on any given day. Even if we save only a few percent, a small percentage of a big number is still a big number. While granted this is just a small portion of the bandwidth demand problem, it is an easy, quick, and logical measure that can perhaps decrease the slope of the demand curve and allow us to recoup bandwidth for use in other areas.

Finally, all of the links must be robust and secure. In many cases, the information that passes among our space command and control assets is some of the most sensitive information our government possesses. In other cases, the information could be the complete picture of force disposition, supply status, or movement information, any part of which would be invaluable in the hands of an opponent. Or, the information would be business information, though not classified, but still critical to the day-to-day functioning of our force. Lastly, the information is of a personal or financial nature, and our soldiers, sailors, Airmen, Marines, coast guardsmen, civilians, and contractors could be individually or as a group subject to hardship, embarrassment, or criminal acts if the data is not protected. In short, what we see is that regardless of the nature of the data that travels on our space command and control links, we must ensure that it is zealously protected. We cannot let our guard down in this domain; any cyber warrior will tell you that our GIG, and therefore our key command and control links, are under attack each and every day. In cyberspace, we are always at war, and we must defend accordingly. If we do not do so effectively, then an enemy could interrupt our command and control, force our forces to operate independently, and therefore take from us our greatest advantage…that of our ability to act in a coordinated fashion, anywhere on the globe.

While the challenges detailed above are shared largely by all services, there are some challenges to effective space command and control that are in many ways unique to the Navy operating environment. There are two that I believe best illustrate challenges facing Navy space command and control on a daily basis.

As we have discussed, Navy forces operate on the world's oceans, sometimes far from other forces. This means that at virtually any spot on the globe, Navy units may be in need of the command and control information that arrives via space assets. However, this is possible only if planners give careful consideration of orbital maintenance and housekeeping periods. It would be very unfortunate to have a Navy ship in need of services during an orbital period when the satellite is unavailable.

Secondly, we in the Navy do not enjoy unlimited space for

US Navy

ground segments onboard our vessels. There just is not the available real estate for multiple large terminals. If you happen to be on a large deck warship, an aircraft carrier, or amphibious ship for example, then life is pretty good relatively speaking. Though not in any way comparable to a shore installation or land base, the fact remains that since the ship is bigger, the superstructure is bigger, and therefore there is a better chance that one can find an acceptable location for the antennas and other necessary gear. However, much of our force: cruisers, destroyers, frigates, and submarines for example, have very limited space on their superstructure for the large terminals necessary to support the bandwidth necessary for some of the advanced capabilities listed above. Yet, if these disadvantaged users are to be an integral part of the larger netted force and linked by space command and control assets, we must plan for their limitation with respect to terminal size and bandwidth available. If we believe that our command and control structure is only as good as the weakest link, then it is the disadvantaged users upon whom we must concentrate. This methodology has the added advantage that a command and control solution that works for submarines or any of the other small ships, may well work for our SPECOPS forces, for those forces also often find themselves pulling their data using terminals measured in inches and not feet.

While there are a great many products, services, and capabilities provided by individual space assets, it is the sum of their contributions and their place in the GIG that really defines why they are so critical. For Navy units at sea, operating in remote parts of the globe, Space dominance is Command and Control. Without it, we cease to be parts of the global netted force and are then limited by the horizon and proximity to land. To preserve and expand our capabilities, we must solve the challenges mentioned earlier. Our battlespace awareness, our targeting information, our communications, our business process, and even the morale of our soldiers, sailors, Airmen, Marines, coast guardsmen, civilians, and contractors depend upon our space assets. In times of national crisis, others depend upon them as well…many without ever even knowing it. In the face of rapidly changing global threats, elusive enemies, and an uncertain future, it is only the space command and control that gives the agility and real time command and control necessary to meet those threats head on and defeat them.

RDML Gerald R. Beaman (BA Business Administration, Marquette University; MA in National Security and Strategic Studies, US Naval War College) is Commander, Naval Network and Space Operations Command and also serves as the Director of Global Operations for Naval Network Warfare Command. RDML Beaman is responsible for the day to day operation and defense of Navy Networks, telecommunications, and space segments through a 4,000 person global organization. The Admiral has commanded VF-211, an F-14 squadron; served at USSPACECOM as Chief, Global Engagement Division; commanded Carrier Air Wing TWO, and served as a Chief of Naval Operations Strategic Studies Group (SSG) Fellow for SSG XXI in Newport, Rhode Island. Prior to being named as Commander, Naval Network and Space Operations Command, he served as Chief of Staff for Commander Naval Air Forces. Along with tours at VF-33, VF-101, and the Naval Fighter Weapons School, he also served as a Special Agent with the Federal Bureau of Investigation, as Flag Lieutenant and Aide to the Commander Operational Test and Evaluation Force, and as Officer in Charge of the Naval Fighter Weapons School detachment in Riyadh, Saudi Arabia during Operation DESERT STORM. The Admiral was commissioned through the Naval Reserve Officer Training Program and designated a Naval Flight Officer in April 1975. He has over 3,300 flight hours in tactical aircraft and 1,050 carrier landings.

The Space C2 Weapon System A Weapon System Approach for the Command and Control of Space Forces

Brig Gen Elaine L. Knight, USAF
Deputy Director of Air and Space Operations
HQ AFSPC

Day in and day out, our space forces contribute to every military mission around the globe. More importantly, the impact of space on all operations and activities—military and commercial—is steadily growing. Space is the largest theater of operations today—if not the most important given the dependency of other theaters upon the services and capabilities delivered through space. Thus, we must incorporate the latest in information technology to ensure we harness the vast potential to accomplish our mission. Our space systems are the underpinning enabling warfighters to perform their missions with precision, lethality, and maximum effectiveness. Space-based enhancements include: theater and strategic missile warning, precision navigation, secure and reliable communications, accurate mapping and weather, and timely intelligence.

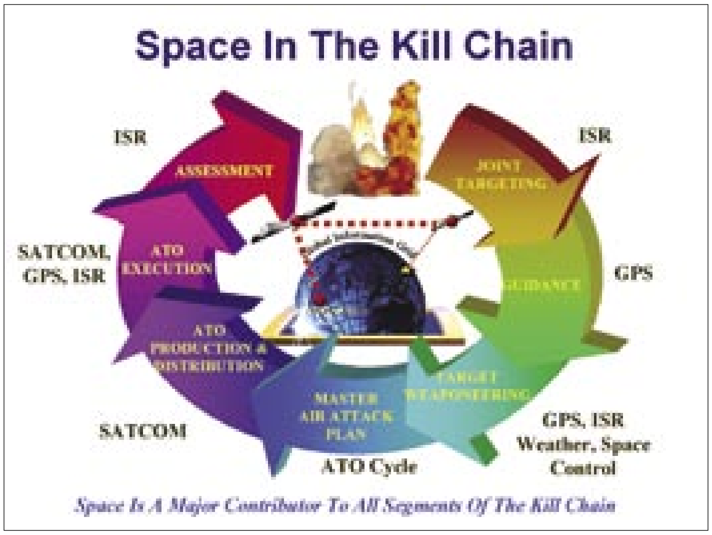


Figure 1. Space In the Kill Chain.

Furthermore, space is an integral part of military planning, execution, and analysis; specifically, space enables effects-based operations by providing warfighters with the information and infrastructure they need to execute the kill chain (figure 1). Given this, Air Force Space Command (AFSPC) is stepping out to address space command and control. This is further reinforced in comments made by General (Ret) Lance W. Lord at the 4 March 2005 Command and Control (C2) Focus Day, "As you know my number one priority is Space Superiority…this cannot be achieved without a robust command and control infrastructure."

Our challenge in creating the new Space Command and Control Weapon System (SpC2WS) is to synchronize critical global and theater space effects to the Combatant Commanders in an effort to satisfy timing and tempo requirements necessary for precise execution of operations. This challenge requires a weapon system that provides in-demand space combat effects for the joint warfighter, assures Space C2 is interoperable with global and theater C2 and synchronizes Space C2 efforts with minimum duplication of effort. Without the advanced development of the SpC2WS, a myriad of mission impacts to the warfighter may occur—a loss of unity of effort at the strategic, operational, and tactical levels; fragmented C2 across disparate systems; manual blue force situation awareness tracking, manual strategy-to-task and Space Tasking Order processes; an inability to correlate space environmental impacts with space system anomalies; and finally the current non-integrated modeling and simulation tools can cause planning and course of action (COA) delays.

The AFSPC response to this challenge is the new Space C2 and Integration Division, HQ AFSPC/A3Z, whose responsibility is to ensure the timely and accurate development of this essential SpC2WS. The division's charter is to establish policy and guidance for the AFSPC family of Space C2 systems, to develop appropriate Concepts of Operations, to fully integrate space capabilities for the warfighter, and to advocate requirements to effectively command and control space forces in support of global and theater Combatant Commanders. The Space C2 and Integration Division will provide centralized advocacy, oversight of the acquisition process and one-stop-shopping in HQ AFSPC for Space C2 by developing and maintaining a big

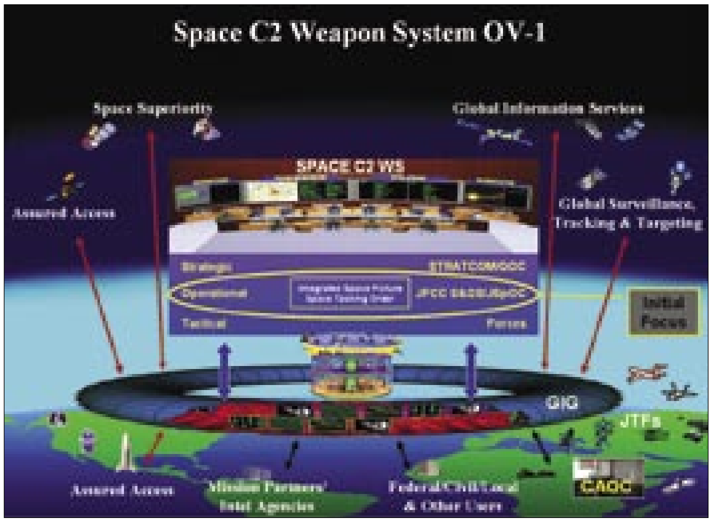

Space C2 Weapon System OV-1
Space Superiority
Global Information Services
SPACE C2 WS
Assured Access
Global Surveillance, Tracking & Targeting
Strategic
STRATCOM/GOC
Operational
JFCC SB/JSpOC
Tactical
Forces
Initial Focus
GIG
JTFs
Assured Access
Mission Partners/ Intel Agencies
Federal/Civil/Local & Other Users
CAOC

Figure 2. Space C2 Weapon System Operational View-1.

picture perspective. Additionally, the division will enforce standardized C2 interfaces across space Weapon Systems and integrate space capabilities and effects to significantly improve warfighter capabilities and effects based operations.

The SpC2WS (figure 2) will enable, integrate and secure Space Superiority, Assured Access, Global Surveillance, Targeting, and Tracking, and Global Information Services (GIS). Initial efforts from GIS include a Space C2 User Defined Operational Picture (UDOP) exposing constellation system health and status, maintenance and launch schedules, capability predictions by time and region, in-space events (conjunctions, new foreign launches, maneuvers, re-entries, etc.), and finally feedback and assessments such as Courses of Action and Commander's intent. The Space C2 services under development to advance space superiority include system effects, counterspace taskings, collision avoidance maneuvers, maintenance schedule direction, and Space Control Center priorities.

The endstate of a comprehensive Net-Centric SpC2WS will be achieved incrementally, transitioning from the currently employed Space Battle Management Core System (SBMCS), to the next generation (Single Integrated Space Picture [SISP]), to a more capable SpC2WS Increment 10 and finally to the fully automated, robust SpC2WS Increment 20 (figure 3). The SpC2WS Increment 20 will be built on a Net-centric Service Oriented Architecture affording multiple UDOPs, expanded space data access, fully capable Integrated Space Picture, Space Tasking Order automation/optimization and a robust Strategy-to-Task tool. The SpC2WS with be fully interoperable with the Falconer Air Operations Group (AOC).

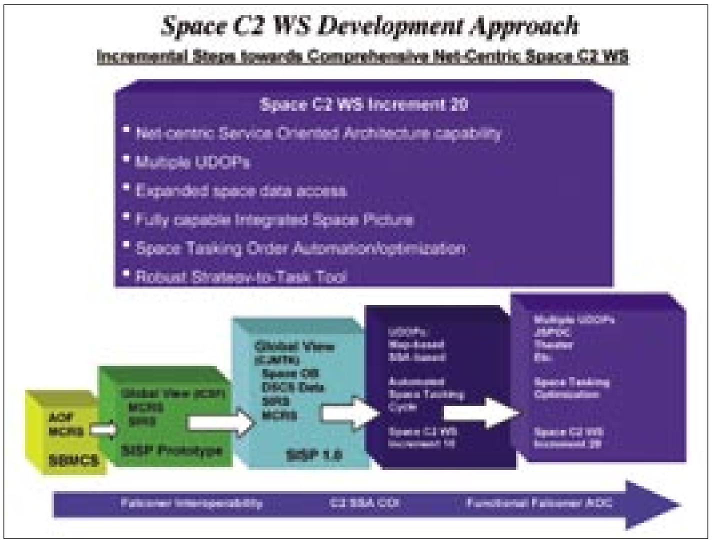


Figure 3. Space C2 Weapon System Development Approach.

The Air Force is in dire need of the ability to synchronize delivery of space effects to Global and Theater warfighters, to the timing and tempo of their operations, and to responsively assess and optimize these capabilities for National Security Space. The SpC2WS brings space C2 into the "net-centric operations and warfare" enabling shortened planning cycles and supporting new, unanticipated users. Furthermore, it provides an integrated roadmap for synchronization of timing/tempo/effects enabling Space to exponentially improve how it supports theater; and creates and shares a worldwide space situational picture to ultimately benefit not only Department of Defense users, but will also be available to our civilian and commercial partners.

Brig Gen Elaine L. Knight (BA, Psychology, University of Nebraska; MS, Logistics Management, Air Force Institute of Technology, Ohio) is the mobilization assistant to the Director of Air and Space Operations, HQ AFSPC, Peterson AFB, Colorado, and is currently serving as the Deputy Director of Air, Space and Information Operations, HQ AFSPC Peterson AFB, Colorado. The directorate is responsible for organizing, training, and equipping all Air Force space and missile operations. The mission area includes missile warning, nuclear event detection, space control, ICBM, spacelift and range operations, satellite command and control, aerospace weather, helicopter and airfield operations, and command and control. The directorate integrates space capabilities into the operational level of war and develops space exploitation and ICBM employment concepts.

As an enlisted member, she served as a communications center specialist and an Air Force recruiter. Following her commissioning, she held positions in munitions maintenance and acquisition logistics before leaving active duty, joining the Air Force Reserve individual mobilization augmentee program, and transitioning into space operations. General Knight has served in staff positions at Headquarters United States Air Force, Headquarters Air Force Space Command, and the Space Warfare Center.

General Knight is also a graduate of Air War College, a distinguished graduate of Squadron Officer School, and top third graduate of Air Command and Staff College.

A Legacy of Support to the Warfighter

Mr. Shephard W. Hill
Senior Vice President, Business Development & Strategy
The Boeing Company

On 20 June 2005, we lost a great visionary when General Bernard A. Schriever passed away. During the 1950s, General Schriever initiated forward-looking discussions regarding the attributes of space capabilities—no one wanted to hear it, or talk about it. He was essentially censored. Then on 4 October 1957 the Soviet Union launched Sputnik into Earth orbit. As the significance of the event settled into the mindset of Americans, the US military and Congress wanted to hear all they could from General Schriever.[1]

Clearly, General Schriever was a futurist who ushered in the development of the systems needed to provide nuclear deterrence during the Cold War. As director of the *Project Forecast* study in 1963, he postulated a comprehensive long-range assessment of military science and technology. A vision emerged that peered into the realm of space as a medium that would play a major role in securing America's national security—today, we continue to see that vision coming into focus.

Since General Schriever's time, space support to the warfighter has steadily grown, and we in Boeing are very proud to be a part of this exciting journey. We were there at the beginning as well. In 1963, it was the Hughes Aircraft Company (now Boeing) that developed Syncom 1, the first geosynchronous earth orbit (GEO) communications satellite. Dr. Harold Rosen and his team, keying off of the impetus created by the launch of Sputnik, envisioned that an object placed over the equator at a height of 22,238 miles and at a speed of 6,878 mph would match the rotation of the earth and become "geostationary." We have covered a lot of ground since then, with satellites providing weather data for US military operations, as well as intelligence, situation awareness, communications, and precision navigation. In the next paragraphs I want to bring you up to date on what we are doing in several of these critical areas and discuss some of the challenging and literally magical things that lie ahead.

Communications Support to the Warfighter

In 1991, during Operation DESERT STORM, military operations relied on commercial satellite communications (SATCOM) for 45 percent of communications between the theater and the continental US. For Operation IRAQI FREEDOM and ongoing operations, this figure jumped to 80 percent.[2] DESERT STORM's total data rate required was 100 megabytes per second (Mbps) for a combined force of 500,000 troops. For Operation ALLIED FORCE, SATCOM bandwidth rose to 250 Mbps for far fewer troops, and in Operation ENDURING FREEDOM a total data rate of 700 Mbps supported a force of only 50,000 troops—one-tenth the number of people engaged in DESERT STORM.[3] Over the last 15 years, we have witnessed the continued expansion of bandwidth demand even as the number of warfighters being employed has decreased. This is because warfighters have been able to collaborate more and benefit from better situation awareness. They now operate more effectively using a common operating picture. I think that Admiral Edmund P. Giambastiani, Jr., the Vice Chairman of the Joint Chiefs of Staff, captured the essence of why this is happening while serving as the Commander of Joint Forces Command. He said, "We had over 40 times the bandwidth capability of Desert Storm (in Operation IRAQI FREEDOM), which allowed our forces to range more rapidly over the whole of Iraq in order to achieve a far more complex mission: defeat and regime change."[4]

This trend is sure to continue as jointness and close collaboration among US and coalition forces continues to grow as a strategic necessity and advantage. The Defense Satellite Communications System (DSCS) constellation that currently supports our warfighters is a super-high frequency, high priority command and control (C2) communications constellation consisting of five operational and four residual satellites in GEO. The final modernized DSCS III was launched in August 2003. The DSCS system has performed well, and the satellites are

Erik Simonsen

Global strike force utilizing GPS-guided JDAMs.

operating longer than their 10-year design life, allowing additional time to deploy new, more capable systems into their orbit slots.

The next generation system, Wideband Gapfiller Satellite (WGS), is a high-capacity satellite communications system designed to support the warfighter with new technology and far greater capabilities. The Boeing Company was selected as the prime contractor for the WGS. When deployed, the system will provide a quantum leap in communications bandwidth to our soldiers, sailors, Airmen, and Marines. For example, one WGS satellite will provide more than 2.1 gigabytes per second (Gbps) of communications capacity—more than the entire existing DSCS constellation. WGS will also provide a substantial augmentation to the Ka-band Global Broadcast mission that is currently provided by Ultra High Frequency Follow-On satellites. This includes two-way, point-to-point, multicast and broadcast communications that will potentially support initial Communications on the Move (COTM) for troops in the field. Commanders have emphasized that COTM is absolutely necessary to the warfighter of the future—without it the warfighter is increasingly vulnerable.

Boeing is under contract with the Space and Missile Systems Center (SMC) for three WGS satellites, plus associated ground-based control systems. The satellites are being built at the Boeing Satellite Development Center, with the Air Force planning to procure at least two additional satellites, slated for launch in 2010 and 2011. WGS is based on the proven 702 bus, and has inherent growth capability to support future transformational communications requirements. During late 2005, an initial full-up spacecraft test successfully demonstrated the performance of the unique X-band and Ka-band WGS communications payloads, and the first WGS has undergone preliminary environmental testing. The Air Force is planning for a first launch in June 2007. I believe former Under Secretary of the Air Force Peter B. Teets captured very succinctly the importance of WGS and related communications initiatives when he said, "In the battlespaces of tomorrow, victory may be won or lost in mere seconds – the seconds it takes to identify and strike a moving target, or the seconds it takes to make a critical decision. We cannot let bandwidth constraints be the Achilles heel of our armed forces in the decades to come. That's why our efforts to transform communications are so critical."[5]

Moving Forward – Transformational Satellite Communications Space Segment

Currently operating at medium altitudes over Iraq and Afghanistan are unmanned aerial vehicles (UAV) accomplishing reconnaissance, surveillance, and armed strike missions. Predator UAVs are controlled by pilots in ground cockpits thousands of miles away. Flying autonomously at altitudes above 60,000 feet, the strategic reconnaissance Global Hawk UAV and the manned U-2S aircraft must be able to capture and transmit imagery quickly to the people who need it. Additionally, UAV flight control and platform imagery generation require high-bandwidth for uplink/downlink and processing.

Boeing

Wideband Gapfiller Satellite.

In tomorrow's battlespace, UAVs and manned platforms will share bandwidth with new-generation Joint Unmanned Combat Air Systems air vehicles flying autonomous reconnaissance, surveillance, and attack missions. Future Combat System brigade combat teams will be equipped with hundreds of UAVs to support tactical-level needs for reconnaissance, surveillance, and communications relay. Needless to say, these continuing developments will place ever-increasing pressure on satellite communications systems as tomorrow's commanders demand more and more bandwidth and connectivity.

To meet this growing need, the Air Force has initiated the Transformational Satellite (TSAT) program. Designed to finally remove communications bandwidth as a constraint to the warfighter, TSAT will provide survivable and protected high capacity internet-like connectivity. This is an extremely capable system providing throughput solutions, and contractors are testing data up to 40 Gbps; however, the requirement is 20 Gbps. That translates into having the ability to process a reconnaissance photo in less than a second, and transmit it instantly. For example, the current Milstar Block II's processing of imagery or data can take up to two minutes—reducing that critical time down to less than a second is a highly desired capability.

"No other space asset being developed even comes close to meeting future bandwidth availability requirements. Everyone thought GPS was a game changer – TSAT is revolutionary."[6]

- John T. Fuller, Vice President,
Boeing Integrated Defense Systems

The Boeing TSAT SS team is one of two contractor teams working under a risk reduction and system definition study contract. This phase continues through 2007, followed by the government selecting a single contractor to proceed with the acquisition and operation phase. Mission success and investing heavily upfront in risk reduction remain top priorities for the Boeing team.

Supported by a small constellation in GEO, TSAT will provide the backbone of the DoD's high-bandwidth networked communications, as well as supporting full-up COTM and protected strategic communications. TSAT will also incorporate secure and protected laser communications (lasercom) for crosslink. It is also the only SATCOM system on the horizon that will establish critical links to airborne intelligence, surveillance, and reconnaissance platforms and double the throughput that a Global Hawk-type UAV requires.

Additionally, this transformational leap will give commanders in the field the ability to react and initiate action more quickly than ever—tactically, before an adversary even has time to conceptualize their next move. With this capability in place, conflicts could be substantially shortened, or even prevented. With TSAT deployed, we will have a space-based network communications link that was designed specifically to realize the full impact and transformational nature of DoD's network-centric warfare vision. Although dependent on funding decisions, the first TSAT launch is currently planned for the middle of the next decade.

Fighter pilots are often quoted that "speed is life." In essence, speed plus bandwidth availability equates with survival in modern network-centric warfare. Steps being initiated today with the WGS and the TSAT program will substantially upgrade military SATCOM, ensuring that warfighters have the information and collaborative capabilities they need to prevail in any situation.

Providing Global Access to Imagery

Boeing's leadership in the development of the Future Imagery Architecture (FIA) for the National Reconnaissance Office, ensures that warfighters and other elements of the national security community will have access to critical imagery for a broad range of applications. When combined with strong emphasis on efforts to create a seamless flow of information where and when it is needed through network-centric capabilities, FIA will enable the seamless transfer of the right information to the right users at the right time to enable responsive and decisive action on the battlefield.

Looking to the future, we see that the need to provide worldwide, on demand, near continuous surveillance and reconnaissance for battlespace characterization is growing. Combatant commanders have a pressing need for responsive multi-theater capability to detect, geo-locate, identify, and track surface objects regardless of motion, location, or environmental conditions.

"At S&IS, we are in the business of collecting data, processing data, and distributing data over different platforms. We enable NCO through our advanced satellite technologies and our imagery and data capabilities." - Howard E. Chambers,
Vice President and General Manager,
Boeing Space & Intelligence Systems

As a result of this requirement, in 2001 the Secretary of Defense established the Space Radar program with the purpose to develop and implement a space-based capability to provide surface moving target indications, synthetic aperture radar imaging and high resolution terrain information mapping that can be made available to national decision makers and joint/coalition forces worldwide.

Achieving this objective will substantially enhance US information dominance in support of both early warning and military operations. The focus will be on maturing technology and developing an ISR system that incorporates battlefield tasking, and control of the system to facilitate near real-time Space Radar availability. The Space Radar system will give military forces the ability to look deep into denied areas without risk to people or resources.

The Boeing team looks forward to working with the Air Force and the Space Radar Joint Program Office as this exciting new capability is developed and fielded early in the next decade.

The Role of GPS

On 22 February 1978, an Atlas F rocket at Vandenberg AFB, California, carried the first 982 lb. (final on-orbit weight) Navstar 1 into orbit. At the time, not many people in the military or aerospace industry thought that a single space program would become such an integral part of military operations and the civilian economy. With varying degrees of accuracy, the US military, allies, and civilian users worldwide are able to acquire precise navigation and timing data.

Declared fully operational by the Air Force in 1995, the Global Positioning System (GPS) constellation is controlled and maintained 24/7 by the Air Force 50th Space Wing's 2nd Space Operations Squadron at Schriever AFB, Colorado. The Control Segment contacts each GPS satellite at least once per day to upload the latest navigational data. GPS satellites travel in circular mid-Earth orbit at 10,900 nautical miles altitude, in six orbital planes at 55 degrees inclination. The operational GPS constellation has 24 defined orbital slots. As of 28 February 2006, there are 29 satellites in the constellation. Each satellite orbits the Earth every 12 hours, compared to approximately 90 minutes for low Earth orbit. The number of satellites and their slow transit time allows worldwide users to acquire a minimum

Erik Simonsen

Global Positioning System IIF.

of four satellites above the horizon to yield a three-dimensional position fix.

Since its inception (Air Force contract in 1974), Boeing (then Rockwell International) has been heavily involved in satellite production and control segment development. Over the duration of the program, Boeing has built 40 Block I, II and IIA satellites. Two Block IIs have recently surpassed 15 years on orbit—exceeding twice their design life.

Currently, the Lockheed Martin Block IIR-M satellites are being launched to replenish the GPS constellation, and beginning in 2008 the Boeing Block IIFs will be delivered to the Air Force. Block IIF will provide increased accuracy, anti-jamming, a secure military code and a third civilian signal called L5. Boeing is currently under SMC contract for nine Block IIFs, with a potential for up to 12 satellites. Assembly of the IIF satellites is underway at the Boeing Satellite Development Center.

Today, no other space asset is considered more vital to both the warfighter and civilian users than GPS. For military platforms, GPS is considered an essential part of network-centric operations not only for precise navigation and timing, but for directing ordnance to time-critical targets.

The GPS-guided Joint Direct Attack Munition (JDAM) has set the standard for attacking targets with precision and keeping collateral damage to an absolute minimum. During Operation IRAQI FREEDOM, coalition aircraft dropped over 5,500 GPS-guided JDAMs. Demonstrating time-critical targeting—a loitering B-1B, dubbed 'Roving Linebacker,' provided a glimpse of what will become very routine in a future network-centric warfare environment. Notified of a time-critical target, the crew was able to re-program four of its JDAMs (GBU-31) and receive a go-ahead to the new target within minutes instead of hours. The time for crucial air tasking orders was dramatically reduced with space assets supporting C2. Precision munitions such as the Small Diameter Bomb (SDB) now being developed will be smaller and more accurate. Tactical aircraft and bombers will be able to carry larger numbers of independently targeted SDBs, with the B-1B carrying up to 96.

Taking a forward-looking path that ensures the US will have necessary the tools for the future, SMC is expected to release an RFP for the next-generation GPS Block III in 2006. Contractor teams will participate in a competition to develop and build the next generation GPS Block III spacecraft and ground segment. The first GPS Block III spacecraft is expected to be launched in 2013.

Space Situation Awareness - Protecting our Space Assets

With the great importance of space assets to the warfighter as a primary concern, in January 2001, the Rumsfeld Space Commission voiced great concern regarding the vulnerability of US space-based assets, and that a very real threat to these assets would eventually arise. The warning concluded with the finding that the US was an attractive candidate for a potential "space Pearl Harbor."[7] Commenting during the AFA National Symposium in November 2003, General Lance W. Lord, then Commander of Air Force Space Command (AFSPC), pointed out, "Space is the center of gravity now. We must not let it become a vulnerability. Our future adversaries understand that we have this advantage, and I think they are trying to develop capabilities right now to thwart that." [8]

Erik Simonsen

F-15/ASAT test on 13 September 1985.

Today, AFSPC operates a worldwide Space Surveillance Network tasked to detect, track, identify, and catalog all space objects to ensure space operations are conducted without interference. The AFSPC Space Control Center in Cheyenne Mountain provides warning to US space system operators to protect their satellites from potentially hostile situations or dangerous natural events.

Excellent ground-based space object detection systems are currently in operation and provide the bulk of the deep space object tracking today. However, their contribution is limited by being fixed on Earth and an inability to operate during daylight and adverse weather. These facilities do not have the ability to "timely" detect small objects in deep space, nor the resolution required for detailed observation of objects in GEO. As we approach the next decade, leaving the limitations of Earth and utilizing the flexibility of space is the next logical step.

During a recent interview Maj Gen James Armor, Director, US DoD National Security Space Office, described Space Situation Awareness (SSA) as a critical item. "We are working on an architecture for SSA that is still being generated, but it's a vital part of the national security space policy—ensuring space sovereignty for our systems. We don't know what to do if we don't know what's going on in space, and right now, our capabilities are frankly rudimentary."

He summed up the results of a recent study. "We're coming to the conclusion of our protection strategy. It looks at every aspect of the space system—what's on orbit, the ground systems, the links, command and control, and the mission segments—and looks for vulnerabilities.[9]

Space Based Space Surveillance

Acutely sensitive to the importance of SSA, the Air Force has taken the initiative to enhance our surveillance and situation awareness capabilities in near and deep space. This new effort to detect and track space objects, including space debris, will ensure the US knows what is going on first-hand in this realm.

"If one of our space assets goes offline we need to know the circumstances immediately in order to access the ramifications and take the proper action. Was it a technical anomaly, or did an unknown hostile action cause the malfunction?"

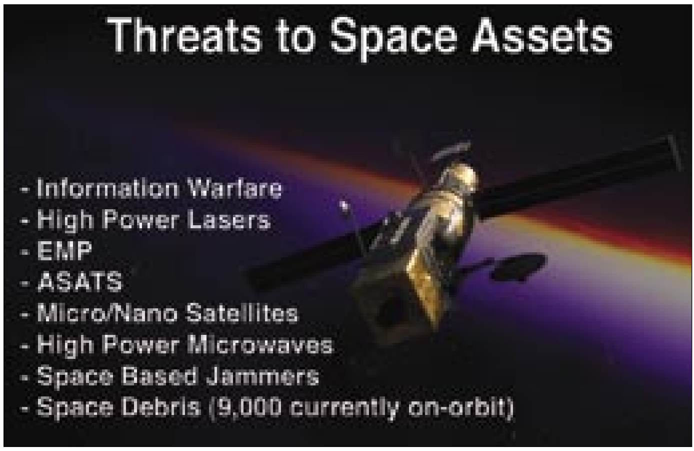
- John T. Fuller, Vice President,
Boeing Integrated Defense Systems

With a rich legacy in this technology, Boeing and a best-of-industry team is embarking on the next step under a partnership with Northrop Grumman Mission Systems. Developing a Space Based Space Surveillance (SBSS) Pathfinder is a low-risk solution with a capability that nearly matches with one satellite the capacity of all the Earth-based optical sensors combined. Furthermore, it offers flexibility to track objects unconstrained by daylight or weather.

The industry team is leveraging expertise in surveillance mission systems engineering and software development under its AFSS unit, and developing high-performance onboard mission data processors at the Satellite Development Center. SBSS is considered an essential element in achieving full SSA capability. A SBSS constellation will eventually provide the coverage required to ensure space superiority capability is available to the warfighter. Our adversaries recognize our overwhelming dependence on space assets and we must have the ability to detect and track space objects—especially those that might be considered a threat. The Pathfinder launch is scheduled for December 2008, followed by two program down-selects to determine the final development contractor. IOC of the constellation is expected in FY 2013.

Threats to Our Space Assets

The US demonstrated micro-sat capability on 29 January 2003 with the Boeing XSS-10 proof-of-concept on-orbit autonomous rendezvous. XSS-10 was launched as a piggyback secondary payload aboard a scheduled Delta II carrying a GPS IIR. The micro-sat maneuvered around the orbiting Delta II second stage, backed away and relocated the stage—and then migrated back as cameras transmitted downlinked imagery to AFSPC. This experiment proved that small robotic space systems could be used to interrogate, and if necessary, negate assets on orbit.



Threats to Space Assets

- Information Warfare
- High Power Lasers
- EMP
- ASATS
- Micro/Nano Satellites
- High Power Microwaves
- Space Based Jammers
- Space Debris (9,000 currently on-orbit)

Erik Simonsen

Threats to Space Assets.

Erik Simonsen

Space assets supporting C2 .

The US tested an antisatellite (ASAT) system in the early 1980s, successfully destroying an obsolete target satellite. The 18 ft. long 2,700 lb. ASAT was carried on the centerline pylon of an F-15A flown by Major Wilbert D. "Doug" Pearson, Jr. (later, Maj Gen Pearson, Commander, Air Force Flight Test Center). After a 3.8g pull-up, commencing on a precise ballistic flight profile, the ASAT launched at 38,100 ft. and kinetically killed the satellite at an altitude of 345 miles. The program ended shortly after that, leaving the US without an operational system. However, research and development into ASAT technology is continuing.[10]

Today, several countries now possess the technology to covertly encounter our assets on orbit. Russia certainly has the capability to launch unannounced secondary payloads that could move covertly into orbits near critical space assets. The Russians also tested ASAT capability during the1970s and a conceptual space-based laser during the late 1980s. Ground-based lasers have also been tested with effective results out to GEO.

In addition, China has firmly established itself as a major player in space with a well-publicized civilian space program consisting of manned and unmanned activities. In areas not so publicized, they are also developing technologies that could threaten our space assets. This could consist of micro-satellites and/or high energy lasers, either ground-based or space-based. A Chinese micro-sat was tested in June 2000 and their work on ASATs with potential laser applications is continuing.[11]

"Our terrestrial, airborne and space ISR assets must be fully integrated to support knowledge creation and we must protect them against physical, electronic and information warfare attacks. We must also have the ability to rapidly reconstitute their capability."

- George K. Muellner, President,
Boeing Advanced Systems

Conclusion

Moving forward, we will experience increased dependence on space systems to provide secure communications, surveillance, early warning, navigation, weather, and precision engagement. Assuring connectivity to our troops with these systems is a top priority. As in the early 1950s, today we stand on the threshold of a new era. The launch of Sputnik provided the catalyst then—we now see a new one emerging. We can no longer assume immunity from attack in the realm of space, and we must take the initiative to ensure the viability of our space assets.

The Air Force has embarked on a path that challenges industry to produce the technology and capabilities necessary to ensure the security of our Nation. We in Boeing have long been a partner with the Air Force in developing and deploying robust space capabilities in what has been a truly fantastic journey. As we stand at the beginning of a new century, we look forward to continuing along this exciting path. Together we take on the daunting challenges of the new frontiers that lie before us.

Notes:

[1] General Lance W. Lord, Commander, AFSPC, 'Tribute to Gen Bernard A. Schriever' (remarks, AFA Annual Salute to SMC, Los Angeles, 15 July 2005).

[2] Maj Charles H. Cynamon, "Protecting Commercial Space Systems: A Critical National Security Issue," Research Report (Maxwell AFB, AL, Air Command and Staff College, 18 April 1999).

[3] Peter B. Teets, former Acting Secretary of the Air Force, (remarks at the National Defense Space Symposium, Fairfax, VA, 26 February 2003).

[4] Statement by Admiral Edmund P. Giambastiani, Jr., Commander, United States Joint Forces Command and Supreme Allied Commander Transformation (NATO), before the House Armed Services Committee, US State House of Representatives, 2 October 2003.

[5] Peter B. Teets, undersecretary of the Air Force, (remarks, National Defense Industrial Association Space Symposium, Fairfax, VA, 26 February 2003).

[6] Erik Simonsen, "2 satellite programs look to meet military's need for bandwidth," Boeing Frontiers 4, no. 9, February 2006, http://www.boeing.com/news/frontiers/i_ids7.html (accessed 28 February 2006).

[7] Benjamin S. Lambeth, *Mastering the Ultimate High Ground: Next Steps in the Military Uses of Space,* (RAND, Project Air Force, 2003) 101.

[8] Robert S. Dudney and Peter Grier, "New Orbit for American Space Power," *Air Force Magazine*, February 2004. Remarks by General Lance W. Lord, Commander, AFSPC, 40.

[9] Maj Gen James Armor, Director, US DoD National Security Space Office, *Space News,* profile, Warren Ferster and Jeremy Singer, 11 July 2005.

[10] Dr. Raymond L. Puffer, "A Death of a Satellite," AFFTC History Office, http://www.Edwards.af.mil/moments/docs_html/85-09-13.html (23 February 2006).

[11] Maj Richard J. Adams and Col Martin E. France, "The Chinese Threat to US Space Superiority," *High Frontier*, Winter (2005), 19-20.

Shephard W. Hill (BA, Stetson University) serves as Senior Vice President, Business Development and Strategy, The Boeing Company. Mr. Hill is responsible for analyzing and developing plans to drive the company's growth and nurture new businesses. A member of the Boeing Executive Council, he oversees the company's Corporate Development function, with responsibility for acquisitions, divestitures, mergers, equity investments, and joint ventures.

Prior to his current position, Hill was Vice President, Business Development, at Boeing Integrated Defense Systems (IDS), with responsibility for the development, integration, and implementation of IDS customer and business strategies.

Prior to that position, Mr. Hill was Vice President, Boeing Space and Communications (S&C) Government Relations responsible for management and direction of S&C's business interests and activities in the Washington DC area, including marketing, legislative affairs, trade, and media relations.

Prior to this position, Mr. Hill served as Space Systems Vice President for Boeing's Integrated Space and Defense Systems business unit.

Mr. Hill joined Boeing when the company acquired Rockwell's Aerospace and Defense business in 1996. At that time, Mr. Hill was Rockwell's Vice President, Aerospace Government Affairs and Marketing.

Prior to joining Rockwell in 1987, Mr. Hill served as Chief of Staff and Legislative Director to Congressman Bill Chappell (D-FL) from 1980 to 1987.

Mr. Hill received his education from John F. Kennedy School of Government Harvard University - Program for Senior Executives in National and International Security (1989); Naval War College (1981-84).

Industry Perspective

Net-Centric Transformation for Space Command and Control

Mr. John Mengucci
Vice President and General Manager, DoD Systems
Lockheed Martin Integrated Systems & Solutions

Space systems play a vital role as a key enabler in the command and control (C2) of US air, land, and sea assets. They are critical systems that have helped transform the way the Nation conducts joint military operations. The effectiveness and optimization of these operations and assets will be made even greater with the net-centric integration of sensors, decision-makers, and shooters to achieve unprecedented advantages in shared awareness, greater speed of command, higher operations tempo, greater lethality, increased survivability, and improved synchronization.

The importance of both net-centricity and space C2 capabilities are essential to Air Force Space Command (AFSPC). AFSPC, with its partners, is transforming satellite communications to provide network-centric, high-capacity communications, and develop transformational advancements in the Command's operations. In particular, Air Force leadership sees the integration of network-enabled systems and solutions delivering much-desired enhancements in the ability to task, collect, process, exploit, and disseminate intelligence, surveillance and reconnaissance (ISR) data in a way that is fully integrated with air, ground, and naval forces for joint operations.

Space C2 capabilities will allow the US to predict and shape the effectiveness of its space assets, initiate actions, and react to developing situations. In responding to these new demands, industry and government must team to develop and field world-class C2 capabilities that enable commanders at many different levels to share information in real-time and across a battlespace. New net-centric technologies, with "Human-In-The Loop" interfaces, will provide our joint space forces the capability to quickly monitor and assess worldwide events and fully integrate space assets to produce enhanced space situation awareness and deliver desired effects.

Lockheed Martin

The Joint Space Operations Center (JSpOC) at Vandenberg AFB, California, is the Nation's focal point for space C2, and will benefit from a net-centric operational environment. Formally established in May 2005, the JSpOC allows the coordination and control of assigned US military space assets, for the first time, under a single authority—the Commander, Joint Space Operations—who provides direction to the JSpOC.

By providing shared situation awareness with regional commanders worldwide, other Joint Functional Component Commanders and special centers in US Strategic Command (USSTRATCOM)—and even among military personnel involved in combat operations—the JSpOC will be a key enabler of Effects-Based Operations around the globe. The bottom line is this: the JSpOC will allow the US and its allies to be more effective, experience greater efficiencies in its operations and have more influence.

Among the JSpOC's essential functions is that of providing space situation awareness. This includes the management of satellite communications as well as ensuring that the Global Positioning System (GPS) constellation of satellites is functioning and available to provide precision navigation and timing. Additional capabilities that benefit warfighters and our citizens include those that enable non-kinetic alternatives, in addition to accurately putting GPS-guided weapons on target. Enabling rapid and accurate response to natural disasters through real-time feedback and imagery is yet another example of benefits derived from US space capabilities.

The JSpOC is viewed by many leaders as the culmination of years of evolutionary thinking about space power and its applications. Establishment of the JSpOC reflects an understanding of the wide-ranging critical importance space plays in enabling US force projection capabilities and helping facilitate the high efficiency of the US economy. The JSpOC will deliver the right capabilities and effects when and where they are needed.

The JSpOC is tasked with providing several areas of support —for STRATCOM's global strike mission and its other functional components' missions and the supporting missions for all geographic and functional combatant commanders.

Challenges Loom to Net-Centricity

One of the JSpOC's many challenges is merging the requirements of USSTRATCOM and the Joint Functional Component Commanders along with theater commanders into an overall strategy that provides a common view of space-derived situation awareness. Directly related to this discussion is the recognition that information from satellites today is often "stove-piped" according to strict categories—communities of users, for instance, or security classification—making it difficult to disseminate that information rapidly.

Indeed, the JSpOC's command and control capabilities will evolve to address these challenging global and theater requirements. Without a doubt, standing up a joint center for C2 of space was the right approach to meet these challenges.

Providing the JSpOC with a "global"-class C2 capability is the next step in addressing these issues. One of the first actions in achieving interoperability is information sharing between theater systems such as the Theater Battle Management Core System that supports joint air operations worldwide, and the Space Battle Management Core System/Single Integrated Space Picture, utilized by the JSpOC. Information sharing among these systems will allow theater and space operations to be synchronized for greater effectiveness—enabling common command and control business processes.

Additionally, leveraging, adapting, and integrating the existing and planned Air Operations Center (AOC) weapons system capabilities may provide the most rapid means to enable vastly improved air and space integration. Indeed, prototyping these integrated capabilities is a high priority for Lockheed Martin. From this work, we intend to evolve significantly improved Joint C2 (JC2) capabilities that will enable integrated space-air-land-sea-cyber operations. Addressing stated and evolving JSpOC global requirements both rapidly and effectively is a key part of our efforts. It's a matter now of getting started and working out the wrinkles.

A Net-Centric Laboratory for Prototyping, Experimentation, and Collaboration

Lockheed Martin is well on the way to meeting these challenges. We have partnered with government to develop responsive service-oriented architectures for nearly ten years and have embarked on the fifth generation of these systems. Technically, in fact, the foundations for the required architectures already exist. At our Center for Innovation net-centric laboratory in Hampton Roads, Virginia, a Global Information Grid test bed and a Net-Centric Enterprise Services prototype have been created to facilitate net-centric architecture convergence and other net-centric synergies. Complex C2 experiments are being conducted with our Department of Defense partners to further improve the state-of-the-art and the state-of-the-possible in achieving a net-centric operational environment.

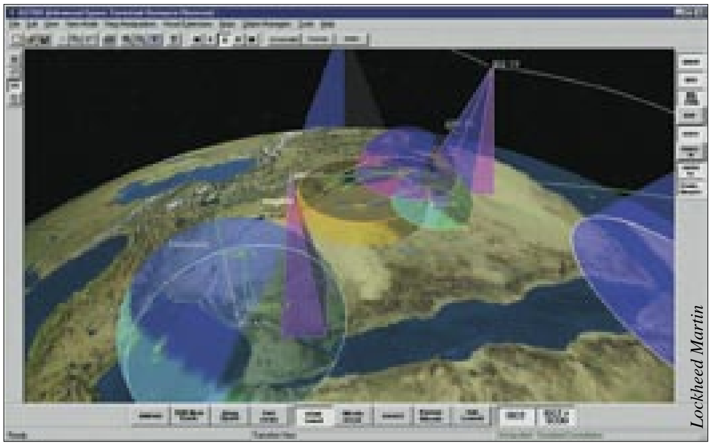
The whole idea of service-oriented architectures is to place real-time information on a network, making it available to multiple users so it can be accessed and shared with the click of a mouse, as easily as information is found with browsers and search engines today. Because this capability is not yet available for space C2, a first goal is to develop meta-tagging capabilities—providing information about information, which would identify its origins and when and where it was produced, as an example. This will be one of the components paving the way to net-centricity.

With this collaborative environment in place, JSpOC C2 capabilities will be enhanced and tough challenges will be more manageable. For one, the JSpOC will be able to manage competing demands for heavily used satellites more efficiently. When information from multiple sources can be fused, a much clearer, focused picture of the area becomes available. Indeed, integrating "multi-int" space data with tradition/non-traditional ISR from air, land, sea and cyber environments enables one of the first opportunities to improve Effects Based Operations with "persistent" ISR.

Lockheed Martin

One result will be a change in the way that warfighters react to new information/direction from higher command levels. As net-centric operations begin to evolve, changes are certain to occur. For instance, not too long ago some aviators would express concern when operational-level commanders scrutinized their tactics or plans from afar. Today, AOCs have access to enhanced multi-intelligence data and connectivity technologies that allows improved battlespace awareness. Often times, this results in flights and missions being redirected to address time-critical targets. In the future, information technology and networks will inevitably make this information more available to our soldiers, sailors, and Airmen in "their cockpits," and the art and science of command and control will inevitably shift again. Net-centricity allows the degree of resilience and flexibility in C2 that addresses these subtle changes.

Lockheed Martin's Total Integrated Warfare (TIW) prototype is clearly on the forefront of this change. TIW exemplifies the power of net-centric operations, allowing battlefield com-



Lockheed Martin

manders to control hundreds of friendly units in real time. It creates a continuous and dynamic link among commanders, troops, platforms—and even missiles after they are launched. This connection enables commanders and warfighters to assess, decide and react to change on the battlefield like never before.

As an example, "air-breathing" ISR capabilities can be integrated with space-based ISR to provide a greater, more agile collection capability (increased persistency) to support both theater and global operations. If a new threat or high-priority target suddenly appears, the TIW system could enable the AOC and/or JSpOC to determine the best course of action or best available resources to re-task. By using net-centric capabilities to cross-reference the current location and status of blue forces, the TIW system could better assist the AOC in time sensitive targeting. The new course of action is transmitted to the mission commander, who generates a new route and targeting plan that is transmitted back to the AOC for authorization. We know all too well that "no plan ever survives first contact with the enemy," but with TIW our forces will be able to adapt, respond, and engage quicker and more effectively.

This same technology can be applied to the command and control of space capabilities. The result is unprecedented flexibility in battle management, giving commanders full control of joint forces across the theater and allowing them to face any threat with speed, precision, and confidence.

Meanwhile, there must be more emphasis on how the space community will employ such architectures to satisfy the mission needs and tasks laid out in the Operating Concepts. The Space Commission report of 2001 outlined improvements that are needed in the areas of space situation awareness and global command, control, and communications in space. The challenge is to fund those recommendations to allow the JSpOC to focus more sharply on its five critical missions—space superiority; global surveillance, tracking, and targeting; global information services; command and control of space forces; and assured access.

Mr. John Mengucci (BS, Computer Science, Clarkson College of Technology; MBA, Organizational Management and International Business, Syracuse University) is vice president and general manager, Department of Defense (DoD) Systems, Lockheed Martin Integrated Systems & Solutions (IS&S).

As Vice President and General Manager for DoD Systems, he is responsible for the delivery of intelligence, surveillance, and reconnaissance (ISR) systems, Command and Control technologies, and Satellite Ground stations to a large DoD customer base. He has served in a number of management assignments for Lockheed Martin, including Chief Executive Officer of Lockheed Martin Orincon prior to consolidation of that acquisition into the Lockheed Martin Corporation. Other key assignments include Vice President of Space-Ground Integration Systems where he was responsible for the design, development and deployment of satellite ground stations for numerous national programs such as the Advanced Extremely High Frequency, the Space Based Infrared System, the Global Positioning System, and the Transformational Communications Satellite—TSAT—program.

Mr. Mengucci has also served as Vice President of Public Safety & Criminal Justice Systems, where he was responsible for entry into new adjacent markets for Lockheed Martin and as Director for International Business Development for Lockheed Martin Global Telecommunications.

Integrated Systems & Solutions is one of five principal business areas within Lockheed Martin. IS&S leads the Corporation's systems engineering and integration activities for high-value network-centric information and intelligence systems that support missions of the DoD and other national security customers. IS&S provides transformational solutions for intelligence, surveillance and reconnaissance, command, control and communications and combat support to the DoD and the Intelligence Community.

Space Command and Control

The First Line of Defense

Col John E. Hyten, USAF
Commander, 50th Space Wing

Since the earliest days of satellite operations, the Air Force (AF) has been a leader and a recognized expert in providing command and control (C2) for our nation's military satellites. Many things have changed over the years—implementation of new technologies, expansion of the role of enlisted satellite operators, standardization of operational procedures as engineers were moved off the operations floor, and reorganization at the strategic and operational levels of space C2, to name a few. What has not changed, in the last 45 years,[1] astonishingly, is the basic philosophy of satellite C2.

Command and control of all our military satellites today is still based on two basic tenets, both of which have serious shortcomings: (1) satellite operations take place in a benign environment, devoid of any threat except the space environment, and (2) each satellite constellation is designed and operated as a separate entity with no need for horizontal integration with other space capabilities. Additionally, there has been a developing perception in the last decade that views space operations as a rote activity requiring only a very basic knowledge of the C2 system and little understanding of satellite weapon system's technical details and its associated mission effects.

Because of our adherence to these two tenets and this perception of space operations, we do not fully comprehend how to fight our space weapon systems at the tactical level of war, are not organized or equipped to carry out such an effort, and have not trained our people to be prepared for such a fight. The organization, processes, and tactics, techniques, and procedures (TTP) used for tactical-level C2 of Department of Defense (DoD) satellites are inadequate to respond to even the most rudimentary enemy actions that would attempt to deny the United States freedom of action in space. Neither are they sufficient for the complexity and greatly increased flexibility of future satellites, nor for the networked architecture of new satellite constellations. This article will present ideas to respond to these challenges and allow AF space operators to effectively fight and defend military space in the coming years.

Vulnerabilities

As pointed out by numerous commissions, including the Rumsfeld Commission,[2] and our national leaders,[3] our ability to operate in space will not go unchallenged for much longer. In fact, we have already begun to be challenged in small ways with efforts to jam or interfere with the Global Positioning System (GPS) and space-based communications in recent conflicts.[4]

There have been literally hundreds of studies on both the threat to US space operations and the vulnerabilities of our space systems. Joint doctrine summarizes the threats and vulnerabilities quite simply:

> Ground to satellite links are susceptible to jamming. Fixed command and control facilities are subject to attack, which could degrade the utility of a satellite's service over time. Launch facilities must be protected to ensure access to space so that force replenishment may be accomplished. Some space capabilities may also be subject to exploitation, such as an adversary using commercial global positioning system (GPS) receivers for navigation. Knowledge of an adversary's negation and exploitation capabilities will allow a joint space planner to develop appropriate responses.[5]

It is curious to note the focus of concern in joint doctrine is on the joint space planner—not on the space operator. It is also interesting to note that in both joint and AF doctrine, only two levels of space command and control are discussed—global and theater. Specifically, the discussion revolves around actions that take place at the strategic and operational levels of war. Even in the AF Doctrine Document, Counterspace Operations,[6] the discussion is based primarily on generating global and theater effects and is structured primarily around how to provide *offensive* counterspace (OCS) effects. Again, even in an OCS scenario, the enemy is assumed not to have a vote—the space environment is still assumed to be benign.

Even though there is general agreement among military space planners that space will eventually become a theater of combat operations,[7] doctrine does not adequately address planning and executing defensive counterspace (DCS) operations. Perhaps this is because the DCS battle would likely be responding to an attack either in the "peaceful" environment of space or an attack on our national infrastructure—neither of which is easy or popular to talk about. However, it is imperative these vulnerabilities be thoroughly addressed.

When conflict in space occurs, the first line of defense will be the satellite operators sitting at a terminal in an operations center at Schriever Air Force Base (AFB) or a similar facility. In the face of an active threat, the operator must be able to quickly detect, analyze, and fight through an attack on his/her satellite ensuring the continued delivery of critical space effects to combat forces (and civil users) around the world. Through no fault of their own, this is not the case today. Unfortunately, our current organization, equipment, C2 structure, and training do not allow this type of response.

Tactical Level of War

Joint Publication 1-02 defines the tactical level of war as:

> The level of war at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.[8]

Does the tactical level of war apply to a space conflict such as those described above? Most certainly.

It takes little imagination to describe the beginnings of such a conflict. Any enemy involved in armed conflict with the United States—from a nation-state to a terrorist group—will likely attempt to deny or degrade the US space advantage. Possible threats include electronic attacks on our spacecraft and critical infrastructure. There are also threats of physical attacks on a remote tracking station somewhere around the world and against our space operators and operations centers in an attempt to deny the United States the capability to command our space systems. In the not-to-distant future, threats may also include an attack with a microsatellite, an interceptor, or a directed energy weapon in an attempt to destroy or degrade the satellite itself.[9]

In each of these situations, satellite operators will almost certainly be the first forces in contact with the enemy. Today, they would likely observe the effects of the jamming or attacks but struggle in discriminating it from environmental effects or satellite anomalies. New and improved capabilities like the Interim Satellite as A Sensor (ISAS) and the Rapid Attack Identification, Detection and Reporting System (RAIDRS) programs have the potential in the near term to allow space operators to begin to quickly characterize the jamming/attack.[10]

The characterization of the attack (and perhaps an initial geolocation) could provide information to allow the negation of the jamming threat—but only if the proper C2 structures are in place to enable timely reporting of the attack to a theater or others who understand the implication of the attack and have the ability to respond against the attacker. The reporting of hostile actions and the impact of those actions to terrestrial forces may, in certain scenarios, be most effectively accomplished through the Joint Space Operations Center (JSpOC)—which exercises operational control (OPCON) of assigned space forces.[11] However, in some cases it may be more timely and effective if these actions are reported directly to the affected theater of operations, if the satellite operators were placed in direct support to that specific theater.

Effective tactics, techniques, and procedures for both these kinds of responses do not yet exist. Developing these TTPs along with new operator skills will be required. We must train and exercise these new capabilities with the tactical units, JSpOC, and the theater to enable the operators at both the tactical and operational levels to effectively respond to attacks on our space systems. With good intelligence, appropriate TTPs, and properly constructed C2 relationships, it can be possible for us to fight and win the DCS battle and ensure the required effects continue to be provided by our space forces. Again, it all begins with the satellite operator.

In addition to our spacecraft and data links, our C2 nodes themselves are potentially vulnerable to attack. Should such an attack be successful, it is essential we have geographically-separated backup C2 capabilities, with all the required planning and support capabilities, to allow us to quickly relocate and continue to influence the battle by providing effects from space. In many cases, these backup nodes do not exist or exist only in a rudimentary fashion.

In the attack scenarios discussed above on spacecraft, data links, and ground nodes, space operators initiate military responses at the tactical level of war—that by law and tradition must be carried out by our Nation's uniformed military forces.[12] Contractors and civilians can perform many of our space operations functions, but they cannot directly engage an enemy.

So, does the *tactical* level of war apply to a space conflict? Yes! As shown, fighting and defending military space, gaining and maintaining space superiority, requires **"battles and engagements"** that must be **"planned and executed"** to allow our Nation to **"accomplish military objectives"** that will be performed by **"*tactical* units"** of our USAF primarily at the wing-level and below. A "space war" is fought, not as a war unto itself, but as part of a larger campaign, and it certainly includes the tactical level of war.

Imperative For New Organizational Structures

Without a doubt, tactical "space battles" will be fought by space operators and space warriors as we move forward into a time of increased threats to our space capabilities. Therefore, it is essential that we begin to modify our C2 approach and organization now to enable operations at the tactical level of war in the future.

As we continue to mature technologies required to fully integrate space effects in the battlespace, we must also examine our existing organizational structures and processes.[13]

- General Lance W. Lord

We are at a critical time in the maturation of military space operations…the threat is very real and ever-increasing. This alone demands a new kind of response and culture. At the same time, the Air Force is modernizing most of our satellite control systems and ground tracking, telemetry, and commanding (TTC) sites. New satellites—Wideband Gapfiller System (WGS), Advanced Extra High Frequency (AEHF), GPS III, and Space Based Infrared System—are in various stages of development and deployment. Even more capable satellites are right around the corner, like the Transformational Satellite Communications System (TSAT) and Space Radar (SR). Over the next decade, if all the potential satellite acquisition programs are delivered, the on-orbit force structure of the 50th Space Wing (50 SW) at Schriever AFB could increase by 350 percent.[14] Even if acquisition programs continue to have problems and are delayed, the on-orbit force structure of the 50 SW will easily double. We must remember that as these new, complex satellite systems come on line, we will continue to operate our legacy systems as well.

If we choose to operate these new weapon systems using the historic satellite operations model, we would double or triple our personnel and add new operations centers. However, in the current fiscally constrained environment, this is clearly not a practical option – and not an option that we are pursuing. The current environment does, however, provide us the opportunity to design and build a new tactical C2 structure that will not only allow us to better fight and defend military space, but do so in a more efficient way that does not stress our personnel and resources.

This demands not only a change in organization, but development of new capabilities emphasizing machine-to-machine interfaces that provide decision-quality information to space operators so they can fight through attacks and ensure required space effects continue to be delivered. These capabilities will enable space operators to efficiently fight these new weapons systems and fully employ their advanced capabilities (flexible power, shaped beams, and other capabilities that enable them to fight through adverse environments).

Integrated Operations Centers

The first step required for more efficient and effective tactical space command and control is the evolution of satellite operations from stove-piped, separate operations centers focused on satellite TTC to Integrated Operations Centers with an unwavering focus on the delivery of combat effects.

The tactical-level C2 architecture of the future requires an effects-based, mission area operations center for each mission area and wing-level, Integrated Operations Centers. For example, an effects-based mission area operations center for military satellite communication (MILSATCOM) would look across all the MILSATCOM satellite constellations to provide the required effects, maintain the initiative in the DCS fight, and ensure maximum effectiveness of system employment. They would gain efficiencies of net-centric operations, and create the environment required for close cooperation across the networked architecture of the future. The operations center of the future must link multiple services and agencies, each operating their portion of the architecture, but doing so in a way that ensures unity of effort that can only be gained by a system-of-system approach to employment and under the tactical-level command of a mission area commander.

A wing-level operations center must then integrate tactical operations across multiple mission areas to ensure the effects required higher levels of command are executed. This is also where an integrated DCS picture is analyzed for possible coordinated action across multiple mission areas. The commander of this wing-level operations center will be responsible for the daily execution of the wing's mission.

This concept of C2 is well correlated with Air Force Space Command's Enabling Concept for the Space Command and Control Weapon System.[15] The enabling concept outlines the need for integration across "disparate systems with limited horizontal and vertical integration."[16] The Space C2 Weapon System will be a critical enabler of the required integration and is designed to "be used by multiple organizations across all levels of command."[17]

This is not a trivial change. Not only does it require a new organization with new equipment and processes, but it must be enabled by four critical elements.

First, our space operators must develop a DCS mindset with a warrior spirit. The traditional satellite operator mindset, when faced with an on-orbit problem, is to assume an environmental upset or on-board anomaly—the canned response is to "safe" the satellite and call the engineers. A DCS-oriented response is to assume a potential attack, develop response options that do not place the satellite at risk, ensure the required effects continue to flow to terrestrial forces, and take action to fight through the problem.

Second, operators with a DCS mindset must be experts on their weapon systems. They must understand what the satellite can and cannot do to enable them to fight through a hostile action and continue to execute their mission. They must understand the effect they are creating, how they fit into campaign plans, and be able to communicate in a common language with other joint warfighters. Satellite operators must be the recognized experts on their weapon systems; so, the training we provide them needs to be restructured to enable such expertise.

Third, operators must be able to integrate and synthesize information from across multiple constellations in order to understand enemy actions—and take actions both in response to and in anticipation of enemy threats and actions. Horizontal integration is vital to assimilation of critical information involving space surveillance, space intelligence, and current operations status from which operators can make accurate and timely decisions.

Fourth, this integration must occur in real time or near-real time and must be reported to the operator and delivered into a common data base (a Single Integrated Space Picture [SISP]) so that warfighters can pull the critical information and fight the fight at every level of war (strategic, operational, as well as tactical). The SISP will not only allow more effective tactical decision making, but will also provide critical information to higher levels of command and influence operational and strategic decisions.[18]

Efforts to develop a SISP have focused on higher levels of war despite the fact that information critical for this data base is mostly generated by tactical military space operations. We struggle to move the concept for a SISP into a useful tool in large part due to this focus on the operational and strategic level—partially because at these higher levels the challenge of the SISP is hard to scope and implement and the answer never is complete. The elegance of SISP is that it leverages available tactical data—the SISP populates itself as information becomes available—continuing to mature as tactical operations mature if the right C2 structure is put in place.

The Integrated Operations Center is also where machine-to-machine interfaces become absolutely essential. Currently there are very few AF satellite C2 systems that deliver information focused on combat effects to anyone who can really make a decision. Only in recent times has the 2nd Space Operations Squadron stood up a GPS Operations Center (separate from the satellite C2) that focuses on delivering effects to GPS users. Likewise the 4th Space Operations Squadron, which operates the Milstar communications system, has internally developed a back room solely focused on responding to real time problems from global users; this back room is also separate from their operations floor.

Unfortunately we are not leveraging automation to help these squadrons respond to problems. Every problem is handled in an ad hoc fashion by a small cadre of systems experts (internally trained) that respond to user problems involving everything from user equipment, to satellite problems, to environmental interference, and, for the first time recently, enemy actions. In the future, these processes must be integrated with the satellite C2 ground system and combined with a new training program focused on developing effects-based weapon systems expertise. This will allow an on-duty commander to comprehend the effect he/she is providing and to take action when that effect is interrupted. The next-generation Air Force Space Command (AFSPC) crew commander will no longer command a crew, but will transition into a full-fledged mission commander delivering combat effects and fighting their weapon systems. Leveraging new machine-to-machine interfaces will improve the timeliness of information and allow a reduction in personnel required to generate the effects.

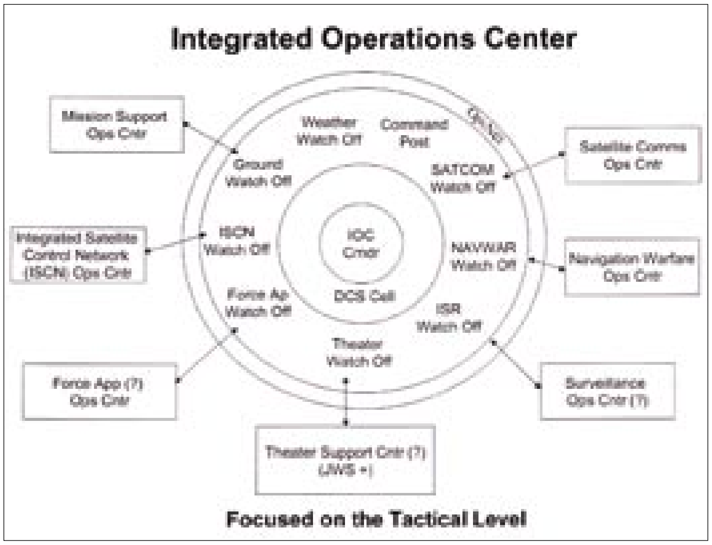


Figure 1. Integrated Operations Center.

Along with the required hardware changes that will enable net-centric operations, we need to ensure clear command relationships are established and articulated between the Combatant Commander (COCOM) that requires effects from space and the operators providing those effects. In the past, most operators controlling space systems did not know who exercised OPCON or tactical control (TACON) over them. They also did not know if they were placed in a direct supporting relationship with another organization or if direct liaison authorized had been granted. Undefined terminology like "ownership" of a system was common. In the future it is imperative the mission commander understands who can direct their actions, who they can directly communicate with, and who is merely raising the noise level. This understanding will enhance unity of effort by ensuring the mission commander understands where they fit within a unified command structure and how they integrate in the larger campaign plan.

In summary, the satellite C2 structure of the future requires horizontal integration of tactical information populating a single picture allowing a commander to make tactical decisions. This commander can then fight through problems and continue to provide combat effects to the supported commander while providing real or near-real time information to both supported and supporting commanders at higher levels of war. The tactical commander must have DCS and Space Situation Awareness information being fed to him/her on a continual basis to allow adjustments within and across satellite constellations. And, the tactical commander must have clear, explicit command relationships.

Although the physical structure of such an organization could take any variety of shapes—virtual connectivity and a network environment minimizes the need for significant new physical structures—conceptually a wing-level integrated space operations center would look something like figure 1.

A structure like the Integrated Operations Center above forces a tactical DCS focus. The DCS Cell, supporting the Integrated Operations Center Commander, will need to have access to tools like ISAS and RAIDRS as well as the ability to effectively populate and pull information from the SISP. The operations center would not have huge teams as with current battle staffs, support battle staffs, and squadron Crisis Reaction Elements (CREs). Quite the contrary, the center commander would be supported by watch officers who connect directly with the various mission commanders and provide direct reporting of critical information.

The Integrated Operations Center commander would be responsible for delivering integrated effects across mission areas—beginning with force protection and ground network operations, incorporating traditional space operations missions delivering global and theater effects from navigation, surveillance, and communications systems, and then evolving in the future to include new capabilities for theater support (i.e., Joint Warfighting Space) and perhaps even force application from or through space.

This C2 construct is equally valid if a system has "chopped" to a theater commander and that commander has TACON of a space-based asset, the mission commander would then be placed in direct support of that theater; or if OPCON/TACON of a system remains with the Commander Joint Space Operations and is exercised through the JSpOC's Space Tasking Order (S-T-O) process.

As the Integrated Operations Center matures and better automated tools are developed, the watch officers may disappear altogether and the operations center commander will interface directly with the various mission commanders.

In the mission area operations centers, satellite TTC will cease to be the primary focus of satellite operations and will evolve into one of many enabling functions. The TTC-focused satellite operations crews of today will be usurped by automated systems requiring much smaller numbers of operators. In their place will be new effects-based crews focused on ensuring the end-to-end success of their mission. The military members in the new integrated mission centers would concentrate on fighting their weapon systems with an absolute focus on the delivery of combat effects; while a small number of civilians or civilian contractors under military direction perform many of the TTC functions performed by military members today.

This is when the crew commander truly transitions to become a mission commander—now focused on the mission, and the mission is delivering effects—as tasked by an effects-based S-T-O, not just flying satellites.

WHAT WE NEED	TODAY	TOMORROW
Real time attack detection and reporting	Some systems	All systems integrated into SISP
Real time response	Minimal	Integrated across all systems
Effects based operations	Infancy	Mature for all systems
Doctrine	Planner focused	Operator focused
Space environment	Assumed peaceful	Assumed hostile
Backups geographically separated	Some	All
Effects based training	No	Critical
Effects based tasking	No	All systems
TTP	System descriptions	Executable in tactical operations
Integrated Ops centers	No	Basis for all space operations

Table 1. First Line of Defense Building Blocks Summary.

The Integrated Operations Center helps enable this transition and breaks down the barriers. With virtual connectivity, it could be hosted at any location, the JSpOC for example, with tactical information pulled from the wings and other operations centers. However, with new, complex, networked, taskable satellites coming on line in the not too distant future, it seems more efficient and effective to place these Integrated Operations Centers at the tactical level, at the wing, where the mission is accomplished. They would then populate the SISP data base and provide critical situation awareness needed at both the operational and strategic levels. By building the SISP at the wings, the operational and strategic levels would not have to filter mountains of tactical information; instead they could configure their own picture to provide the appropriate level of insight needed.

In summary, to continue to build the first line of defense we need to move from today to tomorrow as depicted in table 1 on page 22.

Conclusion

This article has described the need for a new approach to tactical-level satellite C2. This need is based on (1) space now being a theater of hostile action, (2) the complexity of new satellite systems, and (3) the networked architecture of new satellite constellations both within and across constellations. It also pointed out that continuing to build stove-piped systems will create an unmanageable requirement for resources and manpower. It presented a challenge to develop TTP, training programs, and exercises to help transform space operations from primarily providing TTC of satellites to a focus on providing required effects and always approaching operations with a DCS mindset. It then presented a new tactical-level (wing level) C2 construct based on network-centric mission area operation centers and wing-level Integrated Operations Centers. These centers will provide a mechanism to retain the initiative in the DCS battle. They also provide for system-of-systems management of mission areas to enhance responsiveness to the JSpOC and supported commanders through enhanced unity of effort.

This may not be the right vision, but if it isn't, what is? The Integrated Operations Center structure described above may not be the perfect model, but if it isn't, what is? A detailed discussion of the way ahead for tactical space C2 is essential for the future of AFSPC and for the future of military space operations. Whatever the final path turns out to be, a transformation of tactical satellite C2 must take place and changes must begin soon. Now is the time!

Col John E. Hyten (BS, Engineering and Applied Sciences, Harvard University) is the Commander, 50th Space Wing, Air Force Space Command, Schriever AFB, Colorado. As Commander, he is responsible for more than 3,600 military, Department of Defense civilians and contractor personnel serving at 50th SW operating locations worldwide, in support of more than 170 communications, navigation and surveillance satellites with their associated systems valued at more than $46 billion.

Colonel Hyten's career includes assignments in a variety of space acquisition and operations positions. He has served in senior engineering positions on both Air Force and Army anti-satellite weapon system programs. The colonel's staff assignments include tours in the Air Force Secretariat, on the Air Staff, on the Joint Staff and as the Director of the Commander's Action Group at Headquarters Air Force Space Command. He served as a mission director in Cheyenne Mountain and was the last active-duty commander of the 6th Space Operations Squadron at Offutt AFB, Nebraska. Prior to assuming his current position, Colonel Hyten commanded the 595th Space Group in the Space Warfare Center, also at Schriever AFB. He was nominated by the President for promotion to brigadier general 4 November 2005.

Notes:

[1] National Reconnaissance Office, "Corona Facts," http://www.nro.gov/corona/facts.html (accessed 16 February 2006). The NRO Corona satellite was first operational in August 1960.

[2] Space Commission, *Report of the Commission to Assess United States National Security Space Management and Organization*, Executive Summary, 11 January 2001.

[3] Testimony of Acting Secretary of the Air Force Peter B. Teets to the Senate Armed Services Committee, *Fiscal Year 2006 Air Force Posture,* 3 March 2005; Lt Col John E. Hyten, *A Sea of Peace or a Theater of War: Dealing with the Inevitable Conflict in Space,* Program in Arms Control, Disarmament, and International Security, University of Illinois, April 2000.

[4] Bill Gertz, "U.S. Deploys Warfare Unit to Jam Enemy Satellites," *The Washington Times*, 22 September 2005.

[5] Joint Publication (JP) 3-14, *Joint Doctrine for Space Operations*, 9 August 2002, I-3.

[6] Air Force Doctrine Document 2-2.1, *Counterspace Operations,* 2 August 2004, 35-43.

[7] Space Commission, *Report of the Commission*.

[8] JP 1-02, *DoD Dictionary of Military and Associated Terms*, 12 April 2001, tactical level of war, 526.

[9] JP 3-14, *Joint Doctrine for Space Operations*, 4.

[10] Air Force Space Command, *Strategic Master Plan: FY06 and Beyond,* 1 October 2003.

[11] Air Force Operational Tactics, Techniques and Procedures 2-3.4, *Joint Space Operations Center,* 20 January 2006, 1.

[12] The Laws and Customs of War on Land (Hague IV); October 18, 1907 Annex to the Convention Regulations Respecting the Laws and Customs of War On Land Section I on Belligerents has criteria for qualification of belligerents which basically require a person to be a member of a recognized army to be qualified as a belligerent and encompassed within the laws, rights, and duties of war.

[13] General Lance W. Lord, "Introduction: Space Support to the Warfighterm," *High Frontier* 1, no. 4, 2.

[14] Potential new systems that may be assigned to 50 SW include: SBSS, WGS, AEHF, TSAT, GPS IIF, GPS III, SR, TacSat, JWS Sytems, CAV, Kinetic force applications systems, SBL.

[15] Air Force Space Command, *Enabling Concept for Space Command and Control Weapon System,* 29 September 2005, 4.

[16] Ibid., 5.

[17] Ibid., 13.

[18] Col Mike McPherson and Maj Rhonda Leslie, "SISP Provides Big Space Picture," *High Frontier* 1, no. 1 (Summer 2004): 26.

Building a Better Space Picture

Lt Col Walter S. Chai, USAF
Chief, CCIC2S Branch, Directorate of Requirements
HQ AFSPC
Mr. Shane C. Morrison and Mr. Eric J. Todd
The MITRE Corporation

The alert window was flashing on the Global Information Services (GIS) cell workstation in the Joint Space Operations Center (JSpOC). The insistent beeping caught the space cell chief's ear and he quickly turned toward the source of the noise. His eyes narrowed slightly as he read the incoming SIRS alert on the Integrated Space Picture (ISP). SIRS was the satellite communications (SATCOM) Interference Response System and one of the deployed field units had just sent an alert that it detected radio frequency (RF) interference on one of the channels it was monitoring. The cell chief asked one of the GIS staff to query the online database of SATCOM channels to look up who was using the affected channel. They noted this type of interference had not been previously seen on this channel. The captain pulled up a 3-D visualization of the geosynchronous belt on the ISP to see what other communications satellites were positioned in that part of the world. He postulated what the impact might be if the theater J6 had to reallocate channels to work around the interference. He also checked the Space Effects Environmental Forecast System for any solar radio burst warnings in effect that could explain the RF interference. Finding none, the officer used the ISP collaboration services to chat securely with the SIRS command node to relay the environmental assessment. In turn, he queried SIRS as to when a geolocation of the interfering signal might be available. Once the GIS cell had a solid fix on the interference, the JSpOC Director could better assess if this was unintentional electromagnetic interference or something more nefarious.

Integrated Space Picture Context

Converging atoms often share their electrons in covalent bonds to form a molecule with different properties than its constituent atoms. Similarly, the domains of command and control (C2) and Space Situation Awareness (SSA) must combine to share data and information in order to create a complete space picture. Figure 1 illustrates this concept as a synthesis of an Integrated Space Picture produced by the intersection of the C2 and SSA domains. The ISP, at the juncture of SSA and C2, provides C2 operators and planners with the tools needed to visualize the SSA data and information being produced. Without the ISP, the SSA information is only available to the C2 domain in segregated formats and products resulting from multiple applications requiring manual assembly of the space picture. Figure 2 is a notional ISP example showing a three-dimensional global view of earth with an area of interest (AOI) overlay.

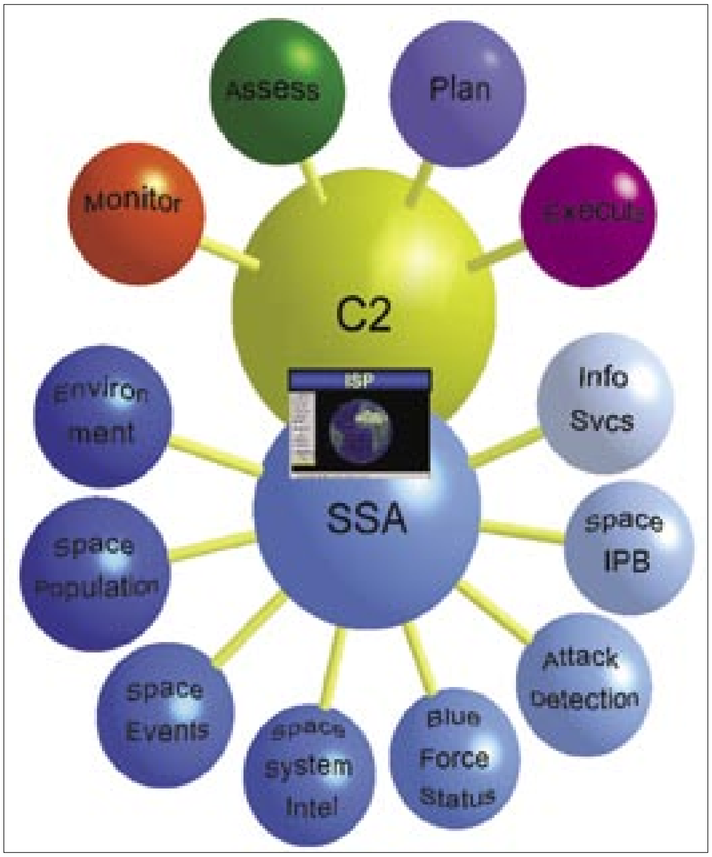


Figure 1. The ISP is a synthesis of C2 and SSA.

The broader and emerging concept of SSA encompasses the use of *intelligence* sources to provide insight into adversary space operations, *surveillance* of all resident space objects, the detailed *reconnaissance* of specific space assets, monitoring and analysis of the space *environment*, and *monitoring* the health and status of cooperative space platforms (US military, national, civil, commercial, and allied). It also includes the command, control, and communications (C3), processing, analysis, and dissemination, and archival used to accomplish these activities. Additionally, SSA provides the foundation for counterspace.[1]

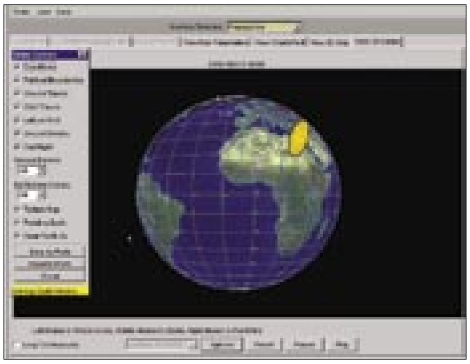


Figure 2. ISP Global View with AOI shown.

Data sharing and fusion was illustrated in the opening scenario where a sensor, like SIRS, detects interference on a Department of Defense communication satellite that could be indications of a hostile action. Determination of intent is the responsibility of decision makers in the C2 domain who will perform the attack assessment; therefore, SIRS must pass the interference detection and characterization information to the C2 system. The C2 system is monitoring its environment looking for specified conditions that will cause it to alert a human when said conditions are met, as in this case, receipt of a SIRS message. The C2 system with its ISP allows the C2 operator to see the interference event in a global context rather than as an isolated event. This facilitates assessment about the nature and impact of the event and allows for sound decision making with respect to response options and warning of other important space operations. Furthermore, the C2 system assists a C2 planner to develop courses of action (COA), which rely on other SSA data for discerning enemy intentions and possible COAs. The subsequent plans and orders will also need SSA in the form of SSA information services like *deconfliction* in order to avoid fratricide or collateral damage to non-combatant assets.

Similarly, SSA is reliant on the C2 domain as a reporting source for the status of blue (friendly) space assets. The status of Blue Forces including operations capability and system capability forms the blue space order of battle and, along with the red and gray space, is an SSA product available to authorized users. Command and control is also required to form task orders and plans to orchestrate the SSA sensors, displays, and personnel in order to collect relevant SSA data.

An Integrated Space Picture – The Problem

Today there is no single comprehensive and consistent view of the space situation. A variety of SSA data exists, but it is often at multiple security levels and is hard to find, access, and/or search. Multiple applications exist at various locations like USSTRATCOM's Global Operations Center (GOC), JSpOC, Space Control Center (SCC), Global SATCOM Support Center (GSSC), and Air and Space Operations Centers (AOC) to assemble a space picture. The rudimentary space picture of today is assembled manually by the JSpOC using MS Office tools; the effort is very labor-intensive and results in a static product. Dissimilar applications can provide contradictory results or show inconsistent aspects of the situation. Furthermore, information rarely is available in real-time to support time sensitive events. SSA information systems are mostly stove-piped with information stored on disparate and segregated systems. Even applications on a single system are typically not integrated, often containing duplicate or even contradictory information. These limitations obstruct the ability to construct relevant comprehensive situation awareness and knowledge that commanders, operators, planners, and warfighters need to perform their missions effectively.

An Integrated Space Picture - Today

Using Air Force Space Command (AFSPC) Directorate of Plans and Requirements (A5) funding, the first iteration of an ISP was demonstrated at the 2004 Joint Expeditionary Forces Experiment (JEFX) under the moniker "SISP," short for Single Integrated Space Picture. SISP is an evolution of the Space Battle Management Core System, a Space C2 system with client software currently deployed in AF AOCs and Army command centers.[2] Space Battle Management Core System (SBMCS) was originally developed for JEFX 99 and 2000 using AFSPC Jumpstart funds as a pathfinder for future Space C2 architecture.

Lockheed Martin

In JEFX 04, SISP successfully demonstrated net-centric information sharing with the SIRS system via the Secret Internet Protocol Router Network to receive and display SIRS electromagnetic interference (EMI) data for an exercise event. The success led to the decision by General John P. Jumper, then Air Force Chief of Staff, to fund a SISP operational leave-behind under the Warfighter Rapid Acquisition Program. SISP version 1.0 will be deployed in mid-2006 to the GOC, JSpOC, HQ AFSPC Space Operations Squadron, the Falconer AOCs (5+1+1), and current SBMCS client users. SISP 1.0 will have the following top-level capabilities:

- EMI alerting
  - Display SIRS alerts for notifications and geolocation of SATCOM interference
- Force status reporting
  - Display status changes received through the Mission Critical Reporting System (MCRS) to include visual and audible alert notifications
  - Display SATCOM (DSCS) operations status. Baseline scalable to permit expanded data interfaces.
- Space Order of Battle
  - Access to red, gray, and blue space order of battle information; mission status; and mission type
- Space Common Operational Picture Exploitation System (SCOPES)
  - Primary modeling and simulation tool to visualize satellite coverage patterns, constellation changes, and satellite overflight
- Navigational accuracy prediction tool
  - Provides prediction of the accuracy the GPS system will provide to a user at specific times and locations in the future based on the geometry of the GPS constellation and other factors

Space Command and Control Weapon System

AFSPC and Electronic Systems Center (ESC) are developing an Integrated Space Picture as part of the Space C2 Weapon

System (SpC2WS). The SpC2WS is a material solution resulting from the need for automated solutions to (1) monitor the space situation and all space forces, (2) assess space situation and operations, (3) plan courses of action and mission tasking, and (4) execute space operations by disseminating orders and information. SpC2WS is currently a sub-program within the Combatant Commanders Integrated C2 System (CCIC2S) program. CCIC2S is an AFSPC program to realize the fixed C2 nodes requirements to support the Commander, North American Aerospace Defense Command and the Commander, USSTRATCOM. For USSTRATCOM, it establishes the capabilities to command and control its service components, space wings and units in support of the space operations mission.[3]

In 2005, AFSPC re-organized its Space C2 Management Process to overcome a perceived lack of organizational focus on Space C2 within the command in order to deploy capabilities faster. The charter of the Space C2 Management Process is to define, validate, and prioritize requirements for the SpC2WS and any segments or elements mandated for use in joint space operations.[4] The management process co-led by AFSPC/A3 and 14 AF/CC covers three levels of authority: the Space C2 Working Group, action officer level; the Space C2 Integrated Product Team, O-6 level; and the Space C2 General Officer Steering Group. Matrix support to the A3 and 14th Air Force is provided within HQ AFSPC by the FM, A2, A5, A6, and A8 directorates, as well by the Space Warfare Center (SWC), Space and Missile Systems Center (SMC), ESC, and the Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC). The Space C2 Working Group may include joint and other service membership to maintain a joint focus throughout the requirements management and system development process.

The principal requirement for SpC2WS is the creation of an Integrated Space Picture. As a primary part of the SpC2WS, the ISP is responsible for consolidating SSA information. The ISP will provide an integrated depiction of the space situation predominately in support of the monitor phase of the C2 process. To an extent, it also supports the assess and plan phases.

Capabilities and Content of Integrated Space Picture

The fundamental purpose of an operational picture is to fuse information from all relevant sources and construct a comprehensive and integrated picture of the battlespace to support accurate assessment and actionable decision-making. The ISP, as a space picture primarily for the operation level of warfare, will provide an integrated depiction of the space situation including the status of forces. The key objectives of the ISP are to:

- Improve the effectiveness of command and control of space forces by:
  - Providing relevant dynamic SSA information for effective decisions
  - Reducing the ambiguity and improve the credibility of the data currently available to Space C2 decision-makers
  - Improving the response time to assessment
- Integrate information about space capabilities and effects horizontally and vertically across all theaters and echelons of command
- Be the authoritative source for knowledge about global and theater space operations to combatant and component commanders and other users.
- Provide information and services that are trustworthy, secure, reliable, and available.
- Provide information and service that are easy to access, understand, use, and tailor to meet specific mission requirements.
- Be compatible with other global C2 and intelligence, surveillance, and reconnaissance (ISR) capabilities to enable integration into global and theater-specific operational pictures.
- Be easy to scale, maintain, modify, update, verify, and control the system configuration.

Monitoring of SSA Information

The creation of situation awareness starts with the collection of data relevant to maintaining a comprehensive picture of space and the relevant global and regional battlespace. This information comes from a large variety of sources including C3 and Battle Management systems, plus intelligence, surveillance, reconnaissance, and environmental (ISR&E) sensor systems. The ISP must integrate this ISR&E data with information as to the status and intent of blue (including national and civil), red, and gray space forces to allow the user to monitor the space situation and answer questions required for informed assessments, COA development, and effective decision-making.[5]

The status of Blue Forces including the operational capability and mission readiness is important to assessing the availability of assets to support planned missions and the impact on current missions. This would include status of satellite systems, ground systems and networks, launch systems, and future systems supporting Responsive Space Operations assigned to theater forces. The ISP must also monitor blue force order of battle; how blue force assets have been apportioned and assigned; what their mission and capabilities are; and what their current and planned tasks are. Maintenance and launch schedules, predicted outages, and the readiness of spare and augmentation assets are also relevant to assessing the availability of assets to support missions in the future.

Monitoring the location, orbital characteristics, activities, and disposition of all space objects (including Intel information on vulnerabilities) is important to being able to characterize space events and assess their impacts, warn of potential hazards, deconflict operations, and understand the ability of specific space assets to support a specific tasking. Monitoring space event *indications and warnings* and notifications of possible attack or RF interference is essential to assessing or predicting the impact to current and future space operations. Monitoring the space environment provides information as to potential operating conditions and potential interference or threats to space assets.

In addition, intelligence information on the status and intent of red and gray forces is important to understand potential threats, strategy and intent of red forces, and centers of gravity. This information is also important for identifying and evaluating courses of action.

Data Fusion

In order to present a comprehensive operational picture, the ISP must fuse information from many different ISR&E data sources. *Data fusion* is the process of aggregating, associating, correlating, and evaluating data from multiple sources to produce information with added value or quality not evident in the input data. Fusion combines information from multiple sensors and related information sources to achieve more specific inferences than could otherwise be achieved with a single sensor or source alone. These inferences are used to improve estimates of the situation that in turn allows improved ability to respond effectively.

Knowledge about a situation is built by inferring relationships between separate pieces of information. Information can be aggregated in tabular or graphical form to show or discover relationships. For example, geographical relationships can be shown and discovered through information overlays on a georectified map display. This allows visualization of geometric relationships such as look angles between a space track ground site (e.g., Maui deep space optical site) and satellites as they pass overhead.

Fusion of SSA information occurs at different levels in the processing and exploitation architecture. Between receiving raw sensor data and assessing the effectiveness of space operations lays a multi-stage fusion process. Fusion at one stage feeds the fusion process at the next stage. These stages conduct fusion at increasing levels of abstraction. Five functional levels for data fusion are defined in a revision of the Joint Directors of Laboratories (JDL) model for data fusion as shown in table 1.[6]

Level	Description	Example
0	Sub-Object Assessment	Sensor Fusion for Precision Tracking
1	Object Assessment	Characterization for Space Object Identification
2	Situation Assessment	Space Situation Assessment
3	Impact Assessment	Space Mission Impact Assessment
4	Performance Assessment	Space Operational or Effects Assessment

Table 1. The functional levels of Data Fusion.

Sensor fusion providing signal and feature characterization (Level 0) would typically be performed at sensor processors. An example is the correlation of multiple observations to provide improved precision tracking of an object in space. The Level 1 fusion is oriented toward combining information about single objects; for example, refining Space Object Identification from the fusion of radar and optical information with electronic or signal intelligence to yield intelligence about an object and its functions. Several intermediate processing capabilities feeding the ISP perform Level 2 and 3 fusion specific to space object cataloging, space event notification, defensive counterspace event assessment, and space and terrestrial environmental conditions. These systems will help the ISP support situation and impact assessments (Levels 2 and 3). Fusion performed by ISP is focused on identifying relationships between entities, events, conditions, and other information. Fusion at this higher level of abstraction builds the situation level assessment, impact level assessment, and performance level assessments. An example would be fusing information from an anomalous event, location and characteristics of satellites, satellite vulnerabilities, considering space environmental conditions, to generate hypotheses about the event, its cause, possible intent, and predicts impacts to operational missions. At Level 4, ISP also supports assessment of the effectiveness of mission operations and space effects.

The ability to perform data fusion in the future will be built from several advanced techniques employing, where appropriate, intelligence agents, genetic algorithms, neural networks, and decision theoretic approaches such as Bayesian inference. These applications would be integrated within a service-oriented architecture including net-centric information, visualization, and collaboration services.

Assessment

Knowledge of the current and predicted future situation is the result of the assessment founded on analysis and interpretation of the information collected during the monitor function. The ISP will support processes that assist in the analysis and assessment of the information collected. At a minimum, the information provided includes what support is needed by the combatant commanders, the capability and status of assigned and attached forces, assessment of vulnerabilities and potential threats, detection and assessment of any active threats to friendly space or terrestrial forces/operations, the nature of adversary's intent and the adversary's capabilities and vulnerabilities. Assessment is conducted in the context of current commander's intent and guidance, strategy, mission objectives, planning, and tasking.

There are several different types of assessments that are essential to developing knowledge about the battlespace situation and formulation of courses of action for the Commander, Joint Space Operations (CDRJSO); Commander, Joint Functional Component Command for Space and Global Strike (CDR JFCC SGS); and combatant commanders. One example is a Space Mission Impact Assessment necessary when there is space event or a change in the state of health of an operational satellite. Verifying the event is the first step in assessing the impact of that event on space missions. The ISP must support the determination and assessment of the nature and impact of events in the battlespace. Impacts can result from changes in solar environmental conditions or events, incidental interference from RF or laser illumination, or deliberate space attack on a system.

- The impact of environmental factors on space operations must be taken into consideration during strategy, planning, and operations decision cycles.[7]
- An actual failure of one or more components of a satellite is another form of 'space event.'

SFC David Dismukes, Third US Army Public Affairs

Third Army's Coalition Forces Land Component Command Operations Center.

Plan and Execute

The information from the monitor and assess functions supported by the ISP must feed into the planning and analysis services and applications including strategy-to-task, course of action generation and development, and workflow and automated checklist functions. These planning functions should be accessible from the same tool menus as the ISP functions and where appropriate through drill-down or popup menus.

ISP System Characteristics

Without the ability to fuse the data, new SSA sensors are of limited use to the decision-maker. Consequently, the two most pressing needs are:

- A net-centric infrastructure to enable easy access to C2 and SSA information
- The ability to fuse and integrate the information currently available

The success of an ISP is tied to the ability to pull information from many sources. The flexibility afforded by the ISP allows dynamically associating different information in new ways to establish and visualize new information relationships, and hence form new knowledge. This requires ISR and environmental sensors and information systems that are interoperable, share a common vocabulary, and are accessible over reliable networks. Success also requires the ISP to be able to share information and provide an integrated and comprehensive picture using a set of tailorable visualization services.

Access to new and existing sensor systems and other data sources will employ a net-centric service-oriented architecture. The ISP will be part of the Global Information Grid (GIG) and will be an integral element of the net-centric enterprise supporting the JSpOC and other global strategic C2 and theater C2 elements. The ISP as well must provide net-centric information services to support the development of user-defined operational pictures and the integration of space information into other C2 and battle management functions. It must also support automated information sharing with subordinate units, combatant commands, service operations centers, federal/civil users, and joint task forces.[8]

Moving to a net-centric architecture should lead to better access to SSA data for current users and provides the ability for unanticipated users to access SSA data without the need for programmatic changes. The C2 SSA Community of Interest (COI) was established to provide common vocabulary and semantics for data shared across the Space C2 and SSA communities and a data strategy for information and information services. This will enable the efficient sharing of volumes of information that are otherwise not accessible to key members of the space community.

The ISP will be developed using a service-oriented architecture that incorporates C2 and SSA COI services. Users will be able to build services and applications that allow them to process the data and present it in a User Defined Operational Picture (UDOP). The UDOP software is essentially a set of COI services enabling the construction of tailored operational and tactical pictures. The ISP will consist of one or more UDOPs that provide a means through which a common view of the battlespace can be constructed, and will support personally tailored views to meet different user information requirements.[9]

In some cases, situation awareness will require the user to understand new situations and require the ISP to build new knowledge about those situations. We cannot predict all emerging situations or new ways of looking at a situation. Therefore, the ISP must be flexible and tailorable in several ways. We need the ability to dynamically associate different information in new ways, establish and visualize new information relationships and form new knowledge. The UDOPs comprising the ISP and its supporting SSA COI and visualization services must have the flexibility to dynamically integrate and fuse a wide array of information from a broader set of relevant sources. The ISP must also allow the user to tailor the depiction of new information to be able to visualize new relationships suitable to an emerging situation.

This degree of tailorability will not be achieved easily. Listed below are features intended to enhance knowledge while reducing operator information overload.

- Selectable association, visualization, and dissemination of information.
- Automated update of underlying information to ensure a timely and accurate picture.
- Filtering, search, subscription, and collection of source information.
- Change detection (driven in part by space event notification), trend analysis, and user notification based on complex conditions.

As an integral part of the Space C2 WS, the ISP will be accessible from the same *common desktop display* as other Space C2 WS applications such as COA and decision support aids. The ISP will be integrated with workflow management and collaboration services.

The ISP, as an element of an emerging net-centric enterprise, will utilize a *spiral development* process. As new capabilities are developed and fielded, they will be able to utilize other net-centric enabled services. In many cases, they will also need to be compatible with legacy, point-to-point systems.[10] Develop-

"I want to know as much as I can about everything that is up there, friend, foe, or otherwise." - Lt Gen Kevin P. Chilton

ment of the ISP will also require synchronization with supporting SSA capabilities and initiatives.

An Integrated Space Picture – The Vision

"I want to know as much as I can about everything that is up there, friend, foe, or otherwise," said Lt Gen Kevin P. Chilton, CDR JFCC SGS, which succinctly states the *raison d'etre* for the ISP. The JSpOC implementing directive assigns responsibility to the CDRJSO to "maintain a space picture as the operational manager for SSA," and to "ensure the space picture is available to combatant commanders [for] planning, decision-making, and situation awareness."

The long-term vision for the ISP is to build an accurate and timely picture of the space situation by autonomously fusing data from all relevant sources to quickly arrive at a comprehensive picture of what is presently happening, what are the probable causes, what the impacts are, and what are possible courses of action. A robust ISP will allow warfighters to assess, plan, and respond faster than the adversary, that is, to operate inside of their decision loop.

Notes:

[1] Air Force Doctrine Document (AFDD) 2-2.1, *Counterspace Operations,* 2 August 2004, 4.

[2] The label "SISP" has been used synonymously with the Space C2 Weapon System currently under development, which includes capabilities for monitor, assess, plan, and execute functions. We will use the term "ISP" to refer to integrated services and views of SSA in support of the monitor and assessment functions of the SpC2WS.

[3] Deputy Chief of Staff for Air & Space Operations, HQ USAF, *Combatant Commanders Integrated Command and Control System (CCIC2S) Operational Requirements Document (ORD),* 1 August 2003, 4. (Secret) Information extracted is unclassified.

[4] Director of Air and Space Operations, Air Force Space Command, *Space Command & Control Management Process Charter,* draft, 1 March 2006.

[5] Director of Air and Space Operations, Air Force Space Command, *Enabling Concept for the Space Command and Control Weapon System,* 29 September 2005, 9.

[6] Alan N. Steinberg and Christopher L. Bowman, "Rethinking the JDL Fusion Levels," NSSDF JHAPL, June 2004.

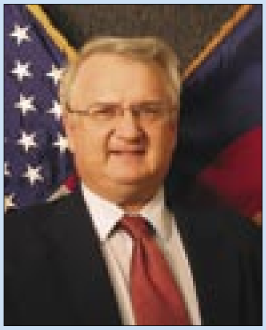
[7] AFSPC/XO, *Enabling Concept for SpC2WS*, 12.

[8] Ibid., 15.

[9] Mark Kuzma, "User Defined Operational Picture C2 COI Services, DISA Enterprise Applications" (briefing, September 2004).

[10] AFSPC/XO, *Enabling Concept for SpC2WS,* 16.

Lt Col Walter S. "Walt" Chai (BS, Electrical Engineering, Carnegie Mellon; BS, Meteorology, Texas A&M; MS, Systems Management, University of Southern California) is the Chief, Combatant Commanders Integrated Command and Control System Branch, Directorate of Requirements, Headquarters Air Force Space Command, Peterson Air Force Base, Colorado. Lieutenant Colonel Chai has served in acquisition positions in various organizations including the Office of the Secretary of Defense, Secretariat of the Air Force, Headquarters Air Force Space Command, and Air Force Material Command. He is Acquisition Level III certified in Program Management and System Planning, Research, Development, and Engineering. In addition, he has served in operational weather positions in the US and the Republic of Korea.



Shane C. Morrison (BA, Mathematics, University of Colorado; MS, Computer Science, Santa Clara University) is a Lead Engineer for The MITRE Corporation currently supporting the Directorate of Plans and Requirements, Headquarters AFSPC. Mr. Morrison has led several AFSPC technical studies on future space C3 capabilities including a recent study on the Integrated Space Picture. He has worked various requirements engineering efforts and several facets of space and theater systems integration. Mr. Morrison was a Test Director for Electronic Systems Center (ESC) for strategic missile warning and Global Electro-optical Deep Space Surveillance (GEODDS). Prior to MITRE, Mr. Morrison was an engineering manager on distributed and real-time embedded software systems at GTE and Litton. His background includes the development of C4, ELINT, SIGINT, and Threat Warning Systems for AF, Navy, NSA, NOAA, and German Air Intelligence.

Eric J. Todd (BS, Biochemistry, Texas A&M University; MS, Space Operations, University of Colorado) joined the MITRE Corporation in 2003 where he is supporting the CCIC2S Branch, Directorate of Plans and Requirements, Headquarters Air Force Space Command. Mr. Todd is working on operational requirements and enterprise architecture for Space Command and Control initiatives such as CCIC2S and Space C2 Weapon System. While supporting the Space Situational Awareness Integration Office (SSAIO), Mr. Todd helped to shape the national SSA modernization and investment strategy plan. He served on active duty with the US Navy as a Naval Flight Officer flying the S-3 Viking on anti-submarine warfare missions in the Indian Ocean, Atlantic, and Mediterranean theaters. Mr. Todd also served with US Space Command as an Orbital Analyst in the Space Surveillance Center at Cheyenne Mountain Air Force Station, Colorado.

ICBM Command and Control – History to Future

Maj Lance K. Adkins, USAF
Command Lead, ICBM Applications Programs
HQ AFSPC

Historical Background: Minuteman I and II

Through years of service, US Intercontinental Ballistic Missiles (ICBMs) have undergone steady and incremental modernization resulting in improved functionality through the incorporation of new technology. However, significant capability improvements generally have required major weapon system upgrades. Nowhere is this more true than in the realm of command and control (C2).

In the earliest ICBM systems (Atlas and Titan), weapon system control was quite direct. Launch control centers were collocated with the launch silos proper. There were no obstacles to running thick bundles of wires and cables through the few hundred feet of tunnel and conduit required.

The development of the Minuteman concept from 1958 to 1962 forced a new look at the control functionality demanded by geographically separated launch facilities (LFs). Whereas collocated missile systems could be guarded and commanded relatively easily within the confines of a secure area, remote LFs required unprecedented innovations in robust digital networking, security perimeter protection, and reliability. With significant modification, these same systems originally emplaced in the early 1960s are still in service today. This first iteration of the Minuteman C2 System was groundbreaking, incorporating a digital network capable of relaying commands from the launch control center (LCC) to individual LFs and returning status messages as needed. This was facilitated by laying tens of thousands of miles of cable that comprised the Hardened Intersite Cable System (HICS) between the launch control centers and launch facilities.

HICS, intended to be protected against acts of man and nature, united the five LCCs and 50 LFs of each missile squadron. It allowed any LCC in a squadron to monitor and command any LF desired within the squadron and was at least nominally survivable against the effects of a nuclear attack. The original Minuteman system did not use encryption or authentication, relying instead on the robustness of the cable's outer casing and maintaining an overpressure of air in the cable for signal protection. An interloper (or more likely a farm implement) cutting into the cable would cause a cable pressure alarm at the owning LCC at which point the duty crew would initiate a security response and investigation of the root cause.

When originally conceived, the concept of an internet-like, packet switched network was still several years in the future, thus the network topology differed significantly from what might be built today.[1] The Minuteman weapon system needed a redundant network that would minimize the average distance between a given point and a set of surrounding points. The result blended features of tree and hub-and-spoke topologies, constructed around the LCC with cables running to multiple LFs and to other LCCs. In practice, it took the form of four radial cables extending from the LCC to a cable ring encircling the LCC at some distance.[2] LFs were connected to branches off this ring and, in some cases, to adjacent rings. This system afforded each LCC the capability to monitor any LF in its squadron of 50. In the Minuteman I system, the missile's own NS10 guidance and control (G&C) computer was integral to the command and control system—receiving, processing, and executing commands transmitted by the LCCs. Additionally, this network (a "strongly connected" network, meaning that it is possible for signals to travel from each node in a squadron to any other node) afforded the system a reasonable measure of redundancy in the event of cables being severed, either by accident or by attack. Finally, commands transmitted from any LCC are repeated by every other node on the network. This "flooding" concept makes the network highly redundant and survivable. As a result, HICS, originally emplaced in the early 1960s, is still in service today, retaining its 1.3 Kbps data rate in the current Minuteman system.

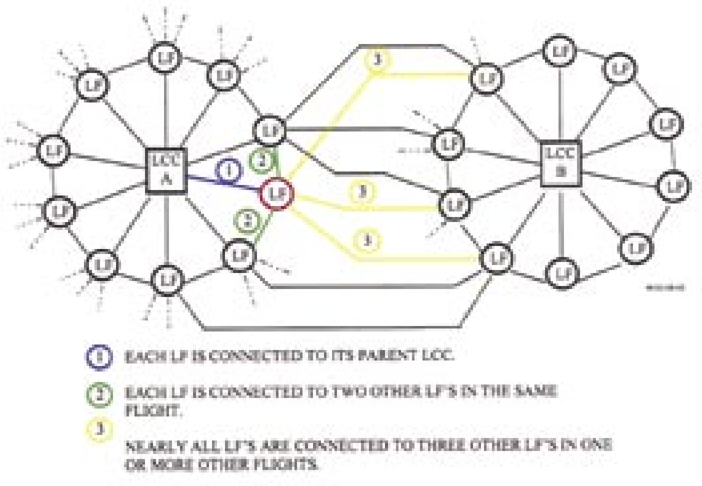

LF
LCC A
LCC B
1
2
3
1 EACH LF IS CONNECTED TO ITS PARENT LCC.
2 EACH LF IS CONNECTED TO TWO OTHER LF'S IN THE SAME FLIGHT.
3 NEARLY ALL LF'S ARE CONNECTED TO THREE OTHER LF'S IN ONE OR MORE OTHER FLIGHTS.

Figure 1. HICS cable runs between LCCs and LFs.

The original Minuteman I guidance system was not capable of being remotely retargeted because of the need to align the missile's internal stabilized platform with a silo-mounted precision North reference. This required that the azimuth of the missile also be aligned to precision North for greatest accuracy. Thus, the missile and its autocollimator (the device used to align the missile guidance to the precision North azimuth) were required to be physically rotated to align to a new target—clearly a challenging process to accomplish under strict time constraints. However, this relatively crude means of aligning missile to target placed very modest requirements on the bandwidth required of the cable system.

In order to achieve the greater levels of versatility required by

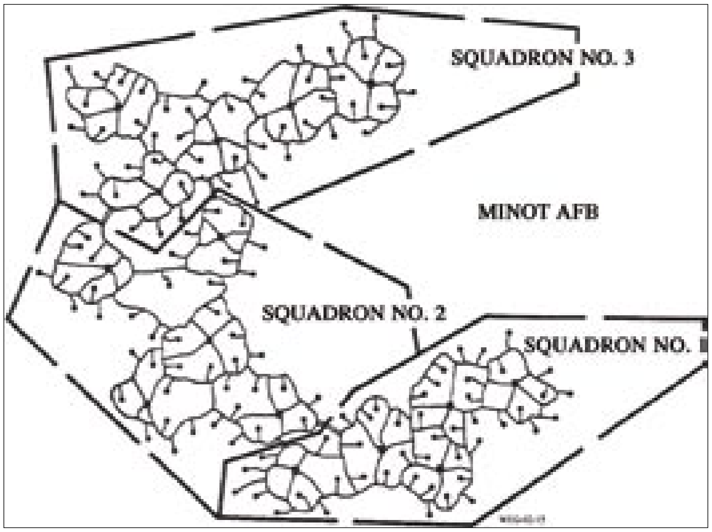


Figure 2. HICS cable layout of Minot AFB, North Dakota, a WS-133A-M system.

Strategic Air Command planners, provisions had to be made for remote retargeting. This upgrade was made in the Minuteman II, which featured the much more sophisticated D37 G&C computer to handle new error correction functions for improved accuracy as well as the faster processing and greater throughput necessitated by the remote retargeting capability. According to the designation system of the time, the original weapon system (designated WS-133A) was redesignated WS-133A-M (or A Modified). Additionally, a new variation on the Minuteman weapon system was developed by Sylvania and designated WS-133B (or the Minuteman II Command Data Buffer). This variant was installed at Grand Forks AFB, North Dakota and in the 564th Missile Squadron at Malmstrom AFB, Montana. Instead of a redundant cable system, the WS-133B used a non-redundant cable system that operated with an independent medium frequency radio that essentially duplicated the command transmission and status monitoring functions of the HICS. A highly survivable architecture in theory, the newer WS-133B was so different from the older WS-133A-M that there was little commonality between the two systems.

A further major change to the Minuteman II C2 system occurred in 1974-1975 when the Software Status Authentication System (SSAS) was incorporated. This change allowed for cryptographic authentication of commands from the LCC and status messages from the LFs. This modification complicated the problems faced by anyone wishing to intercept or spoof traffic moving across the HICS.

Present System: Minuteman III

A desire to improve the accuracy afforded by the Minuteman II led to the Minuteman II Post Boost Control System (PBCS) study, which, in turn, led to the Minuteman III. Minuteman III added a larger third stage motor and a Multiple Independently Targetable Reentry Vehicle capability. Accuracy was greatly improved as a result of the PBCS, which virtually eliminated the downrange error component caused by imprecise Stage III thrust termination. Additionally, a high beta reentry body (one having a finer, more pointed cross-section) was developed that significantly reduced atmospheric dispersion during reentry.[3] Despite these improvements to the missiles themselves, the Minuteman III used the same command and control systems as the older Minuteman I and II. This is not to say, however, that significant changes were not made to the C2 system during this upgrade.

The most sweeping modification to the C2 system since its inception occurred with the Improved Launch Control System (ILCS) upgrade that took place in 1973, starting with Wing V at F. E. Warren AFB, Wyoming. ILCS was needed in order to take advantage of the Minuteman III's remote data change (RDC) capabilities, which were collectively incorporated into the Command Data Buffer (CDB) configuration. Updating to this configuration required significant changes to both the operational flight and operational ground programs as well as to the LCC and LF equipment.[4] In order to prevent unauthorized data change (a potential sabotage method), the RDC protocol employed a second LCC to continually cross-check the information being transmitted by the primary LCC. Any mismatch would result in an abort, which crews would have to cross-check. Significantly, full encryption (as opposed to authentication only in the SSAS upgrade) was now incorporated into the system, and engineers also made significant changes to the G&C system, making the system more capable of handling the kinds of shocks and motion that might result from a nuclear attack. Eventually, five of the six missile wings—regardless of whether they were equipped with Minuteman II or Minuteman III ICBMs—were upgraded to the ILCS standard, with the 44th Missile Wing at Ellsworth AFB, South Dakota, being the sole remaining SSAS Minuteman II wing until it was inactivated in 1994.[5] One disadvantage to CDB was that the encryption scheme slowed the effective data rate of the HICS, making commands and responses somewhat more lethargic from the standpoint of the operator though few today would argue the necessity of strong encryption to nuclear surety.[6]

The most recent and significant upgrade to Minuteman C2 since ILCS has been the Rapid Execution and Combat Targeting (REACT) modification. Essentially computer workstations interfaced with the existing weapon system, REACT was installed at Malmstrom AFB, Minot AFB, and F. E. Warren AFB, during the mid-1990s and allowed for superior integration of communications, weapon system, and retargeting functions at a single two-man console that offered a much improved man-machine interface. Numerous other improvements also came as a result, including data logging, a greater degree of automation in retargeting operations and improved processing of Emergency War Order messages. As sweeping as the changes were to crew operations, the actual changes to the weapon system were less comprehensive. REACT emulates, expedites, and automates the functions performed by the older command consoles but does not otherwise upgrade the C2 network. In order to see dramatically greater performance, the actual C2 infrastructure would have to be upgraded.

In the near future, there will continue to be changes to the Minuteman C2 system, though they will almost certainly remain incremental upgrades rather than wholesale revisions. The first upgrade is known as the ICBM Cryptographic Upgrade (ICU). This involves replacement of the KI-22 cryptovariable used to authenticate and encrypt data moving through the HICS. The KS-60 is an evolved version, designed to be a form, fit, and function replacement for the KI-22, but with a stronger cryptographic scheme and a variety of enhancements, including the ability—following the as-yet unfunded Increment II modification—to have its codes remotely changed, thus saving a considerable number of maintenance hours. The Increment I implementation of KS-60 will reach full operational capability by 2009.

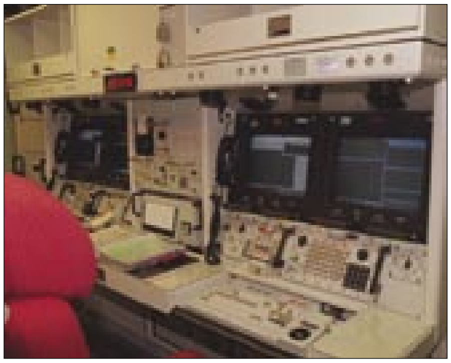


Figure 3. Typical REACT console.

Furthermore, there is a plan afoot to emplace remotely-controlled cameras on LFs to assist in tactical response to security alarms. Designed to address concerns about the lack of updated tactical information available to Alarm Response Team Security Forces, the Remote Visual Assessment (RVA) system (nicknamed "Prairie Hawk") would comprise one or two remotely controlled day/night capable pan-tilt-zoom surveillance cameras on each LF. The concept as currently envisioned uses an 802.11-based wireless internet protocol network, with repeaters mounted on existing structures and purpose-built towers throughout the missile field. Such a system should have fairly significant additional bandwidth and may form the basis of secondary capabilities, such as a means of transmitting data from a variety of portable devices and possibly—following an extensive NSA certification process—form an integral part of the Minuteman C2 architecture. If funded, Prairie Hawk is planned for full operational capability in 2014.

Future Development—the Land-Based Strategic Deterrence Command, Control, Computers, and Communications Study and Minuteman IV

In September of 2005, Air Force Space Command completed the Land Based Strategic Deterrent (LBSD) Analysis of Alternatives. A key part of this study was a Technical Analysis of comand, control, computers, and communications (C4) alternatives conducted by the MITRE Corporation. This analysis examined various technologies from those for enhancing the legacy HICS system to complete replacements for the C4 architecture. These improvements would be integrated into the new Minuteman IV weapon system, planned for deployment in existing Minuteman silos.

One factor that has to be taken into account when Minuteman C4 upgrades are discussed is the expense associated with any sort of HICS replacement. All told, the three remaining Minuteman-equipped space wings have 32,443 miles of buried cable.[7] The cost of replacing this cable with a higher data rate cable is very high (estimated as costing $10.86 per foot or around $2 billion total in 1999 dollars) and would likely represent a significant logistical challenge, as the cables extend largely across privately-owned farms and ranches as well as federally-protected wetlands and other such areas. Naturally, one of the key parts of the LBSD C4 technical analysis involved determining what could be done without incurring the cost of a buried HICS replacement.

Another factor to consider is that the form any C4 system eventually takes will be greatly influenced by the capabilities of the missile guidance set developed for the Minuteman IV. A very fast on-board processor with extensive storage capabilities may well require a high data-rate C4 network to realize the ICBM's full potential, since the new guidance-set computer will likely interface more or less directly with the C4 system. GPS or stellar aiding to augment the accuracy of the inertial guidance system may require regular transmission of almanac data or star catalogs that will place even more demands on bandwidth. Therefore, it appears that some kind of upgrade will be necessary if one of these options is chosen.

Three principal alternatives are described in the study: (1) an Enhanced HICS that as been upgraded to achieve transmission speeds greater than 256 Kbps; (2) a full replacement of the HICS cable with fiber optic cable and; (3) a survivable radio frequency wireless network. Excursions to these alternatives include various hybrids of a fiber-optic and terrestrial radio frequency network. The Extremely High Frequency (EHF) waveform was studied to ensure the alternate launch capability.[8]

The goal of all of these approaches is to produce a net-centric architecture for Air Force ICBMs. This is clearly a big step away from the dedicated, hard-wired infrastructure used in today's Minuteman III system, and it would drive significant increases to speed and flexibility of command. For instance, allowing a missile crew to command any missile in a wing or perhaps even in the entire missile force would become possible. Retargeting could be accomplished in real time to hold more targets at risk, and the possibility exists of using survivable mobile command centers that could deploy in advance of hostilities and perform in a role similar to the current Airborne Launch Control System (ALCS), but more quickly, for longer duration, and at a much reduced operating cost. Next generation ICBM C4 could even be integrated into the Global Information Grid (GIG). This would ensure that the ICBM C4 system remains viable for future network development using common components.

Hardened Intersite Cable System Data Rate Upgrade

According to a 2002 study conducted by General Dynamics, HICS cable is not suitable for extreme upgrades to bandwidth and data rate. Its high capacitance values—due largely to use of Polyvinyl Chloride (PVC) insulation—place a cap on how much frequency bandwidth is available.[9] Modern telephone cables have less than 1/3 the capacitance of HICS cable. This, combined with the extreme length of some stretches of cable between repeaters (in one case 41.7 miles), tends to rule out adding Digital Subscriber Line (DSL) technology to the existing network, at least with commercial, off-the-shelf equipment. Repeaters would have to be added to the network to achieve high data rates, though the study concludes that the existing data rate can probably be improved with DSL, potentially yielding from 64 to 128 Kbps.[10] The aforementioned capacitance issues would also tend to prevent the use of newer Ultra Wide Band (UWB) technology over the existing cable.

The installation of repeaters would alleviate many of the problems but also introduce its own—primarily the need to excavate significant stretches of HICS cable and install nuclear-hardened, radiation-shielded, waterproof amplifiers with some sort of power source, most likely external to the HICS system. Such additional components could introduce new vulnerabilities into an otherwise very robust system.

Fiber Optic Hardened Intersite Cable System Replacement

Another option studied by MITRE Corporation is the outright replacement of the HICS with fiber optic cable. This would provide much faster data signaling rates compared to the HICS. Other advantages include the fact that fiber optic cable runs can easily extend over 100 miles without repeaters, are not susceptible to electromagnetic pulse effects and are lighter and more reliable than copper. However, the cost of replacing the existing HICS, to include obtaining easements, trenching, and laying the cable may be cost-prohibitive in the current fiscal environment. Assuming that fiber optic cable could be installed adjacent to the HICS cable, within the current easements, a wide variety of additional capabilities would be achievable, however, such as transmission of retargeting data to entire wings in fractions of a second, sending and receiving of full-motion video from on-site security systems, and reducing the number of LCCs per squadron from five to one.

A further possibility facilitated by higher bandwidth and fiber optics communication is quantum encryption, which relies upon the quantum physical property of entanglement to protect information from snoopers. Using physical properties of photons which Einstein called “spooky action at a distance,” quantum encryption is protected by the laws of physics and would be theoretically unbreakable, regardless of the growth in computer processing power in coming years.[11]

Radio Frequency Terrestrial Replacement of Hardened Intersite Cable System

In an effort to reduce the considerable cost of outright HICS replacement with fiber optic cable runs, the LBSD C4 technical analysis also examined the feasibility of several wireless technologies including free-space optical and several types of radio frequency (RF) technology. There has been a tremendous amount of work and technical innovation in the field of wireless digital communications in the past decade, driven almost entirely by the commercial sector. These innovations, if they could be made acceptable for the ICBM’s peculiar needs, have the potential to revolutionize the ICBM’s operational art by providing a mixture of low cost, high data rates, flexibility, and potential mobility.

The LBSD study looked at four technological artifices to enable a wireless C4 system. For those familiar with the WS-133B weapon system, wireless ICBM C2 is not a foreign concept. However, the techniques described in the LBSD C4 technical analysis are very distinct from the medium frequency radio incorporated in that system.

The first technology examined involves the use of Free Space Optics, or lasers operating through the air. Such systems exploit very high data rates and low probability of interception, but are also affected by atmospheric conditions, such as rain and snow. Furthermore, the longest sustainable link possible without the use of amplifiers is only around 4 km, requiring numerous amplifier stations.[12] A determined enemy might also attempt to dazzle the laser receivers with other lasers or destroy the amplifier stations to take down the links. Hardening such an architecture would be a considerable challenge.

A second technological possibility examined in the LBSD C4 technical analysis is the new wireless networking technology known as WiMAX, or 802.16. This comparatively recent development incorporates high signal rate line-of-sight (LOS) communications as well as non-line-of-sight (NLOS) communications at a somewhat reduced data rate (nominally 160 Mbps for LOS and 75 Mbps for NLOS). Because it is quite new, WiMAX embodies a variety of technologies to improve the robustness of a wireless C2 system, such as built-in error correcting and adaptive modulation. WiMAX ranges are such that, when within the LOS of other nodes, few amplifiers are required. However, as the NLOS range for WiMAX is less than 10 km, additional amplifiers would be required in occluded terrain.[13]

The greatest weakness of this or any other commercial off-the-shelf (COTS) product will always be nuclear hardness. It is not reasonable to ask hardware designed for business to withstand and operate through the sorts of thermal pulse, blast, and atmospheric scintillation that occur during a nuclear detonation. However, there are improvements that can be made to WiMAX equipment that may make it more tolerant of these conditions and as a waveform and standard, WiMAX seems promising, at least for peacetime operations.[14]

A third type of wireless communications examined by the C4 technical analysis team is known as Ultra Wide Band (UWB). UWB uses extremely short pulses of energy and very accurate timing to produce high data rate signals which are capable of penetrating obstacles, immune to multipath interference, and use very low power levels. Since UWB receivers are only “listening” for a signal at specific and very precisely defined intervals, it is also resistant to jamming or spoofing, since the short receiving intervals act like a range gate on a radar receiver, only accepting signals that fall in a certain time difference of arrival parameters while ignoring all else. A spoofing transmitter would therefore have to be collocated with the spoofed transmitter for its signal not to be rejected.[15] This sort of discrimination, combined with low-probability-of-intercept characteristics makes UWB an alternative with great potential, but its relative novelty means that there are many questions that must be answered before it could begin certification for nuclear C2.[16]

The final possible wireless technology that was explored in the LBSD Analysis of Alternatives (AoA) was based on an advanced EHF satellite communications (SATCOM) equipped with a survivable waveform. While this would be highly dependent upon the funding and development of an appropriate satellite constellation, it would have ample bandwidth for current and future needs as well as providing excellent mobility and survivability, especially in a post-attack scenario, where its EHF signal would be capable of penetrating nuclear scintillation effects.[17] The forthcoming Advanced EHF and Advanced Polar satellite programs will provide a strong combination of survivability and bandwidth that could form the basis of a survivable HICS replacement, assuming that sufficiently hardened EHF terminal can be developed. There would be several drawbacks to such a system, however, including relying on the continued funding, development, and support of the required satellite programs and competing peacetime bandwidth priorities. Additionally, EHF requires exposed antennae, which would be difficult to harden and are susceptible to signal attenuation by precipitation.[18] For this reason, the LBSD AoA recommended consideration of hybrid systems that would use EHF SATCOM as a survivable backup to some other, potentially less survivable system, similar to the role of the ALCS system today, but with greatly enhanced capabilities. The net-centric approach to interlinking the various LFs and LCCs with a packet-switched network could alleviate some of these issues, however, since the SATCOM broadcast would only need to be received at one location in order to be propagated throughout the remainder of the squadron (or wing, or force, depending upon the degree of interconnectivity).[19]

Figure 4. Advanced EHF satellite.

Lockheed Martin Corporation

Conclusion

In the final analysis, Minuteman C2 progress will be dictated by both fiscal reality and the direction of technology. The rapid growth of wireless technology and extremely limited fiscal resources may recommend a wireless or hybrid structure. In any event, the engineers who will lead this effort will be challenged to construct a system that is as robust, long-lived, and sophisticated for its time as the original Minuteman HICS. Even in a very different world than the Cold War Era, the US land-based strategic deterrent has long represented a dagger pointed at the throat of the Nation's would-be adversaries, and as such, commends a high value on the capability to destroy or otherwise marginalize them. A fast, reliable and survivable C2 architecture makes these weapons tougher to counter, more effective, and more defensible—all fundamental to deterrence. A highly accurate, land-based, flexible response option for the President will continue to serve the Nation as a credible deterrent force and the C2 infrastructure must grow along with this option to ensure that this capability is maintained.

Notes:

[1] Albert Wohlstetter and Richard Brody, "Continuing Control as a Requirement for Deterring," *Managing Nuclear Operations*, eds. Ashton Carter, John Steinbruner, Charles Zraket (Washington, DC: The Brookings Institution, 1987), 176.

[2] General Dynamics Communications Systems, *HICS Upgrade Study Technical Report* (Ogden, UT: General Dynamics Communications Systems, 1999), 7-8.

[3] R.F. Nease and Daniel C. Hendrickson, *A Brief History of Minuteman Guidance and Control* (Anaheim, CA: Rockwell Autonetics Defense Electronics, 1995), 3-1.

[4] Ibid., 2-21 – 2-22.

[5] Ibid., 3-34 – 3-35.

[6] Lt Col Erik Hoihjelle, interview by the author, 30 January 2006.

[7] *HICS Upgrade Study*, 91.

[8] Shane Morrison et al., *Land Based Strategic Deterrent (LBSD) Analysis of Alternatives (AoA) – Technical Analysis of Communications Alternatives,* MTR Number 05B0000088 (Bedford, MA: The MITRE Corporation, 2006), 7-1.

[9] Ibid., 2-4.

[10] Ibid., 2-18.

[11] Bob Gourley, *Quantum Encryption vs. Quantum Computing: Will the Defense or Offense Dominate?* (Bethesda, MD: SANS Institute, 2001), http://www.sans.org/rr/whitepapers/vpns/720.php.

[12] Morrison et al., *LBSD AoA* 7-7.

[13] Ibid., 7-5.

[14] Ibid., 7-7.

[15] Ibid., 3-30.

[16] Ibid., 7-7.

[17] Ibid., 4-6.

[18] Ibid., 4-8.

[19] Ibid., 4-8.

Maj Lance K. Adkins (BMusic, University of Tennessee; MS, University of North Dakota; MS, New Mexico Tech) is Command Lead for ICBM Applications Programs in the Directorate of Requirements, Headquarters Air Force Space Command, Peterson AFB, Colorado. He oversees efforts for ensuring the preservation of the ICBM industrial base and development of technologies for future ICBM implementations. He has served as India Flight Commander at Grand Forks AFB, North Dakota; Chief of Flight Test and Chief of Training at the 576th Flight Test Squadron ("TOP HAND"), and Space Superiority Section Chief, Directorate of Transformation, Space and Missile Systems Center. Major Adkins is a graduate of Squadron Officer School and the Sandia Nuclear Weapons Fellowship Program.

Space Command and Control

Managing the Integration of Space and Information Operations

Maj Daniel F. Gottrich, USAF
Michael R. Grimaila, PhD, AFIT

> *We should not go to space unless it's the only way we can do a job, or can do it better, or it's cheaper. The global movement of information seems to be the one thing we can use space for that we have not learned how to do on earth.*[1]
>
> - Lt Gen Richard Henry, 1982

Because over twenty years has passed since the establishment of Space Command in 1982, most members of the military are now comfortable with the axiom that space is the fourth realm of warfare in addition to the traditional spheres of land, air, and sea. However, this transition was slow in coming. Even though the Cold War had seen operations brewing in space since the late 1950s, it took the establishment of a separate unified military command, the United States Space Command, or USSPACECOM (and, in 2001, a scathing Congressional report threatening to establish a separate space service), as well as years of joint space operations and wrangling over the creation of space doctrine, before space was accepted as a separate and distinct sphere of combat.

It is ironic, then, that a fifth dimension of conflict, the realm of information operations (IO), has been less universally accepted as a theater of offensive and defensive warfare, despite the fact that armed forces have sought, defended, attacked, and exploited information in battle for centuries. Information warfare is unfortunately tied to modern technology and computers, forgetting that the concept can be as simple as a wooden horse left as a gift outside a great fortified city.

However, military tacticians now understand and appreciate that the concept of information operations has been gradually getting more attention focused on it in doctrine and contemporary military operations. Inevitably in the 21st century the technological aspect of conducting information operations is going to be linked to two things: space and cyberspace. In this article, we will concentrate on the former, with the understanding that computers and the associated links, networks and nodes play a vital role in the command and control of operations in space. We will discuss the historical ties between space and information operations, the difficulty that we in the space community have had in grasping information operations as a viable separate construct, and we will review some of the Air Force's education efforts being applied to change that paradigm. Finally, we will propose solutions to ensure information operations continue to be an effective weapon in our military's arsenal.

History

> We've spent thirty-five or forty billion dollars on the space program. And if nothing else had come out of it except the knowledge we've gained from space photography it would be worth ten times what the whole program cost. Because tonight we know how many missiles the enemy has and, it turned out, our guesses were way off. We were doing things we didn't need to do. We were building things we didn't need to build. We were harboring fears we didn't need to harbor.[2]
>
> - President Lyndon Johnson, 1967

Similar to the first military uses of airplanes and balloons, the initial utility of satellites came from its surveillance capabilities. Space was the ultimate "high ground"—as every general from Patton to Napoleon to Caesar would tell you, knowing what is happening on the other side of that hill is paramount for situation awareness. The National Reconnaissance Office's recently declassified CORONA program was established in 1960 as the nation's first operational satellite photo reconnaissance project. Imagery intelligence is still a vital asset provided by optical satellite sensors today, though it is telling to see how far the technology has advanced in forty years.

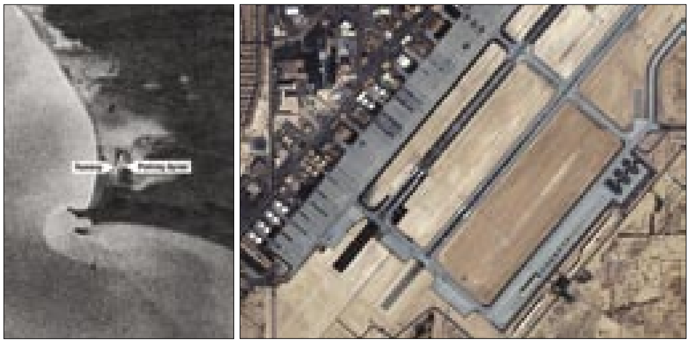


Figure 1. NRO Figure 2. GeoEye

Figure 1. (left) First imagery taken by CORONA, Mys Shmidta Air Field, USSR, 1960. Figure 2. (right) Nellis AFB, Nevada, 2002.

Ever since the 1957 launch of Sputnik, when the United States realized that the Soviet Union could now launch a rocket capable of landing an object (a nuclear warhead?) anywhere on the globe, our military posture became based on information gathering and deterrence based on flexible response. As Lt Col James Lee wrote in *Counterspace Operations for Information Dominance,* "US military space systems were initially developed in a Cold War context and viewed as primarily strategic systems—supporting the Strategic Air Command, the intelligence community, and the National Command Authorities. Timely, accurate, and unambiguous strategic and tactical warning information from reconnaissance, surveillance, and communication satellites provided situation awareness of our perceived enemy and became integral to the deterrent power of the triad."[3]

In essence, Lee asserts that our military systems became almost a hidden fourth leg of the strategic nuclear triad. The strength of Soviet and American nuclear deterrence relied on the ability of satellites and their ground networks to collect, process, and disseminate information. The balance of information provided by these systems resulted in each of the belligerents having a sufficient amount of timely warning of the other side's capabilities and actions. Lee continues, "Maintaining the balance in warning information prevented one side from achieving surprise and rendering the other side incapable of a nuclear retaliatory strike. In fact, the value of the information from space systems was viewed as essential for cold war stability, and many argued that space must remain a sanctuary to preserve stability."[4]

Ultimately, space's role in "standing toe to toe with the Ruskies" has been played out, with, some argue, President Reagan's threats to provide an anti-nuclear blanket of protection with his Strategic Defense Initiative bankrupting the Soviet coffers when they attempted to counter it. Space has more recently moved from this strategic role to the tactical missions of day-to-day combat support.

Operation DESERT STORM is mistakenly referred to as the "first space war," though no battles were fought from or through space. But the Gulf War saw the first combat use of Global Positioning System (GPS) satellites, used both by supporting General Norman Schwarzkopf's "left hook" through the featureless desert and through Joint Direct Attack Munitions, or "smart bombs." This war also highlighted the multiple uses of satellites in providing imagery, weather data, theater ballistic missile launch warning, and, especially, communications in remote areas with not a lot of land lines. More than 90 percent of communications in-theater was provided via the Defense Satellite Communications System, an array of satellites orbiting 28,000 miles overhead.

The conflict also pointed out our asymmetric advantage in the space arena, however, and some of the benefits we enjoyed then, we could not realize today. For example, because of the multitude of commercial imaging satellites on the market, there is no way General Schwarzkopf's maneuver to the west and north around Kuwait would go undetected today. Our use of GPS technology compelled Saddam Hussein to purchase several GPS jamming devices prior to Operation IRAQI FREEDOM (though, fortunately, he and his military did not know how to employ them very effectively). Also, because of our reliance on satellites for communication, bandwidth was used to full capacity, sometimes forcing large files like imagery or Air Tasking Orders to be shipped by airplane rather than satellite links. Further, Operation DESERT STORM forced us to understand that our enemies do not rely on technology like we do, and we were still ineffective in shutting down all aspects of the Iraqi's ability to wage war. Several analysts suspect that after our forces destroyed Saddam Hussein's more advanced telecommunications systems (satellite, microwave, and cable systems), he continued to relay launch orders to Scud missile batteries via courier.[5]

As the last century closed, the cost of launching satellites started to decrease and the number of civil and foreign entities getting into the space business exploded. We had entered what many labeled "the Information Age." But in this case, the availability of information is a double-edged sword that is effectively whittling away at the advantage enjoyed by the United States as one of the historical few that has in the past controlled space system information.[6] The commercial application and exploitation of space information is another threat that must be a part of any military space professional education.

Organization and Education

> We need space professionals in all services and agencies…to exploit space effectively in the interests of national security. Development of a space cadre is one of our top agenda items for national security space programs in 2004.
>
> - Under Secretary of the Air Force Peter Teets
> Report to Congress, 12 March 2003

In 2001, Maj Daniel F. Gottrich was assigned to the USAF Space Operations School (SOPSC), a division in the Space Warfare Center on Schriever AFB, Colorado. Its mission was two-fold: to develop space tactics, techniques, and procedures for warfighting doctrine and to educate space personnel (and members from other specialties who had signed up) about operational space systems. A career space officer who had just returned from an overseas tour in Turkey, he was tasked to develop a lesson for space doctrine, which he knew very little about, satellite communications, which he would have to brush up on, and something called IO. Major Gottrich had never heard of the term, so he was surprised to be assigned responsibility to teach a course on the topic to a room full of joint professionals.

To prepare, Major Gottrich attended an IO conference in February of 2002 in Las Cruces, New Mexico called "Phoenix Challenge" which brought together military, industry, and academic leaders to highlight the latest in IO technology, best practices, and literature. The over-arching message was how prevalent IO was in our society, and Major Gottrich was shocked that he had never heard of it during his military training. Too often we as a military equate IO with computers and consider it the bailiwick of communications experts. Indeed, Major Gottrich would often ask his class members why they thought he was teaching IO in a space operations class, and would inevitably receive the response: "because our satellites are controlled by computers."

The past few years have seen new strides in education, sparked by the creation of the Air Force Doctrine Center at Maxwell AFB, Alabama in 1997 (compare this date with Army's Training and Doctrine Command established in 1968). New space and IO doctrine has been created and updated several times in those eight years, and the lessons are trickling down to the units. "Air, space and information functions work best in an integrated and synergistic way," states a recent Doctrine Watch lecture emailed to every Operations Support Squadron for further dissemination. "Integrating effects-based information operations functions with the other air and space power functions is a crucial part of the Air Force's operational art."[7]

Doctrine became a very important part of SOPSC lectures, particularly tying space and information operations together. The course had already covered space doctrine, and the four core space mission areas:

- Space Control – ensures freedom of action in space for the US and its allies and may deny an adversary freedom of action
- Space Force Support – consists of operations that deploy, augment, sustain, and replenish space forces, including the configuration of command and control structures for space operations and all launch operations
- Space Force Application – would consist of attacks against terrestrial-based targets carried out by military weapons

operating in or through space
- Space Force Enhancement – provides navigation, communications, intelligence, surveillance, reconnaissance (ISR), ballistic missile warning, and environmental sensing (weather)

The SOPSC lesson would demonstrate that the Space Force Enhancement mission had the greatest impact on IO by providing the Information-In-Warfare (IIW) capabilities that enable the commanders to have a full picture of the battlespace in order to make the best decisions. It would also stress how space systems would enable these elements, specifically the IIW capabilities, through satellite support. ISR functions are supported by satellite imaging capabilities, weather services rely on the Defense Meteorological Support Program satellites and the precision, navigation and positioning is provided by GPS.[8]

Furthermore, Air Force Doctrine Document (AFDD) 2-2: Space Operations, states: Space, air, and information platforms are mutually supporting and supported throughout the spectrum of conflict:

- Space assets are unable to contribute if their uplinks and downlinks are interrupted or their ground control and receiving stations are disabled
- Information superiority helps ensure the freedom from attack for control and mission links that tie space providers to ground, air, or sea-based users
- Space, air, and information superiority are mutually supporting objectives. It is extremely difficult to maintain one without the others and the value of one is greatly enhanced when accompanied by the others[9]

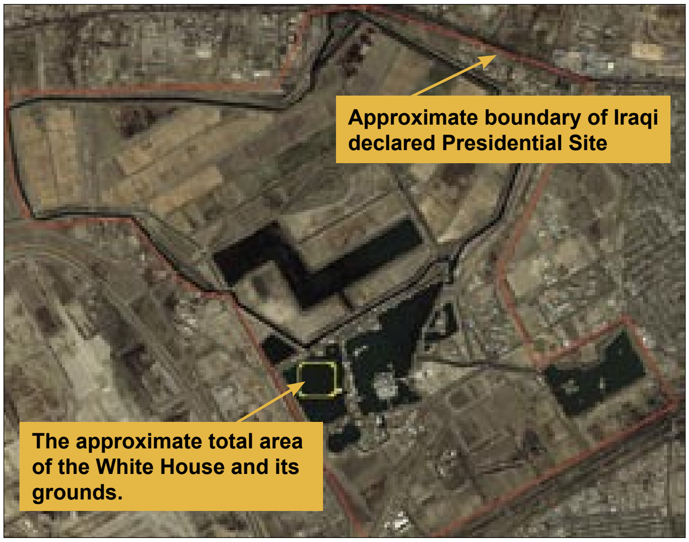
Space and IO capabilities are intertwined and almost have a symbiotic relationship. Information is the lifeblood of IO and space plays a major role in providing the platforms for this info to flow. But space operations also enable some offensive and defensive IO tactics as well. Space assets can be used for public affairs, psychological operations, and operational security (OPSEC). Maj Robert Newberry wrote in *Space Doctrine for the Twenty-first Century* that OPSEC has been a prominent feature of our space forces, and the trick is to balance usability with classification issues. He writes, "A comprehensive OPSEC plan can help prevent attacks on US space forces by making it more difficult for an adversary to launch an attack." Newberry also asserts, "OPSEC can create uncertainty as to the true nature of US space operations and deny the adversary needed targeting data. Although the benefit to some space systems may be negligible, OPSEC can be particularly effective in protecting high-value assets."[10] Major Newberry offers the following table comparing different levels of OPSEC available within space operations and their effects on the enemy's ability to wage war.

Operational Art Element	Adversary's Uncertainty
1. Encryption	I don't know what they are doing.
2. Observation Management	Can I believe what I see?
3. Training	They seem to anticipate my moves.
4. Interoperability	What are the connections?
5. Data Fusion	Can I have a meaningful effect?
6. Launch on Demand	Should I expect more?

Robert D. Newberry

Table 1. Operational Art Element vs. Adversary's Uncertainty.

We can also use space assets to defend our actions or counter enemy propaganda. For instance, in 1998, Saddam Hussein decided to allow the United Nations weapons inspectors back into his country, but informed them that they would not be able to inspect "palace grounds." We were able to use satellites as part of a counter-information campaign to show the world how cooperative the Iraqi leader was really being.


Approximate boundary of Iraqi declared Presidential Site
The approximate total area of the White House and its grounds.

DigitalGlobe - QuickBird

Figure 3. Radwaniyah Presidential Site.

However, satellite technology is not perfect. During Operation ALLIED FORCE, the Serbs were still able to fool some of our most skilled observers with rubber or wooden mock-ups of cannons or aircraft. In one instance, they even hung lanterns in the "exhaust" to make it appear on infra-red sensors to have a heat signature.

About the same time as Major Gottrich's arrival to the SOPSC, Air Force Space Command (AFSPC) was also reeling from a scathing Congressional report released in January of 2001. The *Report of the Commission to Assess United States National Security Space Management and Organization,*[11] also known as the "Rumsfeld Report" since Donald Rumsfeld was the Chairman of the Commission (before recusing himself to become Secretary of Defense) had given the services a failing grade in developing space professionals, in particular decrying the Air Force practice of bringing in pilots to command space units for short periods in a vain attempt to show breadth in leadership. Assignments were poorly managed, and continuing education after entry level (as a young airman or second lieutenant) was non-existent. The report recommended that the Air Force be given one last shot to transform itself before being forced to carve off its space operations into a separate service or a subordinate but separate entity like the Navy/Marine Corps relationship.

Early in 2003, the SOPSC took the lead for developing and executing the first four-week "Space 200" course, geared towards mid-career officers, noncommissioned officers, and civilians at the 8- to 10-year point. The course, using material taken from some existing SOPSC courses and augmented with additional material in the fields of acquisition, engineering, and nuclear operations, had a stronger emphasis on warfighter integration of space power in the joint fight. The course also consisted of increased technical content, to include a design exercise in which student groups designed a satellite program to fulfill a Department of Defense (DoD) requirement, then considered its application in a capstone wargame exercise at the end of the course.

SOPSC also initiated the development of Advanced Space Training (AST) courses in order to produce system experts that will return to unit or wing tactics shops to be instructors. Currently, space officers are sent to the Weapons School at Nellis AFB, Nevada where they become generalists in all space systems and learn integration of air, space, and information operations. These graduates are sent to Major Commands (MAJCOMs), Unified Commands, and theater Air and Space Operations Centers (AOCs). The vision for AST is to mirror the air side of Weapons School, wherein pilots are immersed in their particular weapons system and graduate as experts on that platform. The SOPSC's first AST course, Navigation Operations, took ten officers and NCOs through an intensive, 12-week curriculum where they became experts in GPS, navigation tactics, the command and control structure, concepts of operation, acquisition, and weapon system applications.

In the spring of 2005, the Air Warfare Center and Space Warfare Center were administratively merged into the US Air Force Warfare Center in order to "better manage air, space, and information operations combat capabilities to support missions worldwide."[12] There is talk of including the Information Warfare Center (another potential assignment for space operations personnel), currently located at Lackland AFB, Texas, in future reorganization plans. In addition, more and more space professionals are deploying overseas, and many of them are being attached to Information Warfare (IW) Flights within an AOC.

Organizationally, space command has been tied to IO since the late 1990s. In response to a number of attacks on government computer networks, the Office of the Secretary of Defense ordered the Defense Information Systems Agency to establish the Joint Task Force-Computer Network Defense (JTF-CND), which was transferred to Colorado Springs' then Space Command (USSPACECOM) in 1999. As the senior computer emergency response team in the DoD, the JTF-CND was the responsible cell for all CND issues, including recommending changes to the information condition status when the situation required.[13] In 2001, it was renamed the Joint Task Force-Computer Network Operations to reflect its growth and mission, and continued to operate under the IO portion of the USSPACECOM mission until 2003, when US Northern Command was set up to coordinate military homeland security efforts and USSPACECOM was absorbed into US Strategic Command (USSTRATCOM), with the IO tasking going to USSTRATCOM at Offutt AFB in Omaha, Nebraska.[14]

Securing Information In Space

> The [DoD] must enhance the capability and survivability of its space systems. Activities conducted in space are critical to national security and the economic well-being of the nation. Both friends and potential adversaries will become more dependent on space systems for communications, situational awareness, positioning, navigation, and timing. In addition to exploiting space for their own purposes, future adversaries will likely also seek to deny US forces unimpeded access to and the ability to operate through and from space. US forces must ensure space control and thereby guarantee US freedom of action in space in time of conflict.[15]
>
> - Director, Force Transformation Office, 2003

Our dependence on space makes satellites not only a valuable tool, but prime targets. Ideally, all satellites should be hardened from attack; commercial investors, however, are reluctant to spend the money to protect their satellites.[16] High-altitude nuclear bursts and the resultant electromagnetic pulse (EMP) might render most allied space assets inert. EMP could burn out the circuitry of most allied radio systems, computers, transistors, and power grids in the region of combat, rendering many of the allies' high-tech assets harmless.[17]

On the flip side, because of cost and the physics involved, it is unlikely that many countries are attempting to develop anti-satellite weapons.[18] It is more likely that an adversary will try to exploit the information-gathering apparatus on the ground, either by physical destruction, jamming, or other means of denial. Jamming is very similar to a computer hacker's denial-of-service attack, essentially transmitting a high-power, bogus electronic signal that causes the bit error rate in the satellite's uplink or downlink signals to increase, resulting in the satellite or ground station receiver losing lock.[19] GPS receivers, for example, are notoriously vulnerable to jamming because of the low power in the navigation message. Power of just a few watts can jam the access code at a distance of 10-20 kilometers.[20] Indeed, the signal coming off a GPS satellite, orbiting at 12,500 miles, is the equivalent of a 25 watt light bulb.

Attacking the link segment by spoofing involves taking over the space system by appearing as an authorized user, such as establishing a command link with an enemy satellite and sending anomalous commands to degrade its performance. Spoofing is one of the most discrete and deniable non-lethal methods available for offensive counterspace operations.[21] These ground attacks will appear like a series of nuisance events, or computer vandalism. But how do we distinguish a computer "glitch" from an information attack that has disrupted our satellite command and control network, such as the May 1998 failure of PanAmSat's Galaxy 4 communications satellite? The satellite's computer crashed unexpectedly, and the spacecraft temporarily went out of control. Somewhere between 80 and 90 percent of America's 45 million pagers went dead, and National Public Radio lost its feed to local stations.[22]

Offensively, information dominance can be attained "by collapsing an adversary's command and control infrastructure through offensive operations, such as the disruption of critical communication links; or by denying access to reconnaissance and surveillance information, such as blinding optical sensors with ground-based lasers. Defensively, measures such as hardening, frequency hopping, and encryption further ensure information dominance by helping to ensure friendly forces have uninhibited access to communications, surveillance and reconnaissance information provided by space systems."[23] It is these offensive and defensive IO measures that the US needs to focus training and funding toward in the coming decades in order to thwart the up-and-coming challenges of a technologically savvy adversary such as China.

The US military traditionally uses spacepower assets for two primary purposes: (1) to improve the situation awareness of its forces; and (2) as a means of command, control, and communications. Lieutenant Colonel Lee writes, "We essentially exploit space power assets as a permanent informational infrastructure that is globally available to friendly forces. This allows friendly forces to operate on interior lines of information around the globe."[24] But it also allows our enemies access to this same information. Indian President A.P.J. Abdul Kalam recently expressed concern over Google Earth's free satellite imagery software, which provides clear pictures of some of India's military and government facilities, claiming the information could be used by terrorists to plan attacks.[25]

"No claim is made that US military forces are neutered without space support. Terrestrial forces can still fight without space support," writes Maj M.V. Smith. "However, the absence of space support will inarguably increase the fog, friction, and overall costs of military operations."[26]

Recommendations for the Future

> The Air Force must begin to think and bring forward the technologies necessary for space control. Capabilities to defend our own space based resources and to disrupt, degrade, deny, or destroy that of the enemy will be needed sooner or later in the 21st century. The technologies needed to protect our space resources from enemies include high thrust, high specific impulse electric propulsion, large constellations of low cost satellites with distributed functionality or networking across the system, and autonomous guidance and navigation.[27] - USAF Scientific Advisory Board, 1995

Trying to predict our technological future is futile. In 1982, the contemporary feeling from senior Defense Department leaders was that space-based lasers, capable of global ballistic missile defense from ICBM launches from the Soviet Union, would be in orbit in "ten or eleven years."[28] It is fair to conclude that we are easily the world's best military force, though our dominance may not last forever, given the declining costs and spread of technology.[29] But speculation on our specific offensive and defensive capabilities is something for the scientific journals, though the research labs, battle labs, and warfare centers are doing remarkable research.

> The United States has fielded laser illuminators that use semiconductor laser arrays to aid night vision devices. Projecting a laser beam over a large area on the earth's surface would help low-light imaging systems to find targets. A space-based battlefield illuminator would generate beams from satellites in low-earth orbit and direct them to the target. This technology would allow military forces to acquire targets with low-light imaging systems, insert and remove special operations teams under low light conditions, and increase the security of high-value facilities at night. Because the beam is eye-safe, the illuminator could be used for psychological operations in which US observers search covertly for enemy units.[30]

Fascinating reading, but it doesn't help us prepare the troops for the type of combat we will start to see in the next thirty years, in whatever form it appears. Author Jeffrey Barnett says it best, "Information will dominate future war. Wars will be won by the side that enjoys and can exploit:

- cheap information while making information expensive for its opponent
- accurate information within its own organization while providing or inserting inaccurate data in its opponent's system
- near-real-time information while delaying its opponent's information loop
- massive amounts of data while restricting data available to its opponent; and
- pertinent information while filtering out unnecessary data."[31]

It does not matter who has the most toys, Barnett implies. "Tactical effectiveness … depends on the control systems over the war theater and efficiency in utilizing information from the theater."[32]

Information operations is a skill that must be taught early and properly managed throughout a career, just as AFSPC has tried to turn around the management of space professional education. To that end, it could use a senior-level champion, as proposed in the Space Commission report, which stated that an Under Secretary of Defense for Space, Intelligence and Information should be established to, among other things, "oversee the Department's research and development, acquisition, launch and operation of its space, intelligence and information assets."[33] Unfortunately, in May of 2001, Secretary of Defense Rumsfeld reported that he had instead recommended that the staff "review the responsibilities and functions of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence…" to this end.[34] This is the wrong focus; a cop-out. This again comfortably equates information with technology and allows the management of information operations to be swallowed up by a technocrat.

A second recommendation is to revamp information operations doctrine. As of December 2005, Joint Publication 3-13: *Information Operations,* has not been updated in over seven years.[35] (This is still better than the twelve years it took for JP 3-14, Space Doctrine, to get published initially.) We believe that this is woefully inadequate. AFDD 2-5, *Information Operations,* has been updated twice since 2002. If the military is going to continue to use doctrine as a repository for officially sanctioned beliefs, warfighting principles, and terminology that describes and guides the proper use of air and space forces in military operations, it must remain current, fluid, and substantive. It is appalling that Joint IO doctrine has been allowed to languish for nearly a decade.[36]

Third, the concept of *Information Control* should be adopted within IO doctrine. This would emphasize the importance of capabilities to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. In space doctrine, space control is the overall realm of responsibility in which space superiority is gained and maintained to assure friendly forces can use the space environment while denying its use to the enemy. To accomplish this, space forces must survey space, protect the ability to use space, prevent adversaries from exploiting US or allied space services, and negate the ability of adversaries to exploit their space forces. In the 21st century, air and space superiority is unfortunately almost immediately assumed before the first shot is fired. Implementing the overall situation awareness of the IO battlespace, and comprehending the offensive and defensive requirements necessary to sustain an "information control" mission would help solidify information as the fifth realm of warfare.

Finally, IO has become so important a concept in our military that we should start to train IO specialists, that is, create a separate

Air Force Specialty Code for information operations officers and enlisted troops, so that they can become IO experts. Currently, we train experts in air operations and space operations, in weather, in intelligence, in public affairs, in communications. We then assume that each of them knows enough about information operations that any one of them could fill a slot requiring IO experience. Until we begin to groom a cadre of IO professionals, and start to build a twenty-year arsenal of individuals performing the IO mission day in and day out, we will be forced to re-invent the wheel at every level each time a new person rotates into an IO assignment.

Conclusion

There is nothing we do in space that is not information operations.[36] - Maj Gen Thomas Goslin, 2001

In 2003, the Director of Force Transformation, Office of the Secretary of Defense, wrote that the DoD "will treat information operations, intelligence, and space assets not simply as enablers of current US forces but rather as core capabilities of future forces."[37] Therefore, information operations doctrine, training, and career specialization must continue to evolve in the 21st century, while simultaneiously strengthening its integration with space operations. As commander of the Space Warfare Center, Maj Gen Goslin once said, "Today, more than anything, space provides information. And information today is a show-stopper."[38]

Notes:

[1] Colin S. Gray, *American Military Space Policy: Information Systems, Weapon Systems and Arms Control* (Cambridge, MA: Abt Books, 1982), 37.

[2] William E. Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), vii.

[3] Lt Col James G. Lee, *Counterspace Operations for Information Dominance* (Maxwell Air Force Base, AL: Air University Press, 1994), 1-2.

[4] Ibid.

[5] Maj YuLin G. Whitehead, *Information as a Weapon: Reality versus Promises* (Maxwell Air Force Base, AL: Air University Press, 1999), 30.

[6] Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington: Brassey's, Inc., 2004), 119.

[7] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, Air Force Doctrine Center, 11 January 2005.

[8] *Information Operations,* USAF Space Operations School, Space 200 Lesson Plan (March 2004).

[9] AFDD 2-2, *Space Operations*, AFD Center, 27 November 2001.

[10] Robert D. Newberry, *Space Doctrine for the Twenty-first Century,* (Maxwell Air Force Base, AL: Air University Press, 1998), 32-33.

[11] *Report of the Commission to Assess United States National Security Space Management and Organization,* Space Commission, Pursuant to Public Law 106-65, 11 January 2001.

[12] Lt Gen W.M. Fraser, "Space, Air Warfare Centers Integrate Capabilities," *Defense AT&L*, September-October 2005, 44.

[13] Armistead, *Information Operations,* 33.

[14] Ibid., 33-34.

[15] Director, Force Transformation, Office of the Secretary of Defense. *Military Transformation: A Strategic Approach* (Washington, 2003), 19.

[16] M.V. Smith, *Ten Propositions Regarding Spacepower* (Maxwell Air Force Base, AL: Air University Press, 2002), 100.

[17] Lawrence E. Grinter and Barry R. Schneider, eds., "On Twenty-first Century Warfare," in *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell Air Force Base, AL: Air University, 1998), 269.

[18] Scientific Advisory Board, US Air Force, "New World Vistas: Air & Space Powers for the 21st century," in *The DTIC Review Future Directions: Preparing for the 21st Century* 2, no. 2 (1996), ed., Christian M. Cupp, 46.

[19] Lee, *Counterspace Operations,* 32.

[20] Scientific Advisory Board, "New World Vistas," 46.

[21] Lee, *Counterspace Operations,* 32.

[22] Bruce Berkowitz, *The New Face of War: How War will be Fought in the 21st Century* (New York: The Free Press, 2003), 164-165.

[23] Lee, *Counterspace Operations,* 4.

[24] Smith, *Ten Propositions Regarding Spacepower,* 68.

[25] Associated Press. "India: Google Maps Too Graphic." *Wired News*, 3 December 2005, http://www.wired.com/news/technology/0,1282,6923,00.html?tw=wn_story_related.

[26] Smith, *Ten Propositions Regarding Spacepower,* 68-69.

[27] Scientific Advisory Board, "New World Vistas," 61.

[28] Gray, *American Military Space Policy,* 2.

[29] Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington: Brookings Institution Press, 2000), 17.

[30] William C. Martel ed., *The Technological Arsenal: Emerging Defense Capabilities* (Washington: Smithsonian Institution Press, 2001), 10.

[31] Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, AL: Air University Press, 1996), 2.

[32] Ibid.

[33] Smith, *Ten Propositions Regarding Spacepower,* 122.

[34] Department of Defense, "DOD Press Release on Rumsfeld Space Initiative," news release, 8 May 2001, http://www.space.gov/Articles/Rumsfeld1.asp (accessed 22 February 2006).

[35] Joint Publication 3-13, *Information Operations,* Department of Defense, Washington: GPO, 9 October 1998.

[36] Maj Gen Thomas Goslin, USSPACECOM/J3, Warfighter's Space Conference, 31 January 2001.

[37] Director, Force Transformation, "Military Transformation: A Strategic Approach" (Office of the Secretary of Defense, 2003): 19.

[38] Maj Gen Thomas Goslin, Commander's Call, Schriever AFB, Colorado, February 2002.

Maj Daniel F. Gottrich (BGS, Indiana University; MA, University of Colorado at Colorado Springs), is currently completing Intermediate Developmental Education in-residence at the AF Institute of Technology, Wright-Patterson AFB, Ohio. In previous assignments, he served on operational tours in the 4th Space Operations Squadron (50th Space Wing), 740th Missile Squadron (91st Space Wing), and 39th Wing (Incirlik AB, Turkey). He was also an instructor and Vice Dean of the USAF Space Operations School (Space Warfare Center). He has staff experience as Chief of Defense Integration for the QDR Joint Actions Directorate, Deputy Chief of Staff for Plans and Programs, HQ USAF. Major Gottrich is a distinguished graduate of Squadron Officer School.

Dr. Michael R. Grimaila (BS, MS, PhD, Texas A&M University; CISSP, CISM, GSEC) is currently an Assistant Professor in the Systems and Engineering Management department and a member of the Center for Information Security Education and Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Dr. Grimaila serves as Editor of the Journal of Information Assurance, Security, and Protection (JIASP), Editorial Advisory Board member of the Information System Security Association (ISSA), and is a member of the International Systems Security Engineering Association (ISSEA) Metrics Working Group. He also holds memberships in the ACM, IEEE, IRMA, ISACA, ISC2, ISSA, ISSEA, and the SANS Institute.

Space Situation Awareness: Before You Control, You Must Understand

Maj Thomas R. Hill, USAFR
Reserve Meteorological Satellite Program Element Monitor, AF/A3S-SO

Much has been made of the need for space control, yet so far there's been little effort in creating an integrated method of gathering space situation awareness data in real time. This article covers the reasons why such a system is important and suggests a relatively simple system to start collecting such data.

Incident 1: November 2005. NOAA-17, the second-newest satellite in the National Oceanographic and Atmospheric Administration's Polar-Orbiting Environmental Satellite (POES) constellation suddenly yaws six degrees away from its normal attitude. Initial investigations lead support engineers to believe that a Leonid meteor strike caused the problem, but another similar event brings the troubleshooting closer to home. Final disposition: attitude event described as a spurious thruster firing due to propellants freezing in the feed lines. Spacecraft configuration changed to address further events.[1]

Incident 2: September 2005. The Solar and Heliospheric Observatory (SOHO) detects an X-class x-ray flare and accompanying particle events.[2]

Incident 3: April 2004. Decommissioned Defense Meteorological Satellite Program (DMSP) flight 11 sheds debris. The additional debris in the orbit are tracked, though no solution as to the final cause is determined.[3]

Incident 4: May 1998. Galaxy 4, a commercial communications satellite loses its attitude control processor. The backup does not take over and the satellite drops offline. Civilian services from ATMs through telephone calls are lost until service providers can reroute signals.[4]

The four incidents described above are examples of events that were handled with varying low degrees of space control. It is a valid argument to make that, in most cases, there was very little for the ground to do: a centralized space control system would have been little more than a nuisance, asking for details about the events as they were happening while people in the trenches were trying do their jobs. Yet the knowledge about such events has proven useful in operations and planning since their occurrence.

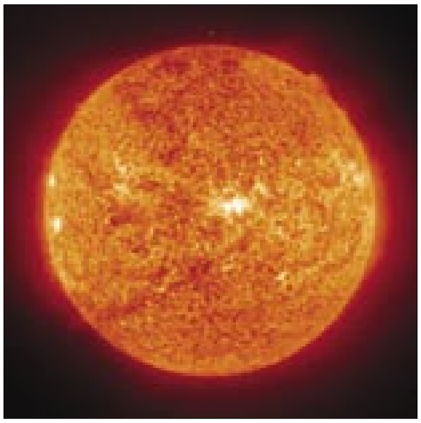


Figure 1. The space environment is often described as harsh, and the sun is a major factor in creating the harsh conditions. Solar radiation, in both long-term streams and short-term flares, can impact spacecraft over the short term (through temporary service interruptions) and long term (in the form of hardware damage). Changes in the solar environment must be monitored in a real-time Space Situation Awareness Center to prevent confusion between a massive solar event and an attack on space assets.

So far, there have been no publicly-reported events where a single event such as a solar flare has led to multiple satellite failures. This should not come as a surprise since, while there are many satellites flying today, they are controlled by a myriad of military, civil, commercial, and international players. These players do not share information very often due to the legal, proprietary, or simple disinterest in how-others-do-business barriers between them. Yet these attitudes must change for a useful command and control structure to form within the space arena.

Before a space command and control entity can serve a useful purpose, the players involved must be aware of what they will be controlling. The first step in that process is space situation awareness.

The space arena is constantly changing: old satellites are decommissioned, operational satellites are changing location or simply being shut down for a short period while their orbits are adjusted, or the sun is impacting Earth's atmosphere and magnetosphere, potentially impacting satellites' communications or hardware. Deeper factors are at work as well: components with recurring manufacturing flaws shorten the lives of otherwise healthy satellites while rocket fleets are grounded by technical problems. There have already been instances of hostile parties interfering with a satellite signal, and it follows that as such players gain the means to impact satellites in other ways, they will do so. Currently, most of the knowledge of such events is relegated to space conferences held long after the fact, when a space control entity would be unable to take any action to correct the problem. In order to make space control relative, it must have this type of information in real time. How can such a goal be accomplished?

The Space Situational Awareness Center

Imagine a room where a 24-hour crew monitors the health of all military, civil, and commercial satellites. Displays are split by classification level, and satellite constellations are grouped together in larger bundles to make their overall status obvious with a glance. For more information, crewmembers can tunnel down into each constellation with a mouse click to find the status of particular satellites, as necessary. The center is also tapped into live feeds from the Space Environment Center, the Space Surveillance Network, and any special event monitors, such as one of the aircraft launched to count meteors during the Leonid meteor storms of the last few years. Another potential group of contributors is the network of amateur satellite watchers who use radio gear and telescopes to keep an eye on satellites. Such a center would have the ability to observe trends as they unfolded. They would know almost immediately if a series of satellite malfunctions could be explained by an unprecedented solar event or if there may be another, darker explanation. Longer-term concerns related to spacecraft that this center could track involve hardware reliability; the changing status of satellites around the globe would feed the most powerful database on the planet about satellite components and their longevity.

Reporting Method

Ideally, the Space Situational Awareness Center (S-SAC) would receive data directly from the satellites in question. This solution is likely too expensive and cumbersome to be feasible unless the center first proves its usefulness. A simpler solution would allow satellite operators from around the country and world to submit status reports over computer networks. The internet would suffice for unclassified, civilian, and international systems while appropriately-classified networks would be necessary for other situations. This data could be filtered as it arrived in the center, processed, and displayed in a user-friendly manner. Each report would also be logged electronically, allowing for later data searches to hunt for patterns.

The Carrot

Why would engineers and operators submit status data about their spacecraft to the S-SAC? The proposed reason is that they get paid to do so. Space situation awareness data is important to the Air Force; therefore the Air Force should be willing to pay for it. The payments can be on a sliding scale based on the timeliness and accuracy of the report, and bonuses could be paid to submitters who contribute to a particularly important revelation about space operations. Payments may also have the side effect of increasing involvement by international players or consortia, who otherwise would have no interest in submitting failure data to the US.

Sample Reports

The following is a list of potential events that would be of interest to the S-SAC. Each would create its own display response within the center, though the specifics of the event may not be reported unless the center operator searches for the details.

Spacecraft Launch – Control center reports satellite purpose, orbital information, command and control as well as user frequencies, expected lifetime, and so forth. More in-depth information would also be useful, including the producer of the various components on board.

Decommissioning – When a satellite is taken out of service, its final state is recorded. Necessary items required for such a report would be: final orbit, residual energy sources on board, potential to broadcast radio signals, attitude state, and so forth.

Maneuver – Usually planned in advance, though space debris could increase the frequency of unplanned maneuvers. Users would report planned pre and post orbital elements, any expected outage time for their services and follow with an after-the-fact maneuver summary.

Internal Mechanical/Electronic Failure – Here, a component failed on the satellite in question, and the user swapped to a different unit. This kind of information will prove useful for future satellite construction and contractor selection.

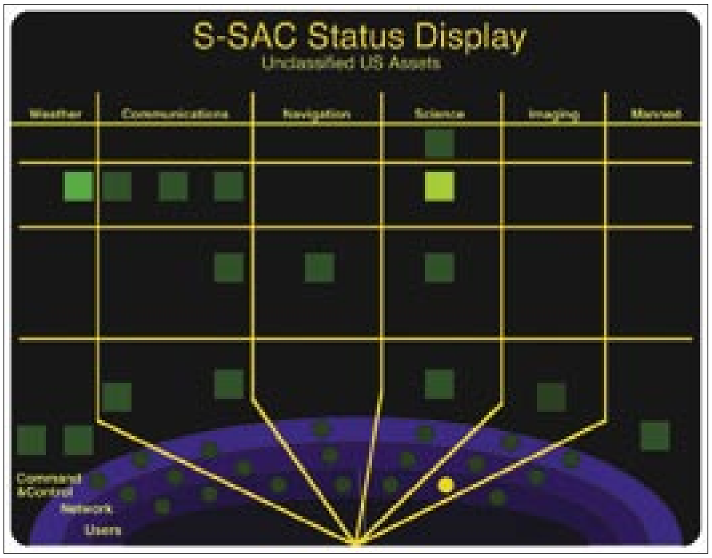


Figure 2. Sample display in the S-SAC. In this example, satellites are divided by mission and orbital altitude. Operators can click on each box or circle to get more information about a particular satellite or constellation. The weather satellite box that is a lighter green than the others is undergoing a planned outage due to a maneuver. The science satellite reading almost yellow experienced a failure that is under investigation. Ground system status is reported in the series of concentric rings representing the Earth.

Impact – Though rare, these events do occur. A meteorite or piece of space debris can cause obvious effects to a satellite in orbit. Trending this type of data could provide concrete information in any changes in the orbital debris situation.

Unknown – These events will likely be the most interesting, as operators notice something different about their satellites but can't figure out exactly what's going on. By being a central repository for such events, it is possible that the S-SAC will be able to help solve the mysteries.

Issues to Consider

As most who have worked in the field know, space operations has many nuances to it that do not allow easy operational reporting. For example: does a satellite that is fully functional on its backup processor require a green reporting status or a yellow? Such nuance leads to other concerns for a space situational awareness center, but there are ways to overcome them.

First Answer is not Usually Correct – As the NOAA-17 anomaly mentioned at the beginning of the article shows, when pressed for a quick cause of an anomaly, that answer might not be correct. In the early moments of a troubleshooting scenario, some of the craziest ideas for the cause have not been eliminated yet, and a report to the S-SAC in those early moments could lead to bad decisions. The tradeoff is that, eventually envisioning space control, quick information is necessary to allow a timely response. In this early incarnation of the S-SAC, operators should be encouraged to report their first indications of a problem, with the cause marked as questionable. Later, as more information comes in, operators can update their believed cause.

Figure 3. Sharing satellite operations data across government agencies faces many historical and bureaucratic hurdles. A satellite like the National Oceanographic and Atmospheric Administration (NOAA) Polar-orbiting Operational Environmental Satellite (POES) pictured here suffered two attitude disturbances in late 2005, and no structured method of quickly sharing that information between agencies existed.

As more data is gathered, certain sources of the information will be given more weight when compared to others, providing an additional check.

"Spoofing" the System – If word gets out that there is a S-SAC and it gathers information over open sources such as the web, there is a subset of people who would be willing to spoof such a system with bogus reports. Many of these people would be involved in such activities for the thrill of the hunt itself, while others would deliberately want to feed false information to the system to confuse the center in an attack situation. This concern is relatively easy to address through user accounts validated through known satellite operations centers, with hobbyists and other contributors taken on a case-by-case basis.

Proprietary Data – Satellite builders are well known for their desire to maintain trade secrets. There are many valid reasons for such concerns, but trade secrets can also make it difficult to spot fleetwide trends. The operators of the S-SAC would have to be aware of the trade sensitivities of the data they handle, and apply appropriate procedures to make sure that the information is usable for the community at large while not compromising such secrets.

Data Sharing – While this information would be very useful to the US, other entities would also find the data interesting. An aggressor who's sharpening his skill in satellite service disruption would like nothing better than to get a confirmation that their efforts were bearing fruit. Data gathered by the S-SAC will have to be tightly controlled, and only released to others who do not pose a threat to US interests.

The architecture described here is not difficult to build, and it could be incorporated into an existing center rather easily. The hardest part will be changing the mindset of the satellite operators around the Nation and/or world that such a center can serve a useful enough purpose that they should contribute their operations data.

When humanity becomes spacefaring, space control will be as commonplace as air traffic control is today. In aircraft terms, space is not far removed from the "big sky" concept in the early days of aviation, where there were few enough aircraft that air traffic control was not considered important. Recent events, combined with our increasing reliance on space assets, do not allow us to hold that mindset. As we make the space control transition, the first steps will be some of the most difficult but are the most critical, and invoking true, real-time, space situation awareness is the first such step.

Notes:

[1] National Oceanographic and Atmospheric Administration (NOAA), National Environmental Satellite, Data, and Information Service (NESDIS) satellite status page, entries dated 14 November 2005-16 December 2005, http://www.oso.noaa.gov/poesstatus/componentStatusSummary.asp?spacecraft=17&subsystem=0 (accessed 20 February 2006).

[2] Robert Roy Britt, "Sun's String of Fury Continues as 7th Flare Erupts," Space.com, 9 September 2005, http://www.space.com/scienceastronomy/050909_solar_flares.html (accessed 20 February 2006).

[3] John A. Tirpak, "Securing the Space Arena," *Air Force Magazine* 87, no. 7 (July 2004), http://www.afa.org/magazine/july2004/0704space.asp (accessed 20 February 2006).

[4] "Pager messages lost in space," *CNN*, 20 May 1998, http://www.cnn.com/TECH/space/9805/20/satellite.outage/ (accessed 20 February 2006).

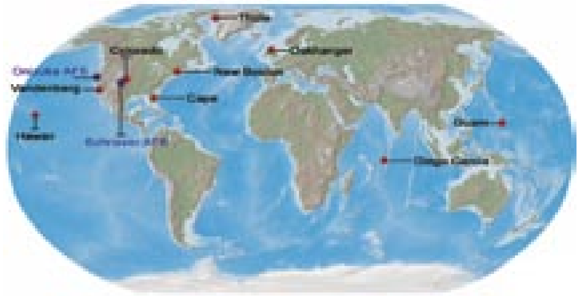
Maj Thomas R. Hill (BS, Penn State University; MS, Colorado Technical University) is the Reserve Meteorological Satellite Program Element Monitor supporting Headquarters Air Force, Space Operation Division (AF/A3S-SO) at the Pentagon. In this position, he monitors and reports status for currently operating and in-development weather satellites. His history includes time in the office of the Undersecretary of the Air Force for Space, as well as service in launch, space track/missile warning, and satellite command and control areas. In his civilian position, he works with national weather satellites. His book, *Space: What Now? The Past, Present, and Possible Futures of Activities in Space* was published in February 2005, and he has written numerous technical papers and articles about the history of space exploration and its place in the future of humankind. He is a graduate of Squadron Officer School in residence and Air Command and Staff College by correspondence.

Evolution Toward the Interoperable Satellite Control Network

Maj Michael J. Dunn, USAF
Deputy Chief, Satellite C2 Branch

Under the auspices of the National Security Space Architect (NSSA), an initiative to establish a shared United States Government (USG) space network comprised of numerous existing independent networks was born.[1] This concept, called the Interoperable Satellite Control Network (ISCN), seems to often be maligned and misunderstood. This article will attempt to dispel misconceptions about ISCN, and raise community awareness of what exactly ISCN is, and is not, meant to be. But before we dive into ISCN, let's first take a brief look back to better understand how we have arrived at where we find ourselves today.

From the dawn of the US space program, a ground network initially developed to support the first military satellites in the late 1950s has continually expanded and evolved into what is now known as the Air Force Satellite Control Network (AFSCN) (figure 1).



MISSION

- **Initial deployment and checkout of DoD, civil, and allied satellites**
- **Assured C3 connectivity between ground SATOPS Centers and operating satellites**
- **Emergency recovery of satellites in trouble**
- **Mission and spacecraft data reception and relay**
- **Space Safety (Collision avoidance & Radio Frequency Interference) for US government**
- **Satellite position determination**
- **Disposal Operations**

Figure 1. Air Force Satellite Control Network.

Today, the AFSCN is the backbone of Department of Defense (DoD) space operations supporting over 150 DoD, national, and civil satellites worldwide.[2] Support includes launch and early orbit, on-orbit, and disposal operations. Additionally, as the DoD's only high-power-transmit capable network, the AFSCN is also called upon to support satellite anomaly resolution operations. In 2004 alone the AFSCN supported 29 satellite vehicle emergencies resulting in $11.5 billion in satellites returned to operations, as well as supporting the NASA Space Shuttle return to flight in 2005.[3] However, the AFSCN is not the only game in town. Other government satellite control networks (SCNs) have also emerged and evolved through the years, among them the National Aeronautics and Space Administration (NASA) Ground Network, Space Network, and Deep Space Network, the National Oceanic and Atmospheric Administration (NOAA) Ground Network, and the Naval Satellite Control Network, as well as a number of other dedicated DoD system networks (figures 2 and 3).

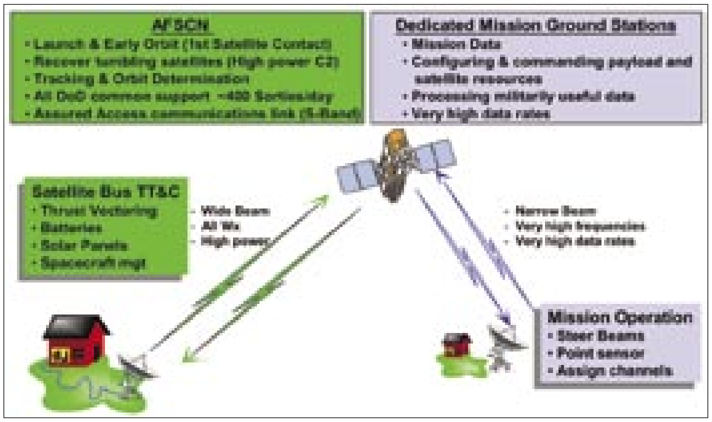

AFSCN
• Launch & Early Orbit (1st Satellite Contact)
• Recover tumbling satellites (High power C2)
• Tracking & Orbit Determination
• All DoD common support ~400 Sorties/day
• Assured Access communications link (S-Band)
Dedicated Mission Ground Stations
• Mission Data
• Configuring & commanding payload and satellite resources
• Processing militarily useful data
• Very high data rates
Satellite Bus TT&C
• Thrust Vectoring
• Batteries
• Solar Panels
• Spacecraft mgt
- Wide Beam
- All Wx
- High power
- Narrow Beam
- Very high frequencies
- Very high data rates
Mission Operation
• Steer Beams
• Point sensor
• Assign channels

Figure 2. Satellite Control.

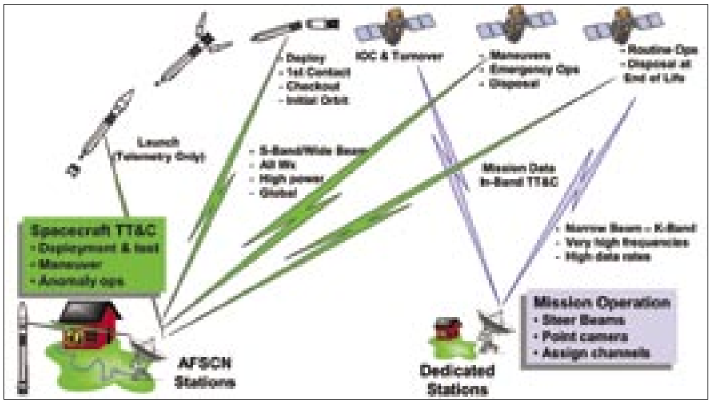


Figure 3. Satellite Command and Control CONOPS.

These SCNs encompass more than one hundred sixty antennas and the associated communications infrastructure with varying capabilities and locations. However, the demand for limited resources within each of these networks has continued to increase. This has, in turn, created a growing need to find more cost effective solutions to the substantial sustainment and replacement costs of multiple individual government networks. As a result, in 1997, the NSSA Satellite Operations (SATOPS) Architecture Development Team recommended an evolution to an interoperable tracking, telemetry and commanding (TT&C) SATOPS architecture for USG space programs. That evolution ultimately leads to the ISCN.[4]

The overarching objective of the ISCN concept is to provide on-demand access and a shared interoperable architecture that allows seamless launch, early orbit, anomaly resolution and disposal (LEOA&D) satellite operations for all USG users.[5] This future architecture will also include new capabilities beyond what is currently available on the AFSCN (e.g., access to space-based TT&C relay assets, multi-band antennas, etc.) and systems needed to meet the required effects, interoperating within a network-centric environment. The ISCN's capability to access assigned space assets anytime, anywhere is critical toward enabling responsive space operations. This capability will enable immediate adjustments to mission profiles and configurations supporting time-sensitive operations, such as reconfiguring/optimizing payloads or repositioning space assets in response to theater operations.

The intent of the ISCN is to evolve selected assets of existing SCNs into a more broadly shared network of interoperable networks to support all assigned USG pre-launch, LEOA&D, low data rate on-orbit data retrieval and backup/contingency operations. The ISCN will provide increased mission assurance, capacity, coverage, automated operations where appropriate, and robustness.[6]

Following guidance issued from the National Security Space Senior Steering Group and Office of the Secretary of Defense, Command, Control, Communications, and Intelligence (C3I), in November 2000,[7] the Joint Requirements Oversight Council, Office of the Assistant Secretary of Defense for Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Space (C3ISR&Space), NASA and NOAA approved the SATOPS Architecture Transition Plan that incorporated this concept.[8] HQ USAF/XOS directed AFSPC to begin implementation in February 2001.[9]

ISCN will be developed and implemented in several spirals. The first spiral, called ISCN Core (ISCN-C), will insert essential interoperability enabling technologies into the current AFSCN, such as dual-band capability, updated standardized interfaces, and cross-domain solutions. With an initial operations capability projected in 2012, ISCN-C will serve as the starting point and mark the beginning of the transition from the AFSCN to the ISCN (figure 4). A series of additional spirals will implement new capabilities and incrementally evolve the ISCN-C to incorporate the use of selected other SCN assets into the ISCN based upon mission needs and cost.[10]

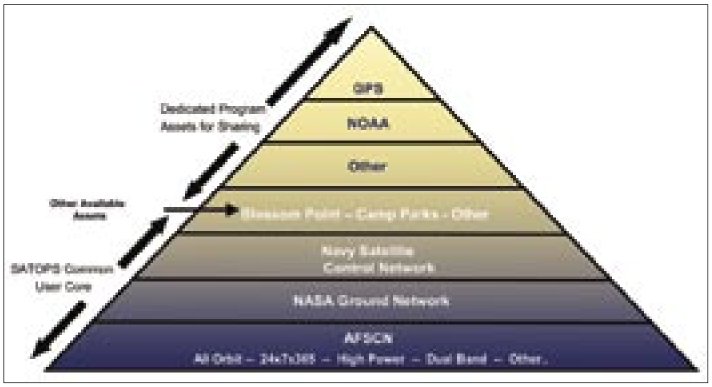

GPS
NOAA
Other
Blossom Point – Camp Parks – Other
Navy Satellite Control Network
NASA Ground Network
AFSCN
All Orbit – 24x7x365 – High Power – Dual Band – Other..
Dedicated Program Assets for Sharing
Other Available Assets
SATOPS Common User Core

Figure 4. Interoperable Satellite Control Network (ISCN) Antenna Architecture.

As the ISCN evolves, it will maintain compatibility with legacy systems and users (e.g., existing on-orbit and in-production satellites that would be cost prohibitive to change). To alleviate potential concerns over a loss of control of resources that individual SCNs currently enjoy, support prioritization and resource scheduling will continue via the same processes used today, that is, each SCN will continue to have first priority on its own resources. In that way, ISCN will allow users to maintain priority control over owned resources while simultaneously gaining the ability to access any unscheduled capacity across the entire interoperable network. ISCN will provide the USG the ability to maximize use of idle capacity from a federation of interoperable USG networks assets. It should also be noted that even under an ISCN construct, some dedicated mission networks may have a need for access to the ISCN but will operate their dedicated network autonomously, outside the ISCN architecture due to their unique mission requirements.[11]

The ISCN will consist of a mix of participating organizations' terrestrial-based fixed sites and transportable assets, communications links and/or space-based TT&C data relay assets to meet required capabilities. User needs and cost-as-an-independent-variable analyses will be used to determine the optimal mix of resources. Any ISCN-C augmentation (e.g., adding additional non-AFSCN antennas with different sets of capabilities) will be accomplished so as to prevent any mission assurance degradation to assigned programs or users (figure 5).

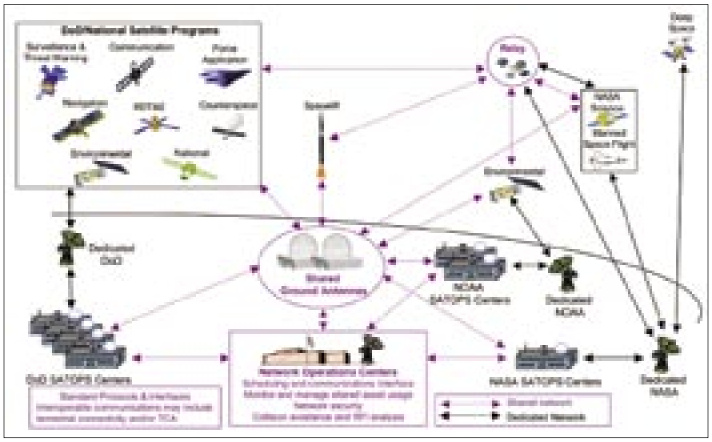


Figure 5. ISCN Future Architecture.

While the potential operational benefits, increased resource effectiveness, and cost efficiencies of the ISCN concept are promising, the ISCN brings with it its own set of significant challenges:[12]

1. **Security/Vulnerability of Assets.** In order for the ISCN to function properly, the challenge of working with multiple organizations with differing security levels and processes must be addressed. For example, information assurance, certification, approval-to-operate, and cross-domain solution issues that come with mixing DoD and civil assets must be resolved. Additionally, increased dependency on non-DoD resources will increase denial of service risks. Signal, data, and site protection are also risk areas that will need to be resolved. DoD operational security must be maintained, even when using civil resources.
2. **Cryptographic Standards.** DoD space policy requires encryption and decryption in satellite ground systems to ensure secure communication with National Security Space (NSS) satellites. However, most existing civil antennas currently do not support encrypted operations, which would significantly limit the ability for NSS satellite programs to use these sites. This limitation must be overcome to ensure

interoperability across the ISCN.

3. **Spectrum Availability.** US government agencies including DoD and civil communities primarily use either the Space-Ground Link Subsystem (SGLS) (1.76 to 1.84 GHz) or Unified S-Band (USB) (2.025 to 2.120 GHz) frequency band to perform uplink functions. Both SGLS and USB share the same 2.2 to 2.3 GHz frequency band for downlink functions, albeit with different modulation schemes. Without national and international regulatory spectrum protection, assured access to satellites could be jeopardized. This is increasingly true with the commercial crowding of the bandwidth adjacent to SGLS frequencies and USB frequencies which are shared with commercial enterprises. The associated financial and national security implications make this a currently growing issue with legacy space systems using these frequencies.[13]
4. **Communications.** Various SCNs have differences in communications system operations concepts, processes, and philosophies. The ISCN must update communications capabilities to provide the diverse routing, redundancy, and capacity necessary to support all assigned user requirements, including on-demand access to users' satellites.
5. **Formal Coordination Process.** The DoD, national, and civil agencies have different requirements for acquisition documentation, operations and planning. Extensive coordination with all participating organizations will be required for successful ISCN operations. This coordination effort will also be critical to ensure planned upgrades to existing individual systems contribute to ISCN interoperability whenever possible.
6. **Funding.** As always, with most programs or initiatives, funding will be a prime concern. Funding for ISCN is further complicated by the nature of the multiple organizations and agencies directly involved in the effort. Funding for various elements of the ISCN will be organizationally dependent and may not be available based upon other organization priorities and/or mission needs. Sufficient funding from all participants will need to be secured to ensure overall ISCN user needs are met.

Fortunately, to help overcome the enormity of resolving all of the above mentioned challenges simultaneously, the ISCN evolution will occur incrementally with system architecture being a key component. Cooperative efforts are already underway among many USG satellite operations providers (e.g., Air Force, Navy, NASA and NOAA) to implement this ISCN concept. For example, the AFSCN provides NASA with launch and manned-flight support, as well as support to NASA and NOAA satellites. Additionally, the Navy has been using AFSCN ground resources to support its satellites for several years. Furthermore, this evolution of cooperation is not without precedent, as evidenced by USAF operation of the spacelift ranges by the 30th and 45th Space Wings at Cape Canaveral AFS, Florida and Vandenberg AFB, California that support all USG missions as well as commercial customers. The ISCN is merely the next logical step in this ongoing cooperative effort.

In a recent interview on the subject of USAF programs whose costs continue to soar, Air Force Chief of Staff, General T. Michael Moseley stated, "It's time to be killing things," and said that some USAF programs may have to be sacrificed for budget reasons. He went on to say that everything will be under review and one of the first areas he specifically intends to look at is "how we leverage capabilities."[14] That is exactly the focus of ISCN. The question will no longer be, "Do we really need to maintain multiple independent government networks providing similar capabilities?" but rather, "Can we afford it and defend it in upcoming program reviews?"

In this fiscal environment, the ISCN is uniquely positioned to simultaneously increase the capabilities of a number of independent USG SCNs by leveraging the capabilities among all of them. ISCN is now not only a concept to enhance future space operations, but may well be a concept of fiscal necessity.

Maj Michael J. Dunn (BS, Southern Illinois University; MAS University of Montana) is Deputy Chief, Satellite Command and Control Branch, C2, Communication and Navigation Division, Directorate of Requirements, Headquarters Air Force Space Command, Peterson AFB, Colorado. In this capacity he is responsible for developing and documenting requirements for the Air Force Satellite Control Network in support of DoD, civil and national users. Major Dunn has previously served as Commander, Guam Tracking Station; Operations Flight Commander and Chief Stan/Eval Section, 22nd Space Operations Squadron; and Missile Operations Support Flight Commander and ICBM Instructor/Evaluator Crew Commander, 12th Missile Squadron. Major Dunn is a graduate of Squadron Officer School and Air Command and Staff College.

Notes:

[1] CAPT Jack Snowden, John Rush, Bruce Needham, *SATOPS Architecture Transition Plan*, OASD C3ISR&Space, NASA, NOAA, 17 November 2000.

[2] Ibid.

[3] Maj Todd Thompson, *NSSPA - FY07 APOM, AFSCN Operations*, AF/XOSSO, Jun 2005.

[4] Snowden, Rush, Needham, *SATOPS Architecture Transition Plan.*

[5] Ibid.

[6] Maj Dominic R. Saymo, *Enabling Concept For An Interoperable Satellite Control Network (ISCN)*, HQ AFSPC/XOR, August 2005, draft version 2.2.

[7] Arthur L. Money, *SATOPS Architecture Implementation Memorandum*, National Security Space Steering Group, 17 November 2000.

[8] Snowden, et al., *SATOPS Architecture Transition Plan.*

[9] Brig Gen Michael A. Hamel, *Implementation of SATOPS Architecture Transition Plan*, HQ UASAF/XOS, 9 February 2001.

[10] Snowden, et al., *SATOPS Architecture Transition Plan.*

[11] Saymo, *Enabling Concept*

[12] Ibid.

[13] Arthur L. Money, *Satellite Operations Architecture Study*, OASD C3I, 7 February 2000.

[14] Michael Fabey,"Air Force's Top Officer Notes Need for Program Cuts," *Air Force Times*, October 2005.

Command and Control: The Future of Space

Col Jay G. Santee, USAF
Commander, 21st Space Wing
Peterson AFB, Colorado

At a recent Air Force Space Command (AFSPC) Commander's Call, General Lance W. Lord described one of the most significant changes in AFSPC he had witnessed during his tenure as commander. When he first came into command, space was not recognized as a warfighting medium. Today however, "Space is a warfighting medium on equal footing with air, land, and sea."[1] One indicator that space is on par with the other warfighting mediums is that we now have a joint commander for space forces.

On 18 May 2005, US Strategic Command, Joint Functional Component Command Space and Global Strike (JFCC SGS), appointed the Commander, 14th Air Force (14 AF) as the Commander, Joint Space Operations (CDRJSO). In the appointment letter, the CDR JFCC SGS outlined the CDRJSO responsibilities:

> Provide space planning and operations support to the CDR JFCC SGS in crisis action planning, development of deliberate plans and establishing/supporting directives, exercise planning and participation, and developing recommendations for space policy, guidance, and doctrine. To achieve the desired objectives and priorities, the CDRJSO is authorized to collaborate and coordinate across JFCC SGS staff, contributing service component staffs assigned to USSTRATCOM and their respective operations centers, combatant commanders [through the Space Coordinating Authority (SCA)], and other DoD and non-DoD partners to ensure unity of effort in support of military and other national security operations.[2]

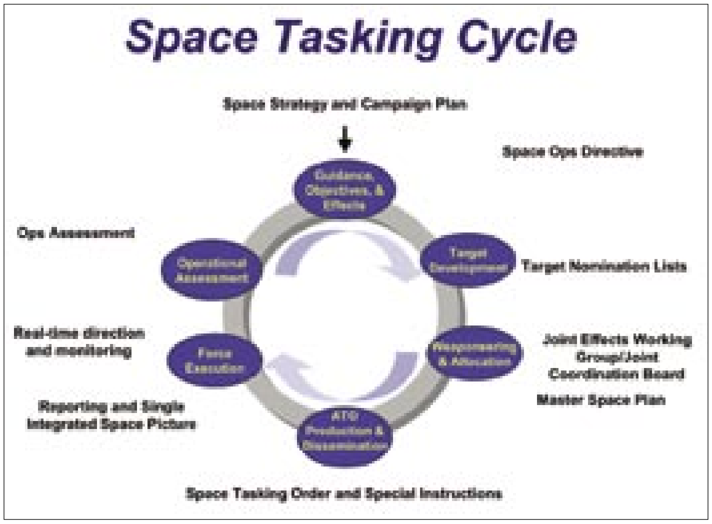
Appointment of the CDRJSO is historically important because it appoints a single joint commander responsible to integrate all available space capabilities into an optimized plan and to maximize the overall effect in theaters given a finite amount of space capabilities. On 30 November 2005, the JFCC SGS delegated tactical control (TACON) to the CDRJSO those units that produce space superiority, Global Information Services, and Global Surveillance, Tracking, and Targeting effects.[3] TACON authority allows the CDRJSO task forces to produce effects for multiple theaters around the globe. It is important to remember that space effects are inherently global because a single space capability has the potential to produce effects locally as well as throughout multiple theaters simultaneously.[4]

Finally, the production of space effects is a joint endeavor. There is hardly a space effect that is produced by a single Service. With the appointment of the CDRJSO, we are now able to integrate and optimize multi-service space capabilities to produce and enhance our Nation's space effects. An example of multi-service effects is Global Infrared Surveillance, Tracking, and Targeting. This involves assets from our Air Force, Air National Guard national space systems as well as the Army-Navy Joint Tactical Ground Station (JTAGS).

Mission of the JTAGS is to provide theater with real-time alerting, warning, and cueing of TMB launches and other tactical events of interest.[5]

It requires multiple satellite communication (SATCOM) lines to deliver information across services and throughout theaters. The CDRJSO has the authority to integrate these multi-service space assets to support multiple theater operations with missile warning. The appointment of the CDRJSO establishes a single joint commander responsible for ensuring competing priorities are resolved and that the highest priority is accommodated with optimized space capabilities for successful in-theater results. The establishment of a Joint Space Operations Center (JSpOC) in May 2005 is important to the CDRJSO to carry out these actions.

Under previous command and control (C2) architectures, daily space operations were heavily stove piped dependent upon mission and sensor types. Units performing space surveillance could and did receive taskings from many agencies including USSTRATCOM, USSPACECOM, AFSPC, 14 AF and the Space Control Center. The recent activation of the JSpOC is a watershed event, altering the basic C2 construct of US space operations and aligning it with proven structures. The new C2 structure has established a single tasking authority, simplifying the tasking process and eliminating confusion and frequent conflicts. The JSpOC is organized with processes modeled after Falconer Air Operations Centers (AOCs) and is well adapted for today's global operations. The JSpOC plans and fights using a Strategy division, Combat Plans division, Combat Operations division, and Intelligence, Surveillance, and Reconnaissance division. Much like the AOC Strategy division, the JSpOC Strategy division looks ahead of the current tasking cycle to determine theater needs. The Combat Plans division develops the Space Tasking Order and the Combat Operations division adjusts the tasking based on changes to the theater situation. The results then go back to the Strategy division to analyze and incorporate any lessons learned.


Space Tasking Cycle
Space Strategy and Campaign Plan
Space Ops Directive
Guidance, Objectives, & Effects
Target Development
Target Nomination Lists
Weaponeering & Allocation
Joint Effects Working Group/Joint Coordination Board
Master Space Plan
ATO Production & Dissemination
Space Tasking Order and Special Instructions
Force Execution
Real-time direction and monitoring
Reporting and Single Integrated Space Picture
Operational Assessment
Ops Assessment

The space tasking cycle has six major phases just like the air tasking cycle.

Additionally, the JSpOC has the Nation's only Space Intelligence organization focused on the operational level of war. This division is responsible for the gathering and analyzing of all-source operational intelligence to support global space missions.[6] This information is critical to our space surveillance, offensive counterspace, and defensive counterspace units providing space superiority to theater warfighting. Organized with proven processes, the JSpOC allows the CDRJSO to look to the future and rapidly react to opportunities and/or threats such as new foreign launches or a downed pilot in theater. With the ability to task joint space capabilities, the JSpOC provides the venue for the CDRJSO to quickly cope with changing theater battle. Accounting for both planning and execution, and serving as a single reach-back point for theaters, the JSpOC provides the necessary integration of space capabilities and commander accountability, at the operational level of war.

Space operators execute the Space Tasking Order on the combat ops floor of the JSpOC.

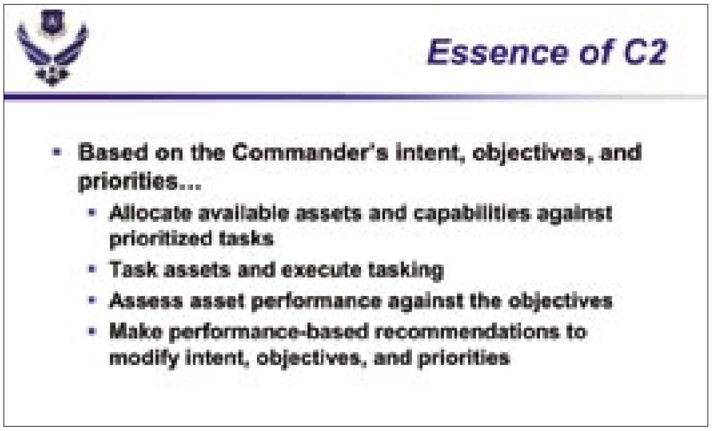
Levels of War: An Airman's View

"The focus at a given level of war is not on the specific weapons used, or on the targets attacked, rather on the desired effects."[7] At the **strategic level** of war, we address why we will fight and what resources we will use, along with identifying why the adversary is fighting against us. The **tactical level of war** resides at the opposite end of the spectrum, and from a space perspective, focuses on how space capabilities are employed, the specifics of how they are employed, and on what targets we will focus our efforts. Tactical level warfare is how we fight the war. In between the strategic and tactical levels of war lies the **operational level**. The operational level of war takes the 'why' from the strategic level and determines the 'what': what we will attack, the order, and for how long. "Operational art is the process of planning and sustaining operations and campaigns to meet strategic objectives; it is the process by which strategic guidance is turned into tactical tasking."[8] In the past, space C2 was executed from the strategic level directly to the tactical level.

Our space forces are integrated, synchronized, and deconflicted for maximum battlespace effect. Still in a period of rapid growth, the JSpOC has assumed the premier role of linking tactical space operations to its strategic intent. It is the center of the operational art translating the national-level strategy and combatant commander's requirements and intent, into clear, attainable military objectives, tasking, and combat assessment. Once planned, tasking flows to the numerous weapon system units for execution.

Although we focus on theaters effects from space capabilities, the CDRJSO is also responsible to other commanders, organizations, and entities that need joint space capabilities to produce space effects needed to accomplish their missions. For example, NASA coordinates shuttle launches through the JSpOC to ensure blue force assets are available to track the launch, mission, shuttle reentry, and conduct collision avoidance. This type of operational coordination ensures the safety of both the shuttle and our blue force assets. Additionally, it assists NASA in completing their mission(s). The Missile Defense Agency (MDA) also utilizes the JSpOC and CDRJSO authority to execute their mission(s). Tasked with missile defense acquisition, the MDA coordinates with the JSpOC in order to integrate testing and training of their upgrades to space systems like the PAVE PAWS Radar operated by 7th Space Warning Squadron at Beale AFB, California. The CDRJSO is responsible for ensuring the unit is available to perform its missile warning mission, as well as ensuring the MDA can perform its necessary testing/training. Coordination at the operational level ensures both missions can be executed. NASA and the MDA are just two examples of non-theater entities utilizing the operational planning conducted by the JSpOC and executed by the CDRJSO. Whether it is to produce theater effects or support other organizations space missions, for the first time in space history, we are actually applying the operational art of war in and for space.

Although we have made vast improvements in properly aligning space C2, we still have room to grow and mature. USSTRATCOM continues to evaluate and adjust the space assets assigned or attached to CDRJSO. Additionally, USSTRATCOM, JFCC Space and Global Strike, and CDRJSO continue to strengthen relationships among other mission partners that contribute space capabilities to the space mission. Some of these partners include the NRO, NOAA, MIT/Lincoln Labs, and AFRL. We also continue to work with other services to optimize our nation's space assets. Army Strategic Command will be moving four billets to the JSpOC in Summer 2006 to better integrate their space capabilities.[9] This is the first step in involving other services into space operational planning. This joint effort is important to space power being fully integrated and optimized into the fight in multiple theaters.



Essence of C2

- Based on the Commander's intent, objectives, and priorities...
  - Allocate available assets and capabilities against prioritized tasks
  - Task assets and execute tasking
  - Assess asset performance against the objectives
  - Make performance-based recommendations to modify intent, objectives, and priorities

The critical role of space and maintaining superiority within it has grown and taken on new dimensions for our military through the years. The Cold War, Operation DESERT STORM, Operation ALLIED FORCE, Operation ENDURING FREEDOM, and most recently, Operation IRAQI FREEDOM have demonstrated the growing importance space capabilities play in the fight. Parallel with this growth, have been mission reorganizations and additions in space doctrine, tactics, techniques, and procedures. Space C2 must now account for more missions, responsibilities, and organizations. As the battlespace expands and the demand for space effects grows, we find ourselves no longer executing in isolation, singularly or alone, but as part of a vast array of multi-service capabilities achieving mutually-supporting and synergistic global effects. Centralized control and decentralized execution, as embodied in the CDRJSO and the JSpOC function, provide the latest evolution in space command and control.

Notes:

[1] General Lance W. Lord, Air Force Space Command, Commander's Call, 17 February 2006.

[2] Lt Gen Bruce Carlson, Commander, Space and Global Strike, letter, 8 July 2005.

[3] Lt Gen Kevin P. Chilton, Commander, Space and Global Strike, letter, 30 November 2005.

[4] Air Force Space Command, Functional Concept for Command and Control of Space Forces, 6 October 2005, 6.

[5] John Pike, "JTAGS, Joint Tactical Ground Station," *FAS Space Policy Project, Military Space Programs,* http://www.fas.org/spp/military/program/warning/jtags.htm.

[6] Capt Floyd Melchor, 21 Operations Support Squadron, Intelligence Flight, 1 March 2006.

[7] Air Force Doctrine Document 2, *Organization and Employment of Aerospace Power,* 17 February 2000, 2-3.

[8] Ibid.

[9] Col Mark P. Jelonek, Commander, 614th Space Operations Group, 2 March 2006.

Col Jay G. Santee (BS, Geography, USAF Academy; MBA, Golden Gate University, California) is Commander, 21st Space Wing, Peterson Air Force Base, Colorado. The Air Force's largest wing geographically and organizationally, which consists of a work force of more than 5,000 officer, enlisted, civilian and contract employees. Spanning the globe this team provides missile warning and space control for combat forces and the national command authorities of the United States and Canada. Colonel Santee entered the Air Force as a distinguished graduate of the United States Air Force Academy in 1981. He performed flying duties in a variety of aircrew positions in the F-111 and EF-111. While on the staff of the Assistant Secretary of the Air Force (Acquisition), he served as a Program Element Monitor and the Assistant Secretary of the Air Force (Acquisition) liaison to the Department of the Navy Research, Development, and Acquisition staff. He is also a joint duty officer, having held a staff directorship at USSPACECOM. Colonel Santee has served as commander of a space warning squadron and space operations group; as the Chief of Operations for 14th Air Force; and as Director of the 14th Air Force Air & Space Operations Center during Operation IRAQI FREEDOM. Colonel Santee has more than 1,800 flying hours with more than 120 during combat. Colonel Santee is also a Distinguished graduate of Squadron Officer School and National War College.

Rainbows in the Firmament: The Blurring of Fantasy and Reality in Visualizing the Future of Humanity in Space

Roger A. Beaumont, PhD
Professor Emeritus of History (retired)
Texas A&M University

". . .the fantasies of Star Wars aren't all far-fetched – and some are getting less so with each passing year"[1]
- Theo Emery

The Duke of Wellington's aphorism about the need to perceive what is happening on "the other side of the hill" identified a primary dilemma for military and naval commanders throughout history, one which has been compounded again and again as warfare became increasingly fragmented and dispersed during the last two centuries or so. Some of the ongoing transition in organization and battle formats was obviously due to technologies of transportation and communication extending range and speed, and some of it because of the growing destruction power of weapons and the consequent need to minimize observation. Both "haves" and "have-nots" have had to grapple with instabilities generated by technical advances that when they first appeared seemed to give an overwhelming advantage to the "haves," but which failed to do so repeatedly. It is not at all clear how the movement of military operations into space is likely to alter that chronic imbalance. But it does seem wholly safe to predict that as difficult as it has been in the past for those responsible for the higher direction of war to visualize its intricate dynamics, the militarization of space will compound that dilemma at least an order of magnitude or two during the next generation, and even further beyond that.

A basic dimension of that unfolding quandary is one that has been visible throughout much of military history—the lack of a shared vision of what is happening, a chronic problem in the domains of tactics, operational art, and strategy. Even though we are almost a century into the "Space Age," the boundaries between solid concepts and actual technology, history, and fantasy remain blurred.[2] That is in good part due to the fact that for literally millennia, imaginary excursions to the cosmos were gossamer fantasies that lacked practical import, from the Egyptian pharaohs' solar boats to Cyrano de Bergerac's ascent to the moon, first by floating atop the rising morning mist, and again by using the detonations of firecrackers.[3] What seemed to be more accurate visions of moving out into space appeared in the early 1800s as an expanding flow of mechanical and electrical innovation inspired authors like Edgar Allen Poe and Jules Verne to concoct depictions of space travel that evolved—and not always on an upward trajectory, to what, in the early 20th century, Hugo Gernsback, a pioneer in the genre, christened "science fiction." That inadvertently led to a smudging of the lines between imagination and reality, even though much early science fiction was deemed "trash" and appeared in pulp magazines or comic strip format. Adding to the confusion, not only did fantastic imagery dominate public perceptions of space, but sometimes became a kind of ideational test bed, usually inadvertently, but also intentionally. John Campbell, editor of *Astounding Science Fiction* magazine, for example, often challenged writers to solve puzzles, quandaries and paradoxes that he set before them. At the same time, after World War I, as both fanciful and concrete views of the "conquest of space" were nudged along by an ascending curve of space-linked science and technology, some of that proto-science fiction served to attract young, intelligent, and impressionable readers to careers in science. And various writers of "serious" literature like E.M. Forster, in "The Machine Stops," Aldous Huxley, who was raised in the domain of "hard" science, in *Brave New World and Ape and Essence*, and George Orwell in *1984*, harnessed the "sci-fi" genre to what they saw as more serious literary purposes.

Although the US ultimately became the dominant player in the "conquest" of space, that rise to eminence was not foreseen in the 1920s and '30s, even though research under official sponsorship, like government support of Robert Goddard's liquid-fueled rocket developments, did sometimes come into public view. Some of the modernist efforts of German and Austrian pioneers also appeared in graphic media and film, and some reasonably accurate forevisions of what actually transpired during the next half-century appeared from time to time, like the American Interplanetary Society president David Lasser's *The Conquest of Space*, published in 1931.[4] During the Great Depression of 1929-42, an expanding torrent of modernist imagery influenced art, architecture, design and public taste as the streamlining fad of that era culminated in elaborate displays at the New York World's Fair of 1939-49, and in the mass marketing of objects from pencil sharpeners and automobiles to civil aircraft as well as military planes.

And then there were the films.[5] From the early 20th century onward, in Europe and the US, movie producers exploited the theme of space travel with widely varying degrees of skill in filmmaking and marketing and imagination—not always the same thing. Production values were sometimes inversely related to content in the age of the grand studio system when filmmaking was usually far more a business than an art form. In contrast with European "realistic" space films of the '20s and '30s like *Metropolis, Rocket to the Moon*, and *The Shape of Things to Come*, Hollywood's futurism fell well short of the more technically credible imagery of European filmmakers, let alone the relatively high quality of Hollywood's better "A" pictures. Nor did America's film industry catch up all that quickly with the arrival of the Space Age during World War II when the Nazis used strategic rockets, or in the immediate post-war years when an expanding torrent of science fiction paperback books and magazines appeared. Practitioners often moved ahead of the visionaries, as when Army Air Forces' Chief Henry H. "Hap" Arnold adumbrated a constellation of "blue sky" space-related concepts and projects that laid the foundations for work done by such luminaries as Professor Teodor von Karman, and General Bernard Schriever. Throughout the late 1940s and into the '50s, newsreels often outdazzled movies, as many American space films continued to reflect the melodramatic "gee whiz" tone of comic strips that had set the tone for Flash Gordon and Buck Rogers "space opera" serials. At the same time, the growing sophistication in hard-core science fiction—based on a firm scientific basis—was reflected unevenly in less than wildly popular radio shows like *Dimension X*, and such futuristic television series as *Tom Corbett, Space Cadet,* and *Men in Space*.

> *"Space is as different from the air as it is from the sea and the ground"*
>
> - John Pike

The popular image of space exploration during the late 1940s and early 1950s included a series of books by Willy Ley, illustrated by Chesley Bonestell, and Noel Sickles' remarkable illustrations in *Life* magazine of a notional moon mission which depicted human excursions into space in serious and credible images.[6] Although some science fiction writing of that era steered very close, both in tone and prescience, to that of the final phase of the Cold War,[7] Hollywood was still struggling to catch up. The highly touted and heavily animated film *Destination Moon*, for example, got some of the technology right, but the plot was laced with the old "gee whiz" flavor, and cornball vaudevillian humor. In essence, the more "serious" space and futuristic films of the late 1940s resembled the pacifist aviation movies of the '20s and '30s in their tendency to mix depictions of "neat" technology with moralizing, as in *When Worlds Collide*, or anti-war or anti-nuclear themes, like *The Day the Earth Stood Still, The Thing*, and *Rocketship XM*. Nevertheless, some filmic efforts of the early 1950s managed to gain some figurative altitude stages both in terms of production values and subtexts in Hollywood, for example, *Forbidden Planet* (loosely based on Shakespeare's *The Tempest*), *Destination Moon,* and the early 1950s modernized version of H.G. Wells' *War of the Worlds*.

Despite the deep secrecy surrounding the building and testing of atomic and hydrogen bombs and rocketry, fragments of those prodigious scientific and technical efforts occasionally came into public view.[8] But it was in the autumn of 1957 that anxieties surged most sharply in the US after the USSR orbited *Sputniks I* and *II*, the first non-lunar earth-orbiting space satellites, and again when Soviet cosmonauts ascended into space in the early 1960s, and during and after the Cuban Missile Crisis of October 1962. From the late 1950s onward, threads of fantasy, science, and national security became confusedly entwined against the backdrop of Cold War rivalry. During the "space race," as the American *Apollo* program strove to land humans on the moon despite an apparent Soviet lead, popular culture portrayals of a space-oriented future in the Western bloc, again, of varying quality and credibility, included the *Star Trek* television series, and Stanley Kubrick's *A Space Odyssey: 2001*. Western European variants ranged from the French comic strip and movie *Barbarella*, and British comic strips *Dan Dare* and *The Trigan Empire*, and such space-oriented films as the *Quatermass* series and the American-produced *Space Odyssey* which, along with *Dr. Strangelove*, laid the foundations of a special effects sub-industry in Britain that flowered in the wake of George Lucas' *Star Wars*. In the Eastern bloc, "Socialist" forevisions were shaped by a popular state-sponsored program of subsidized science fiction writers like Stanislaw Lem, who assailed the imperialist and militarist flavor of Western versions of the genre, and propounded idealistic and collectivist values.[9] Although there were strong lines of conquest and chauvinism in western military science fiction, and much plotting was based on imperialistic models,[10] anti-war, anti-nuclear counter-trends merged during the Cold War,[11] and richened during the Vietnam era.[12]

Alongside those diverse developments was the growth of a new scholarship aimed at serious consideration of such facets of popular culture as jazz, rock 'n' roll, comic strips, and science fiction.[13] Despite continuing estrangement from mainstream literature, some science fiction writers like Frederick Pohl, Isaac Asimov, Robert Silverberg, Harlan Ellison, and Arthur C. Clarke gained reputations in some circles for having greater *gravitas* than most of their peers in framing complex visions of the future.[14] At the same time, a *corpus* of intellectually rigorous space theory was emerging in the scientific communities of many countries, from the sober musings of Soviet space theorist Konstantin Tsiolkovski in the 1920s and '30s, to G. Harry Stine's *The Space Enterprise* promoted as "the first SERIOUS book of the Space Age" in 1981, and, more recently, Barry Watts's "Ten Propositions Regarding Space Power." Special recognition of the especially challenging technical aspects of space exploration was awarded in the domain of popular culture when the epithet "rocket science" became a common reference to the highest level of intellectual excellence.

But it was George Lucas' film *Star Wars* that brought science fiction sharply center stage in 1978 from its relative isolation on the margins of western literary and artistic consciousness, and transformed the genre. Beyond fueling public appetites for space-themed science fiction books and publications, art, comic strips, films, and games, Lucas' epic brought forth a torrent of emulators, and created a symbolic and terminological lexicon from which the Reagan administration chose "Star Wars" as the label for a proposed ballistic missile defense system in 1983. It also highlighted how much extent science fiction was meeting a cultural hunger for heroes other than the sanitized images of the fighter jock astronauts, which only partly offset the bland bureaucratic mien of the National Aeronautics and Space Administration (NASA). Originally created to stand separate from the armed forces, NASA's founding principle of openness was eroded through time by the US-Soviet space race, and the Cold War as American space efforts were increasingly bent to military functions, including reconnaissance and communications satellites, and classified space shuttle missions. By the end of the 20th century, few would recall that the American space program has been designed at the outset in 1958 to be open to public view, in the spirit of democracy, and to facilitate creativity through open exchange, while contrasting with, and thus embarrassing, the militarized Soviet space program.

Partly because of bureaucratic blandness, then, and the drift toward hypercrypticity during the Cold War and afterward, as the 21st century dawned, the longstanding loose blend of fantasy and "hard" science persisted, with some relatively bright threads visible in the otherwise dull tapestry, including the renewed American anti-ballistic missile defense program, Search for Extraterrestrial Intelligence, the rogue asteroid threat, and the spectacle of various nations and commercial aggregates, including "Thrillionaires," moving out into space, or at least announcing their intentions to do so.[15] Nevertheless, the gap between "the Space Program" and public perceptions of the complexities and nuances of space development continued to widen, despite attempts by analysts, popularizers, critics, and enthusiasts to reach broader audiences.[16] As increasingly esoteric technology moved further and further from easy public comprehension, and perhaps as a function of it, public perception of America's space efforts was being further clouded in the early 2000s by a resurgence of the anti-scientism that fueled the stereotyping of the "mad professor" in the popular culture of the late 19th and early and mid-20th centuries. And despite the cliché that studying history conveys a special wisdom to policy-shapers and decision-makers, it was not really clear how much value there was in seining the past to gain special perspective and/or wisdom.

In broader terms, the analytical landscape has long been clouded by the thin and fuzzy epistemology of extra-terrestrial power dynamics as noted by Barry Watts et al., and tendencies to rely on trend analysis, linearity, precision, quantification, and elegance of fit, epitomized in Ludwig J.J. Wittgenstein's admonition that: "Whereof we cannot know, thereof we should not speak," and Werner Karl Heisenberg's uncertainty principle, and evident in deep-seated fears of unfettered imagination in scientific circles.[17] Not only have fanciful visions often occasionally borne rich and varied fruit in the domain of space-related enterprises, but enthusiasm and optimism sometimes yield a kind of speculative fever, as those who witnessed the furor surrounding the issuance of Telstar stock in the mid-1960s will recall. In the domain of command-and-control a distorted variant of the classic GIGO "garbage-in garbage-out" cyber-acronym has appeared, a GO^{nth} effect, as apparently promising innovations amplify the noxious outflow, yielding relatively little of what appear—or are claimed to be—very promising results.[18] But not all visions of space have been viewed through rosy lenses. The winnowing shed of science fiction is bestrewn with utopias and dystopias, and various visionaries have depicted space exploration and settlement as a gritty and risky domain along the lines of Robert Heinlein's *The Moon is a Harsh Mistress*,[19] and the homestead in the first *Star Wars* film.

Considering the low batting average of soothsayers from shamans to modern "experts" and professionals, it is not unreasonable to ask how closely even the most serious and steady prognostications are likely to align with the unfolding of the "Space Age."[20] Guideposts are certainly not solid or evenly spaced. It is, for example, tempting to review the history of the rise of air power when considering the future of armed forces in space,[21] especially the senior airmen's battle for institutional independence between the World Wars which led them to forge close links with industry in the Army Industrial College, and then with the media and Hollywood, as they did when they struggled after 1945 to be primary wielders of strategic nuclear weapons. But whatever the congruence between past instances and impending contingencies may appear to be, the matrices vary widely, perhaps moreso than any differentiation in terrestrial cases, and are likely to more and more over time. To further complicate the picture, America's involvement in space has oscillated from enthusiasm to indifference and hostility, with brief tumults spiking amid the long intervals of calm, for example, the *Gemini* and *Apollo* missions, the 1978 *Cosmos* crash in Canada, and the two tragic shuttle losses.

Despite a host of documentary films, TV docudramas, and "accurate" feature films like *Apollo XIII*, the imagic landscape of space, from cable television to computer games, continues to be heavily dominated by fictional imagery that plays a major role in shaping the general public's view of exterrestrial matters. And despite the events of 11 September 2001, there seems to be little awareness that the apparent calm in the cosmos – or inner space – might suddenly erupt into an unstable if not a cataclysmic state. Nor, as Air Chief Marshal Burridge has suggested, does much consideration seem to be given to "the granularity of aerospace," already visible in the realm of military aviation in the "morality of altitude dilemma," and the convoluted exegesis arising from the unmanned aerial vehicle phenomenon.[22] If history really offers any perspective on the vastness and complexity of the context of space and the broad range of contingencies, the potential for deception in space can be considered in light of the studies of surprise by such analysts as Barton Whaley, Richard Betts, Michael Handel et al., and the increasing frequency and effect of strategic surprises in the 20th century. Grand spoofs like the Channel Dash of 1942, the first use of radar chaff – WINDOW – in 1943, and Operation FORTITUDE, the deception plan for the Normandy invasion in 1944 each left the targeted opponent staggering blindly for a critical period. The befuddled activity in upper echelons of government in the immediate aftermath of such mega-surprises is all the more disconcerting considering that rigorous weighing of contingencies has been common practice at the highest echelons of government and military services for several centuries.[23]

Moving from the uncertain utility of history to the relevance of more immediate experience, arguably the most pertinent dilemma in projecting military force into space is the limited ability—or lack of it altogether—of human reflexes and capacities to deal with stimuli already visible at less complex and far slower speeds and in much smaller matrices than those that are likely to be encountered in space operations. Problems with an operator's coping appear when less than a dozen elements are involved, especially when human controllers are affected by fatigue, fear, overload, and/or distraction, whether those are inadvertent or deliberately imposed by an adversary. A central dilemma here, one in view since the antiballistic missile or ABM debates of the 1960s and '70s, and threaded through the corpus of science fiction as well, is how much strategic command-and-control should be assigned to non-human systems. Some analysts argue that however powerful automatic control becomes in the "information age . . . there are some fundamental reasons why humans must retain their role in command."[24] As understandable as such an assertion may be in political and diplomatic terms as a statement of policy if not actual practice, such delegation of authority has been happening throughout the "machine age," from steam engine governors, and automatic elevators to unmanned buoys, beacons, traffic lights, and air control systems.

In considering what lies ahead–or above–us in the mists of unpredictability, it may be useful to consider that in the domain of military history, for whatever it may be worth, increases in technical capacity have not always outweighed less tangible elements like resolution, tenacity, and creativity.

Considering the ever-widening gap between operational speeds and reliability of automatic control devices on the one hand, and the relatively fixed limits of human capacity, augmenting the latter by conditioning, personnel screening and selection, and pharmacology seems to have been falling further and further behind the curve of technical advances for a long time. From 1942 to 1946, for instance, combined speeds of opposing air elements in daylight bombing raids over Germany from 1943-45 exceeded 600 miles per hour, and less than two decades later, Intercontinental Ballistic Missile launch-to-impact was estimated at 45 minutes. But despite that, many analysts and actors seem to remain confident that human controllers of increasingly advanced technological systems can monitor, weigh decisions, override, or otherwise cope with the complexity and blinding speeds in crisis and battle management in space.[25]

At least some of that may be due to growing faith during the last generation among American elites in diverse aggregate intelligences producing optimal solutions.[26] But it remains unclear how much terrestrial and aviation history or any of the myriad fantastic visions in space fantasy and science fiction will provide any significant wisdom and/or foresight in our trying to foresee what is likely to happen in space. The bewildering array of visions, from the wildly imaginative and apparently absurd to serious and sober derivatives of the *corpus scientiarum* makes it all the harder for an aspirant Carl von Clausewitz or Alfred Thayer Mahan to grapple with the challenge as he or she stands on a figurative diving board from which it is too dark to see how far below the figurative pool is, how deep it is, or with what it may ultimately prove to be filled. Like Clausewitz and Mahan, he/she is facing a complex mix of scientific and technological solidity and "fuzzy" factors. For example, it is not clear how various sub-sectors of humanity will feel—or do feel—about a particular nation's gaining that transcendent high ground. After all, not everyone looking ahead—or up—has been convinced that Earth's civilization has reached the point where thrusting it out toward the cosmos is all that good of an idea.[27] Nor is it evident how the fabric of space powers' national culture and politics may be affected. To fall back on history, will it be as profound a warping experience as it was for the nations who sent galleons and caravels and gunboats and dreadnoughts out to distant lands? Should the vast difference between astrolabes and global positioning systems make us confident that we will be able to anticipate turns of fate beyond Lagrange libration points more effectively than Prince Henry of Portugal, or the worthies in the court of Aragon and Castile hoped when they passed through or by the Pillars of Hercules? How can we be sure how analogous we are to Portugal, Spain, or Britain, and that the extraterrestrial Great Game that lies at hand will be as well thought out as previous extensions of power were?

In considering what lies ahead – or above – us in the mists of unpredictability, it may be useful to consider that in the domain of military history, for whatever it may be worth, increases in technical capacity have not always outweighed less tangible elements like resolution, tenacity, and creativity. From the Sumerian clay tablets onward, it has been a virtual truism that the powerful and intricate norming pressures within hierarchies and bureaucracies often impede forevision and adaptability, and that stratification places premiums on serious demeanor, moderation, and predictability. Vendors, with their reflexive optimism, have always been with us, and may always be, out unto other galaxies. Despite all the attempts to bring such complexities under coherent authority, many things have remained "out of synch," out-of focus, and/or out of control. Major powers' superiority in wealth and technique has chronically been outweighed by the ingenuity of poorer and smaller adversaries and small states. It is hardly surprising, then, that analysts have pointed out potential pitfalls of "weaponizing space."[28]

The tangle of paradoxes and contradictions highlights the broader challenge posed by the advance, climb or whatever term most aptly applies to humankind's movement into space: how much of it will be continuity, and how much change? At the turn of the 21st century, it is not clear just how hardy or "robust" the US military space program or those of other nations really are.[29] Nor is it clear, despite manifold attempts to foresee what military operations in space might look like, how things are likely to unfold in the new ambience. The movement into space is diffuse, inchoate and highly complex, like the great whirling firmament of thousands of pieces of "space junk." Analysts and practitioners share little in the way of a common view of how things are going. As in the era of ascendant air power, poses of confidence and assertiveness in military and aviation sub-cultures slide past such problems as the lack of common understanding of terms and effects, especially the failure of lexicons to dovetail under conditions of stress and pressure, and the persistence of Clausewitzian friction. Transcripts of nuclear power plant failures and crises aboard air and space craft drive home the latent chaos that lies beneath polished shining structures, mechanical and organizational, and emerges full-blown and instantaneously in the heat of crisis and battle, bearing out General Walter Bedell Smith's adage dictum that scared people don't think very clearly.

As suggested earlier, a central emergent dilemma here is what fractions of the movement into space will be discontinuity versus extrapolation, that is, which visions, models, and experiences will apply to contingencies. The mish-mash of concepts, visions and techniques in the subcultures of air and rocket forces, and other space-linked bureaucracies has long been visible,[30] along with the related question of how much military history and its derivatives like "operational art" and "effects-based strategy" are likely to apply to such a different milieu.[31] Alongside a growing sensitivity to growing complexity and associated subtleties and ambiguities,[32] and the expanding forest of terms and acronyms,[33] lies the long-standing dilemma of whether a separate uniformed space service should be created, and, if so, whether it should be more of a paramilitary constabulary force like the Coast Guard than another armed service.[34]

On a parallel but contrary path lies a growing resistance to "militarizing" space, as though that trend has not been under way for more than half-a-century.[35] Linked to that are fears that it might trigger catalytic war,[36] and the hope that technical complexity and internal contradictions of such efforts will ultimately confound militarization,[37] or at least blunt its side-effects.[38] What effect such contrary currents have had or may have on the momentum of space excursions—and how deep and fast they may be running—is, of course, immeasurable. To further cloud the landscape, all the diffuse and intricate images of the extraterrestrial future, fanciful and scientific alike, have added to the confusion regarding what things are likely to look like, including which new players may come on to the proverbial playing field or leave it, or what technologies or paradigms will appear that will tilt it or alter it altogether. And it will bring us closer to determining the dimensions of Shakespeare's vision of "more things in heav'n and earth" than we have dreamed of in our philosophy–actual or fanciful.

Notes:

[1] Theo Emery, "Sci-fi Fantasies Merge with Scientific Realities," *Houston Chronicle*, 27 November 2005, J 11.

[2] For a brief overview, see Bob Preston et al., "Background," *Space Weapons/Earth Wars* (Santa Monica: RAND, 2002), 5-22.

[3] Science fiction bibliographical sources include several encyclopedias, numerous websites, and such individual surveys as Kingsley Amis, *New Maps of Hell* (New York: Ballantine Books, 1960), Sam Lundwall, *Science Fiction: What It's All About,* (New York: Ace Books, 1971); Reginald Bretnor, ed., *Science Fiction: Today and Tomorrow* (New York: Penguin, Books, 1974), and Lester de Rey's *The World of Science Fiction* (New York: Ballantine Books, 1979).

[4] David Lasser, *The Conquest of Space* (New York: Penguin, 1931). As a glance at World-Wide Web book markets will show, it has become a *rara libris*.

[5] For a list, albeit incomplete of space films, see Windows to the Universe, http://www.windows.ucar.edu.

[6] E.g., see Willy Ley, *Rockets, Missiles and Space Travel* (New York: Viking Press, 1961).

[7] A salient example is C. M. Kornbluth's *Not This August*, originally published in 1951, and reprinted and revised three decades later by Pinnacle Books.

[8] E.g., James H. Straubel, et al., *Space Weapons: A Handbook of Military Astronautics* (New York: Praeger, 1959). Less visible was the furor in the upper echelons of the American national defense nexus created by the Soviets development of ICBM-related technology before and after Sputnik 1.

[9] Contemporaneous anthologies include Isaac Asimov, ed., *Soviet Science Fiction*. Trans. Violet I. Dutt (New York: Collier Books, 1962), and *More Soviet Science Fiction*. Trans. R. Prokofieva (New York: Collier Books, 1962). For a view of Soviet futurology in the last days of the USSR, see Ninel Stretsova, *Looking Into the Future* (Moscow: Progress Publishers, 1987).

[10] E.g., Robert Heinlein's *Space Cadet* (New York: Scribner's, 1948); and *Starship Troopers* (Gordon Dickson's *Dorsai* series, Cordwainer Smith's "The Crime and the Glory of Commander Suzdal" in J. J. Pierce, ed., *The Best of Cordwainer Smith* (New York: Ballantine Books, 1975), 98-113, and David Drake's *Hammer's Slammers* (New York: Ace Books, 1979).

[11] E.g., Peter Bryant's *Red Alert* (New York: Ace Books, 1958)—the basis for the film *Failsafe*.

[12] E.g., Steven Utley and Howard Waldrop, "Custer's Last Jump" in Gardner Dozois, ed., *Best Science Fiction of the Year: Sixth Annual Collection* (New York: Ace Books, 1977), 39-90; Richard Lupoff, *Space War Blues* (New York: Dell, 1978); and Joe Haldeman's *Forever Wars* series.

[13] Two of the most salient "serious" anthologists of the 1970s and '80s were veteran science fiction writers Reginald Bretnor, who edited *The Future of War* trilogy, and Jerry Pournelle, compiler of the *There Will Be War* series.

[14] For a recent view of Clarke's role in shaping space technology, see Mark Williamson, "Extra-Terrestrial Relays the Legacy of Arthur C. Clarke," *Spaceflight* 47, no. 11 (November 2005): 420-25.

[15] John Schwartz, "Thrillionaires: The New Space Capitalists," *New York Times*, 14 June 2005, D 1; and Jan Reid, "Rocket Man," *Texas Monthly*, January 2006, 134-37, 204-06, and 235-36.

[16] The appearance of Reagan's "Star Wars" initiative in 1983 was not surprising to those among the general public who had been following trends noted by journalists for several years, e.g., n.a., "Bigger Role for Military in Space," *US News and World Report*, 26 April 1976, 67-8; Michael Mosettig, "Arming for War in Space," *Science Digest Special,* Spring 1980, 94-96; Robert C. Toth, "War in Space," *Science 80* 1, no. 6 (September/October 1980): 74-79; James Canan, *War in Space* (New York: Harper and Row, 1982); and the well-reported pronouncements of Air Force Generals Graham and Keegan.

[17] E.g., see Lorraine Daston, "Fear and Loathing of the Imagination in Science," *Daedalus* 134, no. 5 (Fall 2005): 16-30.

[18] A recent favorable view of network-centeric warfare, see Maryann Lawlor, "War Validates Netcentricity Concept," *Signal* 60, no. 3 (November, 2005): 17-22; for critical views of the continuing centralization-decentralization dilemma, see Robert L. Butterworth, "Centralizing Military Space is a Bad Idea," *Aviation Week and Space Technology*, 12 August 1996, 86. Benjamin S. Lambeth, "Viewpoint: The Downside of Network-Centric Warfare," *Aviation Week and Space Technology*, 2 January 2006, 86.

[19] Robert Heinlein, *The Moon is a Harsh Mistress* (New York: Berkley, 1966).

[20] Examples of such analytics include Francis X. Kane, "Space Age

Geopolitics," *Orbis*, Winter 1971, 911-933; Colin S. Gray and Geoffrey Sloan, eds., *Geopolitics: Geography and Strategy* (London: Frank Cass, 1999) and the journal *Astropolitics*.

[21] E.g., a proposal to re-orient from an "atmospheric " to an "infospheric Air Force," Martin C. Libicki and Richard Szafranski, "Tomorrow's Air Force," *National Defense University Strategic Forum* 79, July 1996.

[22] Brian Burridge, "Post-Modern Warfighting with Unmanned Vehicle Systems," *Royal United Services Institute Journal* 150 no. 5 (October, 2005): 22-23.

[23] In the late 1970s, something of a threshold was crossed by "top-ranking generals and advisors" published a highly detailed "realistic" scenario of the outbreak of nuclear war in Europe, Sir John Hackett, *The Third World War August 1985* (New York: Macmillan, 1979).

[24] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 118

[25] E.g., the recent conclusion of an analyst that: "As more individuals examine the information, and transmit their interpretations to others, the more likely it is that information will be accurately described by one or a combinations of several individuals, and efficiently used," Everett Carl Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (London: Frank Cass, 2005), 181.

[26] E.g., rational action, network-centered warfare, and situation awareness, and various paradigms of revolution and transformation; see Stephen Baxter's "A Human Galaxy: A Prehistory of the Future," *Journal of British Interplanetary Studies* 58, no. 3/4 (March-April, 2005): 138.

[27] E.g., a vintage darkling view of space colonization is Richard Lupoff's "With the Bentfin Boomer Boys on Little Old New Alabama," in Harlan Ellison, *Again, Dangerous Vision* (Garden City: Doubleday, 1972), 671- 765.

[28] A recent example is Jeffrey Lewis, *What if Space Were Weaponized?: Possible Consequences fo Crisis Scenarios* (Washington, DC, Center for Defense Information, 2004), 12.

[29] See Loren B. Thompson's description of "the military's declining space program" as "a seriously dysfunctional part of the space program," in "Policymakers Struggle to Fix Military Space Problems," *Space and Missile Defense* 6, no. 47 (21 November 2005): 3; Frank Morring, Jr., and Michael Mecham, "'One JAXA,': Restructured Japanese Space Agency has Big Plans, but Uncertain Funds," *Aviation Week and Space Technology* 163, no. 21 (28 November 2005): 64-65; and Michael A. Taverna, "Charting a Course: Exploration, Competitiveness Highlight Europe's $10-billion Space Road Map," *Aviation Week and Space Technology* 163, no. 22 (5 December 2005): 24-26, and related articles in that AWST issue.

[30] E.g., Tom Wolfe's *The Right Stuff*, which dissected the "subculture" of NASA, and James Oberg's recent description of its "culture" of "self-confidence bordering on arrogance" and "hostility to outside advice" and learning "from the past," James Oberg, "Sharpening the Focus on the Space Vision," *Adastra*, Spring 2005, 19.

[31] For a somewhat dated but nonetheless pertinent analysis, see Dennis M. Drew, *Military Art and the American Tradition: The Vietnam Paradox Revisited* (Maxwell AFB, AL: Air University Press, 1985), Report No. AU-ARI-CP-85-3, 7-8.

[32] See Hampton Stephens, "Near-Space," *Air Force* 88, no. 7 (July 2005): 36 ff.

[33] For a glimpse of that lexicon, see Stanley B. Alterman, "Complexity of Network Centric Warfare," in Jacques S. Gansler and Hans Binnendijk, eds., *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies* (Washington, DC: National Defense University, 2004), 125-138.

[34] John Diedrich, "Senator Argues for Separate U.S. Space Force: Congress, Air Force Oppose Fifth Branch," *Houston Chronicle*, 26 March 1999. Scanning science fiction models might be interesting, if not wholly useful. Naval forms and terminology have tended to dominate.

[35] E.g., n.a., "The Battle for Outer Space," *Business Week*, 9 November 1957; and James Oberg, "Facts and Fallacies of Space Warfare," *L-5 News*, October 1978, 9-11; Caspar Weinberger, "Space: Vital to U.S. National Security," *Arms Control Update: U.S. Arms Control and Disarmament Agency,* no. 2 (November 1987): 1; William B. Scott, "USSC Prepares for Future Combat Missions in Space," *Aviation Week and Space Technology*, 5 August 1996.

[36] ". . . perhaps the greatest danger posed by the militarization of space is that of war by accident," David Ritchie, *Space War* (New York: Atheneum, 1982), 190-191

[37] Keith Stern, "White House Drafts New Space Policy for Space Threat," *Space and Missile Defense Report* 6, no. 21 (23 May 2005): 1; for a balanced weighing of factors, see Jonathan Coopersmith, "Can We Boldly Go There Any More?" *History News Service*, 7 February 2003, http://www.h-net.org/~hns/articles/2003/020703a.html (accessed 23 February 2006).

[38] E.g., "The continued improvement of space reconnaissance system by the US and Soviet Union and the development of new systems by other nations will have a significant impact on international affairs . . . history seems to testify that satellite reconnaissance has helped moderate the arms race and keep the peace between the US and Soviet Union for 30 years. Perhaps space reconnaissance will limit hostilities between other nations as well." Jeffrey T. Richelson, "The Future of Space Reconnaissance," *Scientific American* 264, no. 1 (January 1991): 44.

Dr. Roger A. Beaumont (BS and MS, UW Madison; PhD, Kansas State) is a Texas A&M emeritus professor (retired). After several years at the University of Wisconsin-Milwaukee as a history instructor and Associate Professor of Organization Science, he taught history at Texas A&M University from 1974 to 2003. Co-founder of the journal *Defense Analysis*, he has authored and edited a dozen books and monographs, most recently, *Right Backed by Might: A History of The International Air Force Concept* [2001], as well as eighty book chapters and articles. After three years in Army Reserve units, Doctor Beaumont served two tours as an Active Army military police officer. He has lectured at higher military schools in Europe and the United States, and consulted to various agencies on defense-related matters. A Secretary of the Navy Fellow at the US Naval Academy (1989-90), he has been an Active Member of the Science Fiction and Fantasy Writers of America since 1974.

The C2 Puzzle: Space Authority and the Operational Level of War

Maj Robert J. Reiss Jr., USAF
Chief, Opposing Forces Division
505th Exercising Control Squadron

Who commands space? Who controls space? Who does space support? Who is the lucky warfighter that gains so much support from space? These pointed questions lie at the heart of space power advocates and operational commanders, as they try to decipher the conundrum known as "space." Commanders will ask, "What can space do for me?" and ideally the advocates can answer, "Space can do this for you, and this and this…"

However, as with most heavily debated topics, the answers clearly depend upon whom you ask. The national agency advocate, that is, National Reconnaissance Office (NRO) or National Security Agency (NSA) might say, "I can provide you this, but only at certain times and under certain conditions." The joint force advocate might say, "I can provide you anything, unless they were previously requested by someone else." The military service advocate might say, "I can give you anything my satellites provide, but I need the request to come from my boss, not directly from you."

In-place command and control (C2) constructs and force development clearly show United States space control and capabilities were originally intended and operated for strategic purposes. Space-supported strategic nuclear forces, reconnaissance, National Command Authority (Presidential/Secretary of Defense) communications, and other high-level national needs.

Satellites were not anticipated for operational/tactical applications, hence the creation of the programs such as Tactical Exploitation of National Capabilities (TENCAP). Although TENCAP was highly successful in accomplishing the spreading of space power benefits to all military forces, it has also diluted the knowledge base of space power and appreciation of how these capabilities came to be. The blowback from this has inadvertently caused arrogance among all non-space recipients of TENCAP and similar programs since end-users, 'the warfighters,' remain unaware of the true origin of the provided support (information/intelligence, communication, location, etc.). Uninformed users therefore hold firm beliefs that a few select United States Air Force (USAF) space units regulate space hardware in orbit and they can also otherwise perform their mission unimpeded without 'space.'

In a brief moment of clarity, this Nation's space leader's task organized its space assets with a combatant command, US Strategic Command (USSTRATCOM), after dismantling US Space Command (USSPACECOM) in 2002. However, with just as much rapidity, the vision lost focus with the creation and dubious implementation of the Joint Space Operations Center (JSpOC) and the Director of Space Forces (DIRSPACEFOR or DS4) in 2005. With this major action, terms such as space coordinating authority (SCA) and C2 became muddled, and the clear and concise flow of information and control from the combatant commander to the warfighter changed from a straight, clear road to a curvy path with roadblocks.

To maintain, or even increase, the force-multiplying effect space has on the battlefield, ideas such as JSpOC need correct implementation. By correctly using these constructs, ideas on how space can, should, and will be used to maximum effect will affect institutionalized space thought in the form of improved doctrine. At minimum, corresponding joint and service space doctrine should reflect changes in technology and capabilities for space assets, not just merely mirror another medium's doctrine (i.e., air, naval, or marine). When this mirror imaging occurs, ideas such as DIRSPACEFOR are confused in scope and responsibility with their better-defined counterparts such as JFACC/COMAFFOR.

Space C2: a Historical Quandary

"American leadership will make no mistakes, the enemy offer no surprises and the situation proffer no unexpected opportunities"[1] - Frederick Kagan

The US current C2 structure for space systems can be traced back to the budget and planning decisions made in the early 1980s.[2] Decisions originating in the Carter Administration were later sustained and expanded during the Reagan Administration. These systems were designed and purchased to render a sufficient network for nuclear warfare C2 at the strategic/presidential level. Some of the systems for this complex nuclear C2 network include the Defense Support Program missile warning satellites, the Nuclear Detection System aboard Global Positioning System (GPS) satellites, the Defense Satellite Communication System, the Military Strategic Tactical and Relay Satellite Communications System and Fleet Satellite Communication System communication satellites. These programs and many others were central to the global C2 structure that was required by the National Command Authority during nuclear conflict.[3] During the later 1980s and throughout the 1990s, military planners believed the influence of C2 dominance on the planned nuclear and conventional battlefields spilled over to shape space forces at the operational level; the reality today is C2 dominance is integral upon being dominant in space first. This view was not always the case.

During the dawn of the Space Age, inherent divisions were created, separating and duplicating efforts without a common goal in mind. From the outset, there were multiple duplicative efforts by the Navy, Army, and Army Air Corps involving captured German V-2 rockets. To a lesser extent, the civilian National Advisory Committee for Aeronautics (NACA) and its successor, the National Aeronautics and Space Administration (NASA) performed additional efforts in research.[4] The rivalry and splitting of focus within the US government is evident in many early space projects:

- RAND Corporation's 1946 study on a "world circling spaceship"
- US Army's Redstone medium-lift boosters
- US Navy's Aerobee and Viking research rockets
- USAF Intercontinental Ballistic Missile (ICBM) research

Even America's first foray into space showed signs of rivalry, pitting the US Navy's Project Vanguard against a more experienced US Army rocket team. Project Vanguard was chosen for its use of 'civilian' research rockets (Aerobee and Viking), instead of modified military missiles, as the booster. The failure of Project Vanguard's first two attempts pushed the Army's plan into action, successfully orbiting the Explorer I satellite in 1958. Until the late 1950s, no service had taken great interest in space: the Army viewed missiles as an extension of artillery, the Air Force focused its attention on its manned bomber fleet, and the Navy supported freedom of all services to develop missiles in response to its own internal needs.[5]

Everything changed on 4 October 1957 with the launch of the Soviet's *Sputnik*; with underlying tones of worldwide reach by Communism, space became a US national priority. Creation of coordinating agencies for space programs came fast and furious. The Department of Defense (DoD) created the Advanced Research Projects Agency, controlling both military and civilian programs until NASA took the civilian portion in 1958. The creation of NASA took resources from the now-defunct NACA and also raided the Navy and Army programs nearly completely. This left the Air Force as the dominant military player in space. However, even operations with *Discoverer*/*CORONA* left the lines of command and control blurred during the joint Central Intelligence Agency/USAF effort.

More fragmentation occurred in 1961, with the creation of NRO, causing the opposite effect from an agency's creation that was to control all overhead intelligence gathering. The NRO took control of all reconnaissance satellites as directed by Under Secretary of USAF (a.k.a. the NRO Director), but excluded any control or participation directed from Headquarters (HQ) USAF. From these brief examples, it is evident that this multi-polar slicing of national space power early in the Space Race and the vacuum of joint cooperation has brought United States' space forces to the point where we are today. This jumble might have been bearable for US forces to operate this way in conflict and peacetime, if not for one missing component: doctrine.

Doctrine: the Glue that Holds it Together or the Ties that Bind?

Fifty years and many agencies later, space doctrine has not kept pace with technological developments or political constraints pertaining to space and the battlefield. New developments are taking place faster than the traditional 5-year doctrinal writing cycle structure (submissions, write/re-write, approval, publish/distribute, submissions). Doctrinal terms that were relevant in the past (operational vs. support) have now become blurred or outright obsolete depending on the situation and platform used. What term adequately describes a situation where one unit's 'support' came from someone else's 'operation?' For the vast majority of space assets, and for the sake of simplicity, their assistance is rendered in the form of 'support' to 'operational' warfighters.

If the concept of support is to remain a common thread throughout the space forces, another underlying concern is "who's in charge?" or "who's in control?" A clear example of the muddled chain-of-command intertwining multiple agencies and missions can be found in the Defense Meteorological Support Program (DMSP), the DoD's primary weather satellite:

> "DMSP weather satellites, provided specifically by and for DoD and limited national-level operations, (currently fall under the combatant command of USSTRATCOM), but are controlled on a daily basis by the National Oceanographic and Atmospheric Administration (NOAA) under the Department of Commerce (DOC). Yet, requirements for on-board sensor tasking are provided by the Air Force Weather Agency, a direct reporting unit to the Chief of Staff, United States Air Force (CSAF)."[6]

Air Force Doctrine Document (AFDD) 2-2 uses DMSP as a positive example as how multiple agencies, missions, and functions can be rolled up into one satellite program while still performing its duties at a high level of confidence. While great for a textbook level analysis, this example is not a true representation of the space arena and all of its 'power' players and their competing interests. Table 1 shows just a small number of the US government agencies that have a vested interest in space.

US Air Force	National Security Agency	Department of State
US Navy	National Reconnaissance Office	Department of Commerce
US Army	Central Intelligence Agency	National Aeronautics and Space Administration
National Geo-spatial Intelligence Agency	Defense Information Systems Agency	National Oceanographic and Atmospheric Administration

Table 1. Selected US agencies.

While space provides a significant percentage of the global C2 infrastructure, Table 1 shows the USAF is not the sole provider in this domain. Can existing military doctrine bridge gaps between military and civil systems (i.e., DMSP and GPS) or military and 'national' systems (i.e., NRO and NSA) when each agency has its own way of doing things? The answer is no. Governmental space doctrine (joint, service, and multi-service) must catch up to the near term, encompassing civil, military, commercial, and national systems and its C2 aspects before a 'stressed' environment (war, conflict, crisis, natural disaster, etc.) exposes its flaws at the cost of human lives. Fixing the doctrine problem is a step in the right direction, however, without wholehearted agency support from all involved players, fragmentation of space asset control will continue to exist.[7]

The Conundrum: USSTRATCOM, JSpOC, and DIRSPACEFOR

With the demise of USSPACECOM in 2002, it seemed the hand-off of space responsibilities to USSTRATCOM would be seamless and a huge force-multiplier for combat forces. In the years immediately following the transition, no major changes to space force C2 were announced, until Air Force-wide changes forced units to 'operationalize' space. In mid-2005, military leaders unveiled a new plan to unify space as a weapon system with 'centralized' C2 in order to increase (presumably deployed) joint force operational effectiveness and efficiency. This space C2 structure plan draws from the agency currently responsible for space (USSTRATCOM), a proposed 'focal point' of space activity (JSpOC), and administratively controlling entities (USAF's 8th and 14th Air Force [AF]), and introduces a new construct, the DIRSPACEFOR or DS4. This plan seems simple when summarized as above, but becomes a bit murky when laid out graphically and with some narrative dialog.

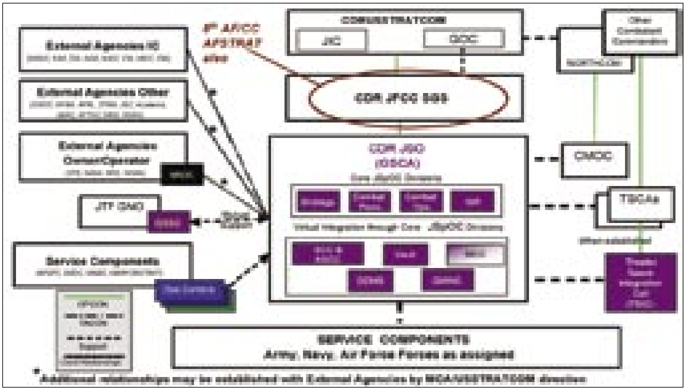

8th AF/CC
AFSTRAT
also
CDRUSSTRATCOM
JIC
GOC
Other Combatant Commanders
NORTHCOM
External Agencies IC
External Agencies Other
External Agencies Owner/Operator
CDR JFCC SGS
CDR JSO
(DSCA)
CMOC
JTF GNO
TSCAs
Service Components
SERVICE COMPONENTS
Army, Navy, Air Force Forces as assigned
*Additional relationships may be established with External Agencies by MOA/USSTRATCOM direction

Figure 1. JSpOC Organizational Structure (FOC).

JSpOC briefing, 8 Jun 2005

Joint Confusion Center?

Part of this new space C2 plan, outlined in a memorandum from Commander, Space and Global Strike (JFCC SGS), to Commander, Joint Space Operations (CDRJSO), established JSpOC. Its official purpose is to "ensure unity of command and unity of effort" for space forces. It should be noted, the CDRJSO is also the 14 AF Commander, under Air Force Space Command (AFSPC). While the JFCC SGS is the 8 AF Commander under Air Combat Command and Barksdale AFB, Louisiana—neither location directly controls space assets, aside from occasional launch vehicles at Vandenberg AFB, California. Figures 2, 3, 4, and 5 graphically display some of the disparity and confusion this has wrought.

The JSpOC is between the service components and USSTRATCOM but has two layers of leadership (8 and 14 AF) before it gets to the Commander, United States Strategic Command (CDRUSSTRATCOM). Its divisions are similar to an Air Operations Center (AOC) layout, with Plans, Operations, and Strategy divisions. One main difference with JSpOC, it is part of a 'virtual AOC' planned to be one of many distributed facilities (Barksdale's AF Global Strike, and 'other' AF AOCs to be determined) as seen in figure 4. A huge failing in the 'mirroring' of its air counterpart is the reality that the JSpOC cannot directly control any space assets (i.e., sensor tasking and orbital maneuvers). Space forces are not the same as terrestrial (air/surface) assets and should not be treated as such. They were never intended for use at the tactical level. They cannot 'surge' or be 'packaged' and tailor made for short-term operations as aircraft, tanks, and ships.

With the inclusion of JSpOC, the command (Aerospace Defense Command, combatant command (COCOM), Tactical Army Command) chain gets very complex. This new space C2 design, seen through the JSpOC organizational chart in figure 1, involves two USAF major commands (MAJCOMs), and two USAF numbered air forces, all under the mantle of USSTRATCOM, a unified combatant command. At first glance, it seems there are new positions to clarify the chain-of-command from the 'satellite driver' to the combatant commander; however, when delving a little deeper, it is evident that the positions listed just become additional job titles for existing commanders.[8]

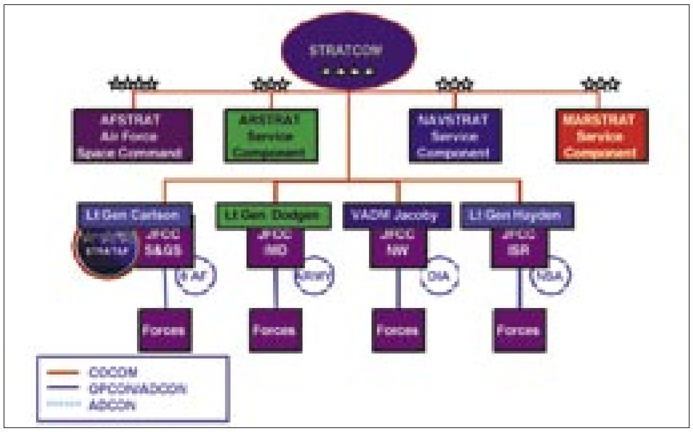
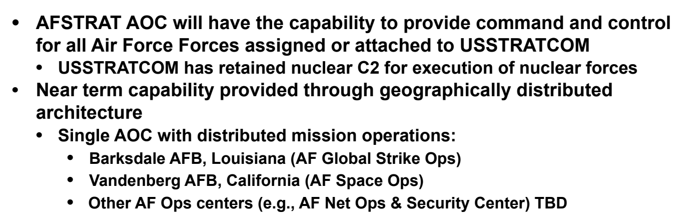


Figure 2. Who I Am: Component Relationships to USSTRATCOM.[9]

JFCC SGS Commander's Call, 22 Apr 05



- AFSTRAT AOC will have the capability to provide command and control for all Air Force Forces assigned or attached to USSTRATCOM
  - USSTRATCOM has retained nuclear C2 for execution of nuclear forces
- Near term capability provided through geographically distributed architecture
  - Single AOC with distributed mission operations:
    - Barksdale AFB, Louisiana (AF Global Strike Ops)
    - Vandenberg AFB, California (AF Space Ops)
    - Other AF Ops centers (e.g., AF Net Ops & Security Center) TBD

Figure 3. AFSTRAT Air and Space Operations Center.

AF to USSTRATCOM, 8 Jun 05

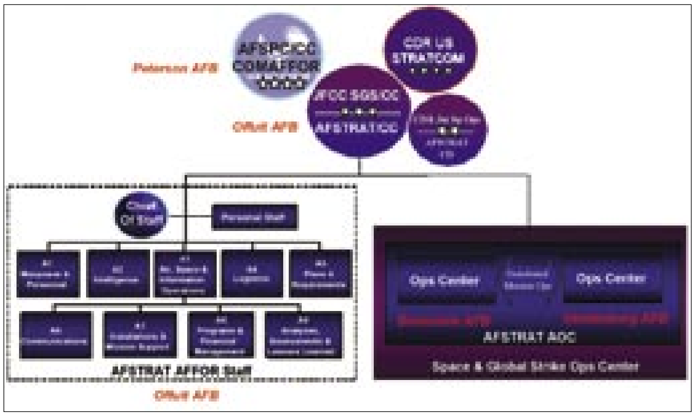
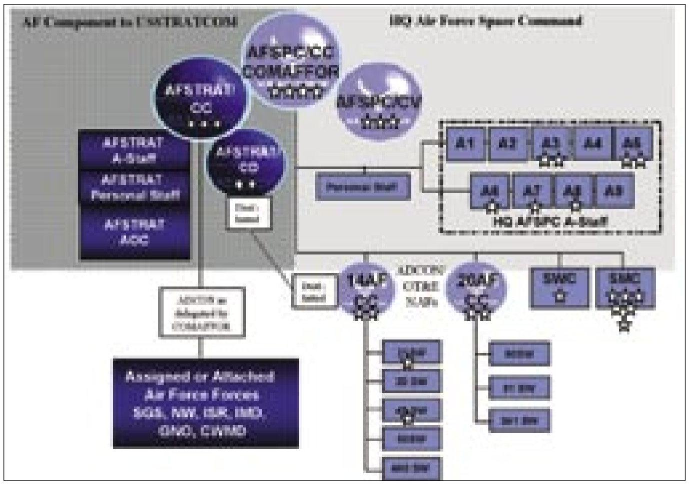


Figure 4. AF Component to USSTRATCOM (Joint Integration).

AF to USSTRATCOM, 8 Jun 05

Who Am I Today? Command Responsibility in Space Command and Control

In adding to the pre-existing C2 structure, the powers-that-be compounded the responsibility hierarchy. Here is a summary of the people and titles involved in these new changes: the Air Force Space Command Commander (AFSPC/CC) (MAJCOM AFSPC) is the Air Force liaison to Strategic Command (AFSTRAT) and the commander, Air Force Forces (COMAFFOR) for USSTRATCOM unless AFSPC/CC delegates AFSTRAT as



AF to USSTRATCOM, 8 Jun 05

Figure 5. AF Component to USSTRATCOM.

COMMAND RELATIONSHIPS

Combatant Command (command authority) (COCOM)
(Unique to Combatant Commander)

- **Budget and Planning, Programming, and Budgeting System Input**
- **Assignment for subordinate commanders**
- **Relations with Department of Defense Agencies**
- **Convene courts-martial**
- **Directive authority for logistics**

When OPERATIONAL CONTROL is delegated

- **Authoritative direction for all military operations and joint training**
- **Organize and employ commands and forces**
- **Assign command functions to subordinates**
- **Establish plans and requirements for intelligence, surveillance, and reconnaissance activities**
- **Suspend from duty subordinate commanders**

When TACTICAL CONTROL is delegated	**Local direction and control of movements or maneuvers to accomplish mission**	When SUPPORT relationship is delegated	**Aid, assist, protect, or sustain another organization**

Joint Publication 3-0, Doctrine for Joint Operations

Figure 6. Command Authorities.[14]

the AF War Fighting HQ; in which case responsibility would fall to 8 AF/CC (under MAJCOM Air Combat Command). In addition to the above relationships, 14 AF/CC (belonging to AFSPC) also holds the position of Deputy Commander for AFSTRAT (AFSTRAT/CD).

This position-shifting and wearing multiple 'hats' is quite surprising, especially within AFSPC, since one recommendation of the Space Commission of 2000 was separating very large job responsibilities to individual positions.[10] Taking the multiple positions of supreme importance (i.e., JSpOC commander) and stacking them with one person (i.e., 14 AF/CC) seems to be going against the Space Commission recommendations and against common sense.[11] Even outside of the space arena, multiple job titles for commanders seem to be the norm. For example, the CDR JFCC SGS is quadruple-hatted: CDR JFCC SGS is also the 8 AF/CC, AFSTRAT, and Air Force Network Operations Commander (AFNETOPS/CC).

With the multiple job titles, the flow of command authority is just as unclear. In figures 4 and 5, AFSTRAT/STRATAF/8 AF/CC reports to AFSPC/CC (as COMAFFOR) for USSTRATCOM. The operational chain (COCOM, OPCON, TACON, Support) runs from the CDRUSSTRATCOM (Offutt AFB, Nebraska), to AFSTRAT/CDR JFCC SGS (Barksdale) then CDR JSO (Vandenberg), to the warfighter.[12] Even the proposed center of operations, the AFSTRAT Air and Space Operations Center (AFSTRAT AOC) is the 'virtual' AOC broken into three pieces at distanced locations: Barksdale AFB for AF Global Strike, Vandenberg AFB for AF Space Ops (i.e., JSpOC) and 'other' AF AOCs yet to be determined (TBD) shown in figure 4.

Somehow, AFSTRAT AOC will have the capability to provide C2 for USAF forces assigned or attached to USSTRATCOM and be able to serve as the "one stop shop" for all military space power, provided 'virtual link' communications do not break down between these distanced facilities. If this does not sound dubious enough, imagine the hands-on C2 required for the number of military and national satellites on orbit. The Air Force Association's *Space Almanac* states as of 31 May 2004 there were 2,884 satellites in orbit, in varying states of operation (fully and partially operational, dead, and in check-out).[13] In the 7 December 2005 issue of the *Washington Post*:

> "Currently, 43 countries own satellites and there are 413 United States and 382 other operational satellites in orbit."
>
> - Katherine Shrader, Journalist

Discounting the civil and commercial satellites, even the sanest individual could not convincingly believe that the JSpOC could command, control and disseminate the products from most, if not all, military and national space systems.

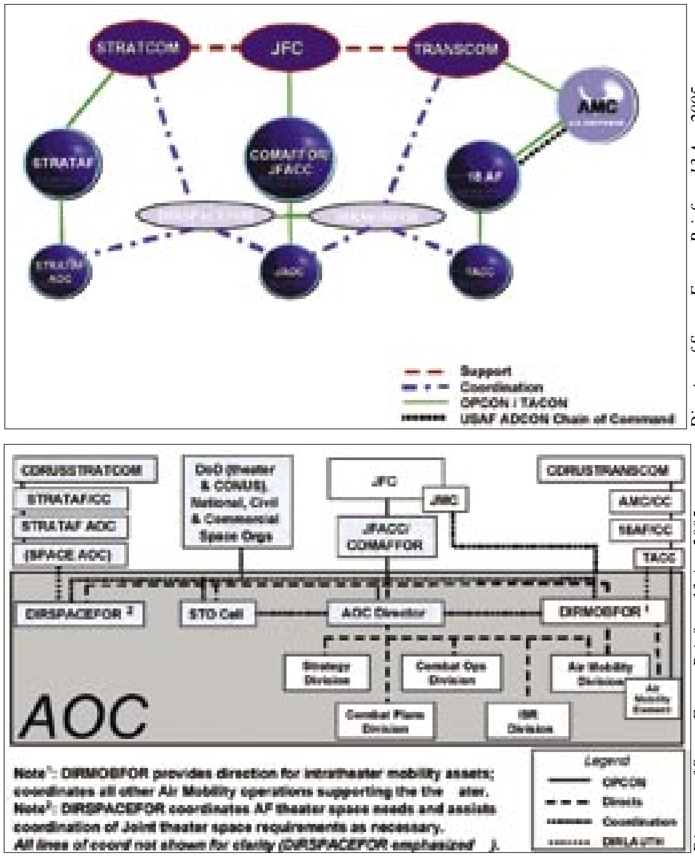
Blast from the Past? Strategic Air Command Lives!

"Senior commanders making decisions about operations, combined with subordinates free to exercise initiative in executing those decisions, make up the heart of C2—centralized control and decentralized execution." - AFDD 2-8, C2

These C2 changes are a bit different than another plan described in a memo by General John P. Jumper as Chief of Staff, USAF to Admiral James O. Ellis Jr., then USSTRATCOM/CC dated 23 February 2004. That memorandum stated that three separate numbered air force headquarters, 8 AF (Bombers), 14 AF (Space), and 20 AF (ICBMs) would combine to form AFSTRAT. The combination of these three NAFs into AFSTRAT, on the surface, appears to reconstitute a large portion of Strategic Air Command (SAC) from the days of the Cold War. Under SAC, the headquarters at Offutt AFB controlled these NAFs, just as USSTRATCOM does today. While SAC did a wonderful job against its programmed threat, resurrecting it in similar forms may not constitute the best C2 example for space assets in the 21st century.

A Conductor with No Orchestra: DIRSPACEFOR

Another area of focus has been in the designation of SCA and creation of a position on the Combined/Joint Forces Air Component Commander (C/JFACC) staff called the DIRSPACEFOR or DS4. As shown in figures 7 and 8, the name and position is similar to the Director of Mobility Forces (DIRMOBFOR), another function within the AOC, with a key difference. This staff position is supposed to bridge the gap between strategic, operational, and tactical application of space power.[16] The DS4 role seems to exist at the operational level, but reality shows that misconception is due to their position's location at the Combined AOC (CAOC). All support provided is actually tactical. In a similar vein, the JSpOC is also tactically orientated because it



Note1: DIRMOBFOR provides direction for intratheater mobility assets; coordinates all other Air Mobility operations supporting the the ater.
Note2: DIRSPACEFOR coordinates AF theater space needs and assists coordination of Joint theater space requirements as necessary.
All lines of coord not shown for clarity (DIRSPACEFOR emphasized).

Director of Space Forces Briefing, 13 Apr 2005

Director of Space Forces Briefing, 13 Apr 2005

Figures 7 and 8. DIRSPACEFOR Mirroring DIRMOBFOR.

cannot actually 'control' the strategic assets it monitors on ownership rights alone.

DIRSPACEFOR is a relatively new concept, assigned to support the combined force air component commander (CFACC) at the operational level of war. The DS4's central role is the senior space expert on the CFACC staff, and accordingly has a complement of 8–12 personnel including space weapons officers (W13S or 'whiskeys'). DS4's job description requires delegated space coordinating authority obtained by the CFACC, who in turn received it from the Combined Forces Commander (CFC). Before the creation of DS4, a space support team performed advisory and support functions; there was no existing concept of SCA. One important fact to note is DS4 offers only coordination, via SCA, not C2 of any forces. This is the key difference between DIRMOBFOR and DS4 - DIRMOBFOR can actually control taskings for inter- and intra-theater assets (in this case, mobility assets like cargo, tanker, and personnel transport aircraft)

Adherence to joint military doctrine gives clear messages about the transferability of command authority. Joint Pub 3-14, Joint Doctrine for Space Operations, dated 9 August 2002, does discuss "space authority" to the joint force commander for coordinating space operations, integrating space capabilities, and responsibility for in-theater joint space operations planning. What does joint doctrine discuss about coordinating authority? Nothing. However, found in Air Force doctrine as stated by AFDD 1-1, coordinating authority is:

Agency	Level of War	Level of Command	Space Forces
USSTRATCOM	Strategic/ Operational	COCOM	All Military
AFSPC	N/A	OPCON/ADCON	Air Force
JFCC SGS	Operational	TACON (?)	Air Force
JSPOC	Operational (?)	*	Air Force (Navy?)
DIRSPACEFOR/ DS4	Operational/ Tactical	*	(?)

** Space Coordinating Authority, not direct command*

Table 2. Positions and their Level of War.

1. The authority delegated to a commander or individual for coordinating specific functions and activities involving forces of two or more military departments or two or more forces of the same Service.
2. The commander can require consultation between the agencies involved but **does not** have the authority to compel agreement.
3. More applicable to **planning** and similar activities than to operations.
4. May be exercised by commanders or individuals at any echelon **at or below** the level of combatant command.
5. A **consultation relationship** between commanders, not an authority by which command may be exercised.
6. **Not** a command authority.

On the surface, DS4 appears to be a good centralizing solution on bringing space power and capabilities to the warfighter. However, with the DS4 being located in the AOC as part of the C/JFACC's staff, his or her view of space is limited to the tactical level as part of air operations. What about support for the combined forces land and maritime component commanders (joint force land component commander and joint force maritime component commander respectively) of the joint fight? Where is the coordination and C2 for them in the space picture? DS4 does not have much visibility outside the theater (except through reach-back to JSpOC), and has very little visibility within theater outside the AOC.

Providing the DS4 with information flow, the JSPOC offers the same problem but on a larger scale: it is supposed to operate at all levels of war (strategic, operational, and tactical). But in its current form as a non-joint entity, JSpOC does not carry enough weight to authoritatively deal with all agencies required. The head of the JSPOC has Global Space Coordinating Authority (GSCA), which amounts to little for the joint fighting force and has no influence beyond AF space assets, equaling the uselessness provided by DS4 but on a global scale. Coordination authority has no teeth; it is only a short-term solution.

Concerning AF space forces, SCA is the wrong focus. Coordination and cooperation between varying entities is not leadership. The DS4 position provides neither command nor control; during a fast-paced campaign, the coordinating process could waste valuable time and effort. Seen from an operational sense, SCA and GSCA provide unnecessary bureaucratic layers. This current setup fits outdated and outmoded doctrine, which is outpaced by new events constantly. The DS4 responsibility does not solve any fundamental issues (i.e., "Who controls space?") or pave the way for future flexibility. This current structure of SCA may suffice in the short term provided the system is not stressed due to intense adversary action. How long will this situation continue?

Concerns

One mantra is always preached throughout USAF doctrine and PowerPoint briefings: *centralized decision-making, decentralized execution*. Yet, the current structure of space is a thinly spread polyglot of space power whose products and services are in high demand by everyone (military and civilian). At best, what we currently have is fragmented, compartmentalized decision-making and very little decentralized execution, if any. That only covers the US military. The situation becomes much worse when we introduce the headaches involving information sharing with other US government agencies.

Upping the complexity of the problem is sharing information with coalition partners. In a combined operations center (i.e., CAOC), the information dissemination problem poses many questions: Who decides what information needs to be shared and how much? Who else has indigenous space capabilities? What do primary allies and/or host nations need to know and what is their usage or level of understanding? Do we include end user *products* like GPS, weather data, and imagery?

Regardless of the answers, history has shown that allies usually equate to short-term fair weather friends, in most cases. Usually, their strategic concerns are usually not on par with the United States. Even in rare cases when they are, sometimes governments are one election or revolution away from change. Historical evidence such as the 1979 overthrow of the Shah in Iran or recent events in Spain, Pakistan, and Venezuela show the likelihood of this. What happens when the US embraces those countries, sharing knowledge of our full capabilities in space, and then they go bad?

Historical Case Study: the RAF and the Battle of Britain

In 1940, Great Britain's Royal Air Force (RAF) had the most modern air defense system, while the Germans had the most modern air force. The RAF had a C2 system with outstanding fighters, ground controllers, and a new overlapping radar system with centralized control. In comparison, the Luftwaffe was the only air force in world technologically and operationally prepared for a strategic bombing campaign. It possessed capable bombers, excellent fighters and had "blind" bombing and navigation system for guiding planes to targets. Intelligence, however, was not its forte. Estimates issued just prior to the Battle of Britain inflated German superiority and underplayed British strengths, including a lack of attention to the RAF radar system plus a condescending opinion of RAF Fighter Command's C2:

> "inflexible, formations are rigidly attached to their home bases… command at low level is generally energetic but lacks tactical skill."[17] - Williamson Murray

A single German Luftflotte (air fleet) had unity of command and controlled both fighters and bombers in combined operations, contrasting the RAF with separate command chains for the two tasks. In July 1940, the RAF had a total strength of 640 fighters, against more than 2,600 Luftwaffe bombers and fighters. To employ effective economy of force and mass the limited fighter strength, Britain had a simplistic C2 defense system that maximized all the weapons available. Each group was split into sectors with RAF stations in each, one of which was the Sector Control Station, the lowest level of C2 in the system yet it seemed to perform the operational level of war. All the Sector Control Stations reported to the Group HQ, (this HQs acted as a filter and communications center) and they in turn reported to Fighter Command HQ.

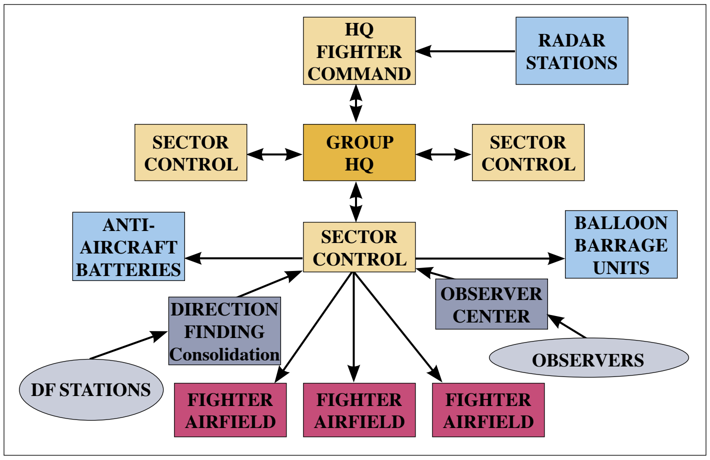


Figure 9. 1940 Royal Air Force C2 System.

Central to situation awareness were coastal radar stations, which had sufficient range to detect formations while still over France. Contacts were reported to Fighter Command HQ (FCHQ) where it was plotted on a large map (the 'big board') while simultaneously passed to the Group HQ, who passed it down to the Sector Control affected by the plot. Observer posts reported the formation once they had crossed the coast and were behind the radar. They reported to Observer Corps Centers, who passed the information on to their Sector Control, then to Group HQ, who in turn sent it to FCHQ and the plot of the raid was kept up to date.

All information was passed up or down to the Sector Control Centers, giving them accurate situation awareness and they directly controlled the defenses: balloons, anti-aircraft guns, and fighters. Without this vital system, resources (time and fuel) would have been wasted in constant airborne patrolling of the coast; the full effect of limited resources would not have been brought to bear and air raids could have made it to their targets with little to no warning at all. All information was transmitted to every sector to keep situation awareness spread throughout the command system. By doing this, the loss of a single Sector Control Room did not limit the elastic, effective defense.

How many United States intelligence estimates reflect the exact same words and attitude toward our potential opponents? Cumbersome and technologically superiority-based C2 does not necessarily equate to victory over a simplistic, streamlined C2 organization fighting for survival.[18]

An In-Place Solution: USSTRATCOM

What is the best solution? One need not look further than the foundation USSTRATCOM provides, and then expand on the basics: firm C2 by USSTRATCOM of all military space and direct linkage to other government agencies with space assets with tasking authority and setting priorities, with appropriate levels of assumable authority in time of war for other assets. The in-place structure of USSTRATCOM offers an excellent framework in which to build. Since USSTRATCOM already has COCOM for strategic forces and should not have anything below it concerning space forces,[19] any lesser level of command (OPCON or TACON) hampers their ability to provide true unity of joint space power. Only USSTRATCOM has, with COCOM, the authority for relations with DoD agencies and weight to deal with other agencies.[20]

In addition, JSpOC should exist as an organic unit to USSTRATCOM, not a 'for-hire' unit ran by a service-specific level of command (i.e., USAF numbered air force). Since the Air Force firmly believes in the centralization of air power, allowing it to dominate the entire theater operating area (in the form of the CFACC), the JSpOC concept goes against that belief on the joint force level. When the Air Force deploys forces, they become part of a geographic combatant command. Joint space power should evolve through USSTRATCOM.

A model similar to the RAF Fighter Command in 1940 would have a central C2 node physically located at Offutt or Cheyenne Mountain (or one back up another). The primary location is not important as long as the chain of command is directly from CDRUSSTRATCOM to the C2 node (figure 10). The space C2 system can be further streamlined from the RAF model, eliminating "multiple sector control centers" and "Group HQ," which only served to centralize and consolidate sector controls. Unless JSPOC takes the place of "Group HQ" and the sector control centers are the actual units that deal directly with space assets, the JSPOC should have actual control of all military space assets (Army, Navy, USAF) with assigned liaisons from all agencies/departments of the government with space assets. An incredibly critical component to maximizing space power, those liaisons also must have a *level of authority* to enact C2 decision-making and implementation. This is the key component to solidifying truly unified space power: rapid situation assessment and execution by all those in the space 'field' at the same time with the same information. To do otherwise, leaves the system with an ineffective, inelastic "message taking board" and not a dynamic, flexible, responsive C2 to fight our future wars.[21]

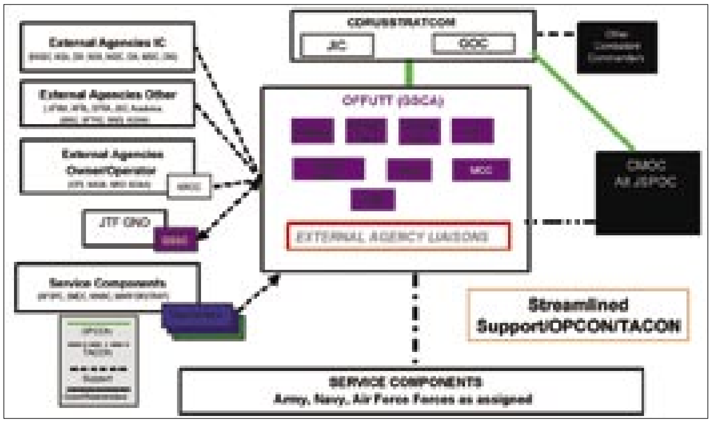


Figure 10. Better JSpOC Organizational Structure.

What is Best for the Future?

Distributed warfare equals coordination nightmare and that's at the *tactical* level. Until we develop uninterruptible instantaneous communications, the system currently in place will not be sufficiently responsive to rapidly changing battlefields. Self-imposed vulnerabilities in the form of critical communication nodes (i.e., DIRSPACEFOR reach-back to JSpOC, distributed 'virtual' AOCs) hamper our ability to utilize our technologically superior assets to either mass or perform economy of force. Modern successful joint maneuver warfare depends upon speed of command. C2 of joint military space power is entirely too vital to leave anywhere below the combatant command level. Without precision guidance, there can be no precision weapons. Without robust, reliable communication, there can be no reach-back. Without a clear, dominant C2 of forces, there can be no assurance of victory.

Once the military space side of the house is brought into order with this clear C2 system, the other US government agencies with space assets will naturally follow suit. US space assets began and continue to be national-level treasures. Evolution of US space assets into a solid, unified space power is a natural progression. Looking from the adversary's point of view, we are already unified: they do not care if they send the 14 AF JSPOC into crisis mode or if their attack is directed towards a 2 SOPS satellite or 1st Space Battalion crew. A US satellite or space capability is seen as just that: a US asset to be attacked. The more we complicate the C2 process, the slower our response becomes and greater the effect against our warfighters.

Notes:

[1] R. Mullen, "Dearth of Reserves Threatens US, Expert Says," *Defense Today,* 19 August 2005, 1.

[2] Joint Publication (JP) 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, Command and Control (C2), 101. "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission."

[3] Thomas P. Coakley, *Command and Control for War and Peace* (Washington DC: National Defense University, 1992), 60-63

[4] David N. Spires, *Beyond Horizons: A Half Century of Air Force Space Leadership* (Air University Press, 1998), (3rd printing, 2002), chapter 1.

[5] Ibid.

[6] Air Force Doctrine Document (AFDD) 2-2, *Space Operations,* 27 November 2001, 23.

[7] John M. Collins, *Military Space Forces: The Next 50 Years* (Brassey's Inc, November 1989), 74. "Military activities in space . . . strongly influence all armed forces on Earth. Military space policymaking, planning and programming at the apex (of command) should transcend partisan interests. Sound organizational decisions based on objective reviews of realistic options . . . because far-reaching decisions made in the near future will have long-term ramifications."

[8] 'Satellite driver' is a generic term for the person or unit who operates a space system.

[9] Lt Gen Bruce Carlson, "Space and Global Strike" (commander's call, JFCC, 22 April 2005).

[10] AFSPC Public Affairs, "Key Events in AFSPC History," http://www.peterson.af.mil/hqafspc/history/chronology.htm (accessed 19 January 2006).

[11] Space Commission, *Report of the Commission to Assess United States National Security Space Management and Organization*, Executive Summary, 11 January 2001, http://space.au.af.mil/space_commission/ (accessed 24 February 2006).

[12] Captain Ray Fernandez, HQ AFDC/DR, USAF Doctrine Center, Maxwell, AFB, e-mail to author, 15-16 November 2005.

[13] Air Force Association, Space Almanac 2004, *Air Force Magazine* 87, no. 5 (31 May 2004): 28.

[14] JP 3-0, II-7, *Doctrine for Joint Operations*, 10 September 2001.

[15] Director of Space Forces (briefing, 13 Apr 2005).

[16] JP 1-02, *DOD Dictionary of Military and Associated Terms*, Operational Level of War, GL-15. "the level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives."

[17] Williamson Murray, "How Did 'The Few' Win," *Great Battles* special issue 2003, 36-46 and 92.

[18] History is replete with examples of how simple yet effective C2 can overcome mass, superior technology, arrogance, etc. The RAF example, while affecting a relative short-term time frame, one must understand that at that point in time, Germany had every reason to believe that the British would capitulate and make peace which also added to the overconfidence. The Nazi war machine was in for a shock that upset the operational timetable and had lasting effects on grand strategy as well.

[19] JP 3-0, II-6, *Doctrine for Joint Operations,* 10 September 2001, Combatant Command. "COCOM is the command authority over assigned forces vested only in the commanders of combatant commands by title 10, USC, section 164, or as directed by the President in the UCP, and cannot be delegated or transferred."

[20] Selected agencies include: NASIC/AIA, NSA, DIA, DISA, NGA, CIA, AFWA, DTRA, JSC, AFTAC, NOAA, NASA

[21] AFDD 2-8, *Command and Control,* 16 February 2001, 3. "The commander will never have all the information desired. Accepting and taking reasonable risks to achieve mission success is the norm in warfare—efficient and effective C2 minimizes that risk."

Sources:

J.D. Morelock, *Generals of the Ardennes: American Leadership in the Battle of the Bulge* (National Defense University Press, 1994).

Williamson Murray, *Strategy for Defeat: The Luftwaffe 1933-1945* (Air University Press, 1983).

Williamson Murray, "How Did 'The Few' Win," *Great Battles* special issue 2003, 36-46 and 92.

Thomas P. Coakley, *Command and Control for War and Peace* (Washington DC: National Defense University, 1992).

Kenneth Allard, *Command, Control and the Common Defense,* 2d ed. rev. (National Defense University Press, 1999).

AFDD 2, *Organization and Employment of Aerospace Power,* 17 February 2000.

AFDD 2-2, *Space Operations,* 27 November 2001.

AFDD 2-8, *Command and Control,* 16 February 2001.

Joint Publication 3-14, *Joint Doctrine for Space Operations,* 9 August 2002.

Field Manual 100-18, *Space Support to Army Operations,* 20 July 1995.

Kevin C. Holzimmer, "Joint Operations in the Southwest Pacific, 1943-1945," *Joint Forces Quarterly* 38, 3rd quarter (2005), 100-108.

David N. Spires, *Beyond Horizons* (Air University Press, 1998), 3rd printing 2002.

John M. Collins, *Military Space Forces: The Next 50 Years* (Brassey's Inc., November 1989).

T. Harry Williams, *Lincoln and His Generals* (Knopf Inc., 1952).

Army Tactical Exploitation of National Capabilities (TENCAP), Army Space Program Office, 2003.

Briefings:

Lt Gen Daniel P. Leaf, AF Componency to USSTRATCOM, 8 June 2005.

Maj Gen William L. Shelton, Joint Space Operations Center, 8 June 2005.

Maj Gen Douglas M. Fraser, Space C2 Weapon System Information Brief, 8 June 2005

Lt Gen Bruce Carlson, Space and Global Strike JFCC Commander's Call, 22 April 2005.

Maj Robert J. Reiss Jr. (BS, Aviation Management, Wilmington College, Delaware; MBA, Regis University, Colorado) is currently the Chief of Opposing Forces for the 505th Exercise Control Sq, 505th Command and Control Wing, Hurlburt Field, Florida. He has been the Chief of Space and IO and a qualified Air and Space Operations Center (AOC) instructor. Since assigned to the 505th he has directly participated in ULCHI FOCUS LENS 03, TERMINAL FURY 04/05, BLUE FLAG 05, JOINT RED FLAG, PACIFIC WARRIOR 04, JEFX 04 and CJTFEX. He has held command leadership positions as flight commander, an acting intelligence SQ/CC, and as a joint executive officer for a USCENTCOM HQ element. Major Reiss has extensive background in operational war plans, intelligence/counter-intelligence, counter-terrorism, ICBM operations, deception/counter-deception, information operations, force protection and OPSEC through assignments in missile, fighter and intelligence wings, a tour with the National Security Agency and deployment in USCENTCOM AOR. He is a graduate of Squadron Officer's School and Air Command and Staff College. Major Reiss is a lifetime member of the 16th Cavalry (Armored) Regiment.

AFSPC's Pilot Projects – Building Net-Centric Relationships

Capt Neil A. Soliman, USAF
Systems Engineer, Space Division,
Combatant Commanders C2 Systems Group

In civil aviation, the men and women who perform air traffic control (ATC) are responsible for protecting the lives of millions of airline passengers each year, and the controllers do not physically work in aircraft cockpits. The "pilot," addressed in this article, doesn't fly aircraft either; the term pilot used here refers to a "first-of-its-kind" effort …. a pathfinder. Under Air Force Space Command (AFSPC) leadership, a pilot effort is bringing together over 30 interested organizations across Department of Defense's (DoD) space community for the purpose of negotiating and collaborating on how they will exchange very specific Space Situation Awareness (SSA) information crucial to military command and control (C2). It is based on a coalition of the willing, and it's called the C2-SSA Community of Interest (COI). Its outcome will be innovative development of net-centric services.

This article is also founded on what many of us take for granted—the role that C2 plays every single day in protecting lives and coordinating important events. Since space data is often instrumental to the success of military operations at all echelons of conflict, it is a force multiplier that must be continually improved in terms of reliability, understandability, accessibility, discoverability, and interoperability. The C2-SSA COI will drive this improvement, not just in small increments, but with transforming leaps ahead once the COI's processes are in place. It is the COI Pilot projects that are forcing those processes to develop and mature.

The Two Pilot Projects

The C2-SSA pilot will demonstrate two net-centric capabilities—one that helps users understand the availability of a Defense Satellite Communications System (DSCS) satellite link that those same users are depending on and a second capability that provides users with a Global Positioning System (GPS) Navigational Accuracy (NavAcc) prediction alert service.

The Army is leading development of the net-centric DSCS status capability within the COI. DSCS link status data will be pushed from the closed DSCS network (which is "closed" so that it remains "secure") onto a new "open" server on the SECRET Internet Protocol Router Network (SIPRNET)—this will allow DSCS status data to become accessible for machine-to-machine (M2M) exchange via web services. Automating this reporting via M2M exchange means that end users, which includes combatant commanders, space analysts and planners, battalion commanders and space operations officers, would all have access to DSCS outage information in near real-time (within seconds or minutes instead of hours). Therefore, a space ops officer supporting covert special forces inside enemy lines could react intelligently to a loss of direct communications with the special forces. Different actions would result if the silence from the special forces was due to the enemy's proximity (alert the battalion commander) versus if the silence was due to a DSCS link failure (direct the Ops Center to switch to secondary communications).

AFMC's Electronic System Center (ESC)/Combatant Commanders C2 Systems Group is leading the COI's development of an event-triggered navigational accuracy alert service. This capability will allow users to subscribe to and receive updated GPS navigational accuracy predictions (for a particular location and a particular time period). When GPS accuracy degrades, this service will identify the impacted subscribers, re-run the NavAcc software with the new relevant parameters, alert affected users of the change, and provide them with updated NavAcc predictions. The goal is to implement this service such that SIPRNET users with only a browser can both access and benefit from this service. When implemented, changes to GPS signal accuracy, after mission planning is completed but before GPS-guided munitions are released, will result in fewer instances of collateral damage and missed targets. Since GPS signal accuracy is also instrumental to certain unmanned aerial vehicle operations, to rescue operations, and to other categories of combat superiority, the implications of this new service are far-reaching.

Through a User Defined Operating Picture (UDOP), end users will be able to subscribe to either one or both capabilities, which will allow them to receive timely updates. These are just the first two of many services which will eventually be developed under the COI's authority. The UDOP is a first step to achieve a true synthesis of C2-SSA information.

Four Attributes of Net-Centric Ops

ATC needs have pushed creation of a command and control service to aircraft operators, coordinating navigation routes to ensure aircraft are adequately separated both in-flight and on the ground. In the same way, C2-SSA needs are pushing creation of a community-owned process for providing space services net-centrically. There are, in fact, four key attributes common to both ATC and C2-SSA—sharing of information, governance, standard vocabulary, and synthesis of key related information. For ATC, these key attributes are critical in improving and maintaining air safety in civil aviation. For C2-SSA, these attributes are instrumental to the global utilization of DoD's space systems in support of theater operations.

#1. Sharing of Information

In the early days of aviation, only a few aircraft were in the skies; therefore, aircraft operators performed independently from one another and had little need for ground-based control of aircraft. However, as aviation increased in popularity, aircraft were increasingly flown across international and language boundaries. It soon became apparent that aircraft operators needed to communicate and share information, such as their flight path, altitude, and speed of aircraft in order to prevent collisions. Through developments in radio communications, air traffic controllers and aircraft operators were able to communicate over long distances. Sharing information became foundational to avoiding life-or-death catastrophes.

Likewise, at the onset of the information age, information technology (IT) systems were developed in a fragmentary fashion, catering only to specific needs of those users for which they were built. Many IT platforms shared today by our military services, national agencies, and coalition partners still operate as stand-alone systems, managed as independently funded programs, most of which need to exchange data with one another using completely different formats. Sharing data is based on platform communication capabilities and requirements, and each data link may require some translation from one format to another.[1] The C2-SSA information domain is no exception. To fully support the C2 of ALL military services across a wide range of operations, SSA data has to be translated across a spectrum of space systems. Although this is a huge programmatic and social undertaking, limiting the amount of SSA data available is not an option. That would only reduce the Combatant Commanders ability to prosecute their missions effectively.

The DoD published Directive 8320.2, 'Information Sharing in a Net-Centric DoD' in December 2004, codifying the DoD Net-Centric Data Strategy created in May 2003. The Directive describes the DoD's official vision for data and information sharing in a net-centric environment through collaborative forums referred to as COI.[2] Current ongoing efforts by the DoD in general, and through the C2-SSA pilot in particular, will demonstrate how data will be exposed in a net-centric fashion. The C2 SSA COI pilot is a pathfinder for moving to a new paradigm for information sharing across the DoD. Moving to net-centric approaches, including the use of Net-Centric Core Enterprise Services, should lead to: (a) faster access for current users of SSA data, and (b) the ability for unanticipated users to access SSA data without the need for programmatic changes to fielded capabilities. The DoD Net-Centric Data Strategy goals are summarized in figure 1.[3]

Visible	Is an information resource and associated POC discoverable by most users?
Accessible	Is it connected to the network(s), and are tools readily available to use it?
Understandable	Can it be intelligibly used? Are the semantics well documented?
Trusted	Is the source, accuracy, and currency of the resource available to users?
Interoperable	Can it be easily combined or compared with other information or mediated?
Responsive	Is the resource answering user needs? Are robust, direct user feedback mechanisms in place to guide development?

Figure 1. DoD Net-Centric Data Strategy Goals.

#2. Governance

As the need for ATC became prevalent, nations realized that governance would be a major concern. To secure international agreement and the highest possible degree of uniformity across regulations, standards, procedures, and organizations, 32 nations agreed to create the permanent International Civil Aviation Organization (ICAO) on 4 April 1947.[4] ICAO, an agency of the United Nations, established rules and regulations regarding air navigation on a strategic scale, which brought safety in flying a huge step forward and paved the way for the application of a common air navigation system throughout the world.

Similarly, to fuel cooperation and participation across the C2-SSA community, the C2-SSA COI, chaired by the Vice Commander of Air Force Space Command (AFSPC/CV), was established in 2005. DoD Directive 8320.2 defines a COI as "a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes…"[5] Membership includes the ESC, US Army Space and Missile Defense Command, Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC), Space and Missile Center, Joint Space Operations Center, and US Strategic Command. The C2-SSA COI approved the two pilot projects and is exercising the entire COI process while delivering these two operational capabilities within a 12-month period. After the completion of the two pilots, the COI will evaluate the lessons learned and the use of Net-Centric Core Enterprise Services to improve the processes used, bringing C2-SSA a step toward a new approach that is market-based, enterprise-wide, and joint by design.

#3. Standard vocabulary

Because ATC crosses international borders, the vocabulary used to share information must be standardized. ICAO uses the NATO phonetic alphabet, a common name for the international radiotelephony spelling alphabet, which assigns code words to the letters of the English alphabet so that critical combinations of letters (and numbers) can be pronounced and understood by those who transmit and receive voice messages by radio or telephone regardless of their native language. This is especially important when flight safety is at stake. Native English speakers recognize most of the words because English must be used upon request for communication between aircraft and control towers whenever two nations are involved, regardless of their native languages.[6]

The C2-SSA community also realizes the importance of a standard vocabulary in sharing information. By agreeing on a vocabulary, translation from one data format to another will be minimized. The C2-SSA pilot has begun with a small, well-defined vocabulary that will be used as a building block for future capabilities. The C2 SSA COI Data Management Working Group is defining a shared vocabulary unique to both satellite status information and navigational accuracy services. The goal is to create definitions for common terms extensible enough to address specific SSA needs for C2 by operational and tactical commanders. For example, a space operator interprets the term "tank" as a residual piece of a rocket (now orbiting space junk) that held fuel used during the rocket's launch. Ground forces interpret the term "tank" quite differently. The vocabulary must be agreed on (term by term) and then documented in a set of vocabulary products. Finally, it must be formally registered as prescribed by the DoD Data Management Strategy so that all network users can see it, learn it, and use it properly.

#4. Synthesis of Key Related Information

Civil aviation, not only emphasizes the significance of information sharing and governance among air traffic controllers and aircraft operators, but also aims to integrate information from other related areas. To have a complete operational picture, ATC first needs to receive all information affecting the aircraft throughout its flight and then synthesize those inputs so that aircraft operators understand how one type of information affects another. Tests are underway to design new cockpit displays that will allow aircraft operators to better control their aircraft by combining as many as 32 types of information about traffic, weather, and hazards.[7]

In order for C2-SSA to be utilized fully, key related information must to be synthesized as well. During Operation IRAQI FREEDOM (OIF), space systems repeatedly showed how they were a crucial element of our national military power:

- Navigation: 24/7 GPS Enhanced Theater Support—enabled time sensitive and dynamic targeting for OIF
  - o Approximately 70 percent of all munitions used were guided to their targets by GPS signals[8]
- Weather: NASA's Aqua and DoD's DMSP satellites predicted sandstorms and other terrestrial weather events so that commanders and troops could effectively fold that information into their combat planning[9]
- SATCOM: air tasking order transmissions over MILSTAR took six seconds
  - o Approximately 750 Tomahawk missile updates were transmitted via SATCOM
  - o Communications capacity increased from 100 megabits to 2.6 gigabits
  - o Commercial satellites provided 80 percent bandwidth[10]
- Combat support and rescue: the largest number (55 missions) of space-enabled, joint search and rescue operations in history were accomplished, resulting in 73 people saved[11]

The Bottom Line

SSA is an integral part of the space C2 required by all military services across a wide range of operations, and these military ops are comprised of people and resources. So, how does C2-SSA compare with ATC in its impact to its users? Since military forces are put in harm's way as they conduct certain operations, we all share in the responsibility of ensuring that our forces are equipped, not only with proper weapons and gear, but also with the most accurate, reliable, and meaningful information that we have control over. A student pilot once became lost during a solo cross-country flight. While attempting to locate the aircraft on radar, ATC asked him when he last knew his position. The student radioed his reply: "When I was number one for takeoff." ATC eventually found the lost student and guided him safely home. Net-centric C2-SSA information will soon contribute to lives saved and increased levels of military effectiveness; it is already beginning with two pilot projects to map out enduring COI core processes.

Capt Neil A. Soliman (BS, Electrical Engineering and Computer Science, University of California in Berkeley; MBA, University of Colorado in Colorado Springs) is Systems Engineer, Space Division, Combatant Commanders C2 Systems Group, Peterson AFB, Colorado. Captain Soliman serves as the GPS domain expert and DSCS security engineer for the C2 Space Situational Awareness Community of Interest Pilot Working Group. He is responsible for the design, development, and operation of the Net-Centric GPS navigation accuracy prediction alert service and leads the information assurance efforts of the Net-Centric DSCS link status capability.

Captain Soliman was commissioned as a second lieutenant through AFROTC Detachment 085, University of California in Berkeley, in December 1999, where he was a distinguished graduate. Prior to his current position, he served as a GPS space operator, instructor, and navigation analyst and a SATCOM Systems Engineer for the Mobile Consolidated Command Centers.

Notes:

[1] Col Charles Murray, C2ISRC/SC, AFC2ISRC's Vision for Unifying the Air Operations Warfighter Data (briefing, 9-10 August 2005).

[2] DOD Directive (DODD) 8320.2, *Information Sharing in a Net-Centric DoD*, December 2004.

[3] Department of Defense, *DoD Net-Centric Data Strategy,* 9 May 2003.

[4] International Civil Aviation Organization, "Foundation of the International Civil Aviation Organization (ICAO)," http://www.icao.int/cgi/goto_m.pl?icao/en/hist/history02.htm.

[5] DOD Directive (DODD) 8320.2, *Information Sharing in a Net-Centric DoD,* December 2004.

[6] *Wikipedia,* s.v. "NATO phonetic alphabet," http://en.wikipedia.org/wiki/NATO_phonetic_alphabet (accessed 6 February 2006).

[7] US Centennial of Flight Commission, "Air Traffic Control," http://www.centennialofflight.gov/essay/Government_Role/Air_traffic_control/POL15.htm (accessed 23 February 2006).

[8] Lt Gen Michael T. Moseley, "Operation Iraqi Freedom – By The Numbers," 30 April 2003, 11, www.globalsecurity.org/military/library/report/2003/uscentaf_oif_report_30apr2003.pdf

[9] Loring Wirbel, "Technology goes to war: Space nets take commanding role," *Electronic Engineering Times*, 14 April 2003.

[10] "War in IRAQ," *Aviation Weekly*, 9 June 2003, 50.

[11] "War in IRAQ," *Aviation Weekly*, 9 June 2003, 44.

Future Forecasts

Contingency Planning and an Air Force Space Command Information System

Maj Kaylin Freedman, USAF
Michael R. Grimaila, PhD, AFIT

It is a quiet afternoon. You are sitting in your office thinking about how many wings in Air Force Space Command (AFSPC) utilize electronic databases to enter and track operational training, evaluation, and Crew Force Management (CFM) data. This data directly supports the missions of the units by meeting regulatory requirements to maintain proficiency and qualifications, ensuring only personnel meeting the physical requirements perform shifts, determining crew member proficiency for advancement within the unit, and enabling analysis of data to improve operations. No single, common system is in use across the command. The databases in use are not consolidated or standardized and do not interface. This is not efficient and a new system would offer advantages.

You look out the window and envision the accolades you will get if you propose a single, common training, evaluation, and CFM information system and wonder what leadership could possibly fear about a proposal such as this one. Suddenly the phone rings, the site administrator for your single, common information system is on the line wanting to know if you have seen the news and would like your opinion on what to do next. Every phone line in your office starts ringing. Your flustered assistant runs in. You do not know what to do. You put everyone on hold as your assistant explains that a tornado has touched down in Colorado Springs. The building that houses the servers for your system for the entire command was destroyed. The loss of the system means that eight wings and one group, comprising 38 operational units, will have to spend an unspeakable number of man-hours to reproduce, to retrain, and possibly reevaluate over 3,000 operators. Even worse, a data loss could compromise the weapon systems because without the data the units would no longer know who is physically and proficiency qualified to perform a shift. For the three Intercontinental Ballistic Missile bases, this means a nuclear surety incident could occur which would result in a reduction of alert rate for the first time in over 50 years. As you are thinking about what this means for AFSPC and the country, the commander enters your office. You know the commander is looking for answers, but you simply stare speechlessly. Every minute that ticks by you know the units are falling behind, nuclear surety is possibly compromised, and precious manpower is being wasted. The commander is furious and tells you to grab a box and start packing.

The phone rings again, and you realize you were daydreaming. There is no crisis, but now you realize that leadership might resist your idea of a single, common training, evaluation, and CFM information system because of the risk of losing the data due to a contingency such as a natural disaster. So, before you start a proposal for AFSPC, you decide to examine what is necessary to reduce the risk associated with a critical information system and contingencies.

Overview

Building contingency plans calms fears regarding potential losses of information systems which are critical to an organization and vital to the operation's continued success in a time of crisis; the drama demonstrated above provides just some of the results of not planning ahead. For the purposes of this discussion, the focus of the contingency planning is mainly on the impact to information systems and not the impact on people. Although the impact on people is important, military units are required to maintain disaster preparedness plans which already focus on what steps leadership and subordinates should take during disasters to assist with personnel requirements such as first aid, and assembly points. The term "contingency" refers to an event which makes usage of an information system, asset or process, not possible for a period of time or permanently. A contingency does not include an event which precludes usage of an information system as a result of a security issue such as a compromise or malicious attack.

This article will illustrate that a contingency plan reduces risk by examining the impact on civilian organizations and providing examples from 11 September 2001. We then examine the purpose of risk assessment and a technique for conducting risk assessment. A planner cannot properly design a contingency plan until the risk and potential losses are determined because these factors establish the need for a plan. Finally, we provide a guide for constructing a contingency plan. The planner must adhere to a guide to build the plan in order to ensure that it encompasses what is necessary for survival and to ensure the plan is thorough. This article is not all-inclusive, and it is important to note there are a variety of approaches to contingency plans and procedures; the purpose here is to highlight the importance of developing and using a contingency plan and to provide an insight into the overall process of contingency plan construction.

Why Contingency Plans Are Critical

The role of information and the systems providing the information in today's society are vital. The vast majority of organizations would not be able to function without information, and if information were lost, it could be detrimental to operations. In 2000, Price Waterhouse Coopers reported "that 90 percent of all companies that experience a computer 'disaster' with no pre-existing survival plan go out of business within 18 months."[1] The survival rate of organizations without a pre-existing contingency plan seems extremely low, and Price Waterhouse's data would be suspect if other institutions did not report similar results. However, the Hartford Insurance Company found that "on average, over 40 percent of businesses that do not have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm."[2] Gartner Dataquest further substantiated the findings by reporting that "two out of five enterprises that experience a disaster go out of business within five years."[3] Organizations that understand the criticality of contingency plans devote the necessary resources to ensure they are available when needed. According to Donna Scott, a consultant with Gartner Group, banks expend seven to eight percent of their data center budgets on disaster recovery.[4] The number of organizations predicted to fail due to a contingency are astounding, and the amount financial institutions expend on contingency plans highlight the importance of having a solid plan in place.

Unfortunately, 11 September 2001 illustrated why contingency plans are critical. Due to the visibility and the centralization of financial institutions in the World Trade Center, their destruction and the impact widely increased the impact of the desolation. Many companies could not function for days while others were able to return to operations within hours. Deutsche Bank had to evacuate over 5,000 employees, and lost offices and all equipment, but were operational within two hours. A bank spokesperson said, "Our plans worked well, our systems came back up; we were well prepared."[5] Unfortunately, others were not as lucky.

The most significant and common technology failure was the loss of telecommunication. This factor severely hampered disaster recovery for many organizations: "Two major Verizon points-of-presence were located in the World Trade Center complex, and damage was also sustained by a nearby switching unit."[6] Organizations attempting to restore operations and who relied on telecommunications for data transfers and customer support were severely hampered by the reduction in capabilities. An additional crippling factor was the lack of redundancy. Todd Gordon, vice president and general manger for business continuity and recovery services at IBM, said, "There was too much concentration of traffic over networks at one Verizon site" and added that organizations will "require greater redundancy in telecommunications and networking in the future."[7]

Another issue that companies experienced was the complete loss of systems and vital information infrastructure. This caused significant and challenging problems: office space had to be secured, equipment located, and systems built. Leslie Hunt, chief information officer of the Greater New York chapter of the Red Cross, highlighted the importance of having plans in place to establish systems for people to use. Her office had lost everything, and had no plan for how to obtain equipment. Hunt was able to secure 12 computers, create local area network and wide area network, and proceed to work on making the e-mail servers function.[8] However, without a plan, the cannibalized system was fragile and vulnerable. The computers and network were not properly configured and, in the end, could not handle the workload. The Greater New York Website crashed several times and a virus infected the e-mail server, making the systems inoperable for a period of time.[9] For the survivors of 11 September, the Red Cross provided an essential source of information, and without the website and e-mail the Red Cross was crippled. Hunt pointed out the need to have plans which ensure the systems are in place during a disaster so that people can do their jobs "without having to worry about the technology they are using."[10]

Risk Assessment

When the organization is undergoing a contingency, it is not the time to try to determine what information systems are the most critical. In order to avoid this, organizations must conduct a risk assessment prior to a contingency plan being composed or in concert with the initial steps. The assessment should entail determining the organization's assets and processes, assigning a value to the assets and processes, identifying possible contingencies the organization faces, and assembling a detailed report which provides recommendations for building the contingency plan. The risk assessment will ensure the need for a contingency plan is determined before manning is expended on drafting one, and a risk assessment will also ensure the focus of the plan is on the systems the organization has assessed as critical to the organization's operations. A planner can conduct risk assessment or management in a number of ways. The methods are very similar and serve the same goal of helping the organization understand, manage, and reduce the risks encountered in conducting their mission. The process described here is based on the steps highlighted by Michael Erbschloe, author of "Guide to Disaster Recovery." Figure 1 displays the steps involved:

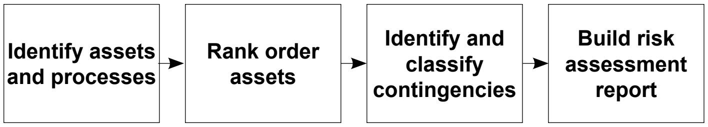

Identify assets and processes
Rank order assets
Identify and classify contingencies
Build risk assessment report

Figure 1: Risk Assessment Steps.

One of the first steps of risk assessment is to identify what assets the organization possesses and the processes used to conduct operations. This means conducting an inventory of every piece of equipment the organization has and documenting the processes that the organization accomplishes in order to fulfill its mission. Erbschloe suggests an organization conduct an exposure inventory which lists "all facilities, processes, systems, and resources that an organization uses to maintain operations and sustain revenue" and includes physical facilities, personnel, equipment, installed systems, information technology, office equipment, and products or parts.[11] Once the equipment is identified, the organization must be aware of how the inventory is used so that during a contingency the right equipment is made available to the right people so the right tasks are accomplished to ensure continued operations. Erbschloe identifies this as the "business processes inventory" and clarifies that it must include: "how a process works, the facilities and buildings in which the process occurs, the departments that perform the process, the personnel who work in the departments, the equipment used by the departments, the installed systems on which the departments rely, the information technology that the departments have in place, and the parts and supplies that the departments need to accomplish their work."[12]

Once planners know what assets are in the organization, they need to know which ones require the most protection. The organization must carefully rank order its assets. During a crisis, people should not spend valuable time determining what equipment is critical to operations and what should be saved. Determining the value of systems in the military can be problematic because there is no profit affected and sometimes no identifiable customer impacted. The planner for a military unit needs to assess the value of the assets or processes based on support to the mission. Can the mission be accomplished without the asset or process? If not, the value is high and the asset or process should earn the highest value of 10. If the answer is yes, the planner must determine at what point the asset or process *does* affect the ability of the unit to perform the mission and assign a value based upon this assessment. According to this model, the greater the number of hours between the assets or processes inoperability and the resulting impact on the mission then the lower the value (determining the spread of the size of the value awarded would be contingent to the number of assets and processes). In other words, a system which would impact the mission in eight hours if the system is not operable would garner a value of eight, whereas a system which would impact the mission in 16 hours if the system is not operable would be given a five.

Once the assets and processes at risk are identified and the value is known, the planner must list and classify the possible contingencies. Peter G. Neumann, moderator of the online ACM Risks Forum, noted that organizations, especially governments, build plans to meet the situations of the past instead of designing plans to meet the potential new situation.[13] One way to avoid this trap is for the planner to ensure all contingencies are classified even though the utility may initially seem insignificant. Listing and classifying all possible contingencies regardless of the probability will actually improve the process by ensuring the organization is prepared for all possibilities and not just the known or most recent ones.

Michael Whitman and Herbert J. Mattord, authors of "Managing Information Security," provide a method to accomplish this task. The planner should separate natural disasters from man-made disasters and list the event followed by the suspected effect on information systems.[14] Erbschloe recommends another process of grouping threats by recurring natural disasters, accidents, and "destructive or disruptive deliberate actions" and classifying as catastrophic, major, and minor.[15] Comprehensive Consulting Solutions, however, suggests creating three different categories for classification. Category I represents the least serious threats that only last for a few hours, such as a brief loss of power. Category II consists of "localized man-made disasters and natural disasters of a more serious nature" with effects lasting for days or weeks. Category III consists of widespread events such as earthquakes or flooding with the potential to have an impact for weeks.[16]

Each of the proposed methods is adequate but when combined they provide a better picture for the planner. The planner should categorize the threats utilizing the numbering system of Comprehensive Consulting Solutions, identify the categories utilizing Erbschloe's categories, and add the suspected effect as Whitman and Mattord suggest. The resulting categories would be as follows: Category I, accidents; Category II, minor natural or human-made disasters; Category III, major human-made or natural disasters; and Category IV, widespread or catastrophic events. Part of identifying and classifying the contingencies is determining the likelihood of the event occurring. The planner must research the probability and devise a probability rating to be included for each contingency. The likelihood of a contingency occurring can be determined by contacting local agencies and conducting research on, for example, flood plains, weather patterns, fault lines, power outages, or grid construction.

Once this research is complete, the planner must tie all of this information together. Erbschole defines this activity as the risk assessment report. This consists of describing the "asset or business process that is exposed to risk, the risks themselves, and the effectiveness of existing systems designed to mitigate these risks."[17] The report is the process of compiling the first three steps described and next determining if the organization's procedures reduce or eliminate the risks identified. Initially, the planner should focus on developing a risk assessment report for the critical assets and processes. When time permits, the planner can return to this step and complete it for those assets and processes that are not as critical. Completing this step and moving to developing a contingency plan should not be delayed in order to accomplish a risk assessment report on low value assets and processes.

Erbschloe also warns that a risk assessment report may contain proprietary information due to its comprehensive details, and organizations should treat the reports as confidential. The planning team will require the reports and leadership may want to review them, but minimal dissemination is ideal due to the detailed content.

Building a Contingency Plan and Beyond

After the planner has assessed risk, the actual contingency plans can be written. A number of different methodologies for writing plans exist and most of them are very similar. "Management of Information Security" presents a comprehensive and usable contingency plan model. This model leads the planner through a logical procession from a minor contingency, to a major, to a catastrophic and describes how to construct plans to address each type. What follows is a broad overview of the model.

According to "Managing Information Security," the contingency plan consists of three components: the incident response plan, the disaster recovery plan, and the business continuity plan. An organization must develop each component for each category of contingency identified during the risk assessment phase. This will ensure that personnel are clear on the required steps and procedures to take during a contingency. As William A. Hussong, Jr., the senior member of the professional staff of the special operations division of System

Research Applications, Inc., explains, "The plan must basically outline people's responsibilities, the use of equipment and other material resources, and detailed operating instructions; nothing can be assumed. The plan is the organization's strategic battle plan for recovery… [and the components] …become the organization's tactical battle plans for survival."[18]

The first, and the largest, component of the contingency plan is the Incident Response Plan (IRP). This is a reactive measure that "comprises a detailed set of processes and procedures that anticipate, detect, and mitigate the effects of an unexpected event that might compromise information resources and assets."[19] It is the starting point for all events and includes a set of procedures for personnel to follow. If at all possible, a contingency should be contained and kept at what was defined as the minor - Category I or II - level with the goal to address it before it becomes a major event. To accomplish this task, the incident response plan must detail the procedures for personnel and the organization to take during, after, and before a contingency occurs. The actions taken are function-specific and are grouped and specifically assigned to individuals.[20]

The IRP is the first component of a contingency plan, and a Disaster Recovery Plan (DRP) is the second. This plan is enacted when a natural or human-made event occurs in which the organization cannot control the impact of an event or the level of damage is so severe that the organization cannot quickly recovery.[21] The DRP plan focuses on preparing for a disaster so that restoring operations and recovery is quickly possible. The plan must address all category levels of contingencies identified during the risk assessment phase. However, the planner must understand that even though the major and catastrophic contingencies - Category III and Category IV - have a lower probability of occurring, they can have the most overwhelming impact to an organization.

The key points of the DRP are "clear delegation of roles and responsibilities," "execution of the alert roster and notification of key personnel," "clear establishment of priorities," "documentation of the disaster," "inclusion of action steps to mitigate the impact of the disaster on the operations of the organization," and "inclusion of alternative implementations for the various systems components, should primary versions be unavailable."[22] The DRP focuses on restoring normal operations to the organization as quickly as possible and includes crisis management steps. The crisis management actions are those "that deal primarily with the people involved" and comprise of detailing public affairs responses, handling emotional issues, and verifying personnel status.[23] The disaster recovery plan prepares the organization to restore operations when the primary operating location is still intact.

When a contingency is so catastrophic that an organization is unable to operate out of its primary location, then the last component of the contingency plan, the Business Continuity Plan (BCP), must be enacted. This plan includes the strategies to ensure the company can continue to perform its mission and continue to function during a contingency, regardless of the magnitude, and is usually managed by the leadership.[24] The BCP is critical because an organization must continue to perform its mission or the organization risks going out of business, which for a military organization could impact the security of the entire nation or worse. The key here is developing plans to ensure the most mission critical assets or processes are able to continue to function or to ensure they can be quickly restored regardless of the occurrence of a contingency.

Restoring assets and processes is possible by taking pre-contingency actions to protect the information. Accomplishing this serves several purposes such as ensuring that data critical to the organization's mission is available, guaranteeing facilities are available, and reducing risk. The organization should conduct pre-contingency actions on those high value assets and processes identified in the risk assessment phase.

As mentioned above, the organization's assets and processes were ranked based upon their value to mission performance. The planner used this information, budgetary constraints, and acceptable risk levels to evaluate which options work best for contingency. Six available options are suggested: hot site, warm site, cold site, timeshare, service bureau, and mutual agreement. The first three options are "exclusive-use" (only the organization can use the site) and the remaining options are shared-use. "A hot site is a fully configured computer facility, [and it has]…all services, communication links, and physical plant operations" available.[25] Although this option is expensive, it provides instant recovery of data and operations can continue almost seamlessly (assuming the hot site is not also impacted by the contingency). The next option is a warm site which "provides many of the same services and options as the hot site, but typically software applications either are not included, or are not installed and configured."[26] Finally, a cold site, the least expensive option, consists of "only rudimentary services and facilities" and is essentially "an empty room with standard heating, air conditioning, and electrical services."[27]

Shared-use options, unlike exclusive-use, mean that the organization shares usage of the facility or services with another organization. The timeshare option can be a hot, warm, or cold site, "but it is leased in conjunction with a business partner or sister organization."[28] Success is contingent upon the partner or sister organization's cooperation and adherence to the timeshare agreement. A service bureau can be employed and is "a service agency that provides a service for a fee" such as data storage or floor space.[29] The final option is the mutual agreement which "is a contract between two organizations in which each party agrees to assist the other in the event of a disaster."[30] An organization chooses which option is right for them based upon what expense it can support, what level of risk it is willing to accept, and the timeframe of desired operational recovery.

All of the options require the ability to access the organization's data, information systems, and processes in order to operate. There are three different methods of storing or protecting the data, information systems, and processes. One of these is electronic vaulting: "the bulk batch-transfer of data to an off-site facility."[31] The organization periodically conducts a batch-transfer of data to a server at another location. Except that the server is located off site, this is similar to a traditional back up; the data is only as current as the latest transfer. Remote journaling, another option, transfers "live transactions to an off-site facility" so the transaction is current, but it does not transfer the archived data.[32] The last and most comprehensive option is data shadowing which "combines electronic vaulting with remote journaling, by writing multiple copies of the database simultaneously in two separate locations."[33] Although data shadowing is expensive, it is the most thorough, will reduce the time required to recover operations, and ensures profit loss and mission impact is minimal.

Once the planner writes the contingency plans, they must be tested and updated on a regular basis to ensure currency, accuracy, feasibility, and applicability. Although many organizations affected on 11 September had contingency plans, many were not usable. A consultant at Strohl Systems, a recovery software and services firm, explained that "in some cases, the plans were too big and ignored detailed issues-where to meet, how to contact people, having a disaster hotline that works when all phone systems are down."[34] The senior vice president of field operations at Comdisco, a contingency services provider added, "We found that [during the events of 11 September] our clients were for the most part undersubscribed in terms of their need for contingency work areas and networks and terminals…Plans need to be updated every six months."[35] Hussong, the senior member from System Research Applications, Inc., however recommends rewriting contingency plan procedures at least every five years to ensure requirements are kept current, new technologies are utilized, and "fresh eyes…look at old solutions to new problems."[36]

The actual contingency plan must be available during a contingency. As one firm discovered during 11 September, the only copy of the contingency plan was located in the World Trade Center offices, and at another organization, said Strohl Systems' Banker, "they had copies of the recovery plan on the network in New York and London and Tokyo, but they could not get to any of them [due to the lack of telecommunication]."[37] However, there is a difficult balance to maintain between availability and protecting the organization. To ensure the plan is available accessible, organizations must have multiple copies of contingency plans available as hard copies, on different networks, and even on multiple hard drives. However, due to the proprietary issues and other classifications issues, the organization must be careful not to broadcast the plan to uncontrolled locations. This is an essential point for the planner to keep in mind as they disseminate the completed plan to the personnel in the organization.

Option For Air Force Space Command

A single, common training, evaluation, and CFM information system for all of AFSPC would be subject to risk from a contingency just like any other system. However, if risk assessment is conducted and a contingency plan is built AFSPCs leaders could accept the risk of a contingency occurring.

One way to immediately reduce the risk of a contingency is to wisely choose the location of the database server based upon what was learned about contingency plan building. Utilizing the Air Force's Global Combat Support System (GCSS) is one way to apply this knowledge. According to the Warfighting Integration and Chief Information Officer, Knowledge Information Management Branch at Headquarters Air Force, the GCSS provides a central enterprise server bus to house data that permits authorized users access via remote sign on; it is a set of enterprise information services and is protected by multiple layers of security.[38] Defense Information Systems Agency (DISA) is responsible for parts of GCSS. DISA hosts GCSS on a server farm located in Alabama with data shadowing occurring with a server farm at Wright Patterson AFB in Dayton, Ohio. There is a third server farm proposed for San Antonio, Texas which will have the same data shadowing service. Data and transactions will therefore be stored in three different geographical locations, significantly reducing risks. AFSPC users would access the single, common information system via remote sign on through the Air Force Portal Graphic User Interface.

Housing the database on the GCSS is only one way to reduce the risks associated with this system and will increase leadership support. A full risk assessment and contingency plan would need to be accomplished in order to further mitigate the risk to an acceptable level.

Conclusion

Without contingency plans, organizations risk not being able to survive or experience mission failure. Contingency plans help an organization to determine what risks they are willing to accept and what risks are unacceptable, providing the opportunity to take actions to mitigate unacceptable risks. Using examples of what organizations experienced during 11 September, we have illustrated why a contingency plan is critical. As highlighted, the loss of capabilities for organizations without a plan or those with untested plans is devastating. Before a contingency plan can be initiated, a risk assessment must be accomplished as it identifies the assets and procedures that are important to the organization, attempts to determine types and chances of a contingency occurring, and assigns a value level to the asset or process so the organization knows where to focus its efforts. Only after this has occurred can a contingency plan be built. A number of different approaches exist to build a contingency plan. The blueprint presented here is a logical and thorough method. An incident response plan is designed to establish procedures to deal with the event immediately. A disaster response plan is the next step. This will ensure there are procedures available if the contingency cannot be contained with the incident response plan. The last plan to be designed is the business continuity plan which ensures the organization can restore operations if the contingency renders the primary site unusable. With the contingency plan, comprised of these components, an organization is prepared to successfully face almost any risk.

Armed with this information, an organization will be able to face a contingency and survive. Now you can stop staring out the window and begin to effectively address some of leaderships' possible concerns regarding the implementation of a single, common training, evaluation, and CFM information system and finally make the dream a reality. Each of us has a responsibility to contribute to the survivability of their organization. Can your organization survive a disaster?

Notes:

[1] Andy S. Krupa, "The Oversight of Physical Security and Contingency Planning," SANS Institute (2003), 1.

[2] Michael Whitman and Herbert J. Mattord, *Management of Information Security* (Canada: Course Technology, 2004), 65.

[3] Parveen Bansal, "Ministers of Information," *The Banker* 151 (November 2001) 92-93.

[4] Johannah Rodgers, "A Sense of Urgency," *Bank Systems & Technology* 38 (7 December 2001) 32-34.

[5] Ibid., 32.

[6] Ibid., 33.

[7] Ibid., 33.

[8] Matthew Vilano, "9/11: A Lesson in Crisis Control," *TechRepublic*, 21 December 2001, http://www.techrepublic.com (12 November 2005).

[9] Ibid.

[10] Ibid.

[11] Michael Erbschloe, *Guide to Disaster Recovery*, (Canada: Course Technology, 2003), 52.

[12] Ibid., 58.

[13] Peter G. Neumann, "Anticipating Disasters," *Communications of the ACM* 48 (Mar 2005), 128.

[14] Whitman and Mattord, *Management of Information Security,* 77-78.

[15] Erbschloe, *Guide to Disaster Recovery,* 62, 137.

[16] "Defining what Types of Disasters Need to be Planned for," Comprehensive Consulting Solutions, Inc., March 2001, http://www.compsoln.com (11 November 2005).

[17] Erbschloe, *Guide to Disaster Recovery,* 64.

[18] William Hussong Jr., "So You're the Company's New Contingency Planner!," *Disaster Recovery Journal*, http://www.drj.com (12 November 2005).

[19] Whitman and Mattord, *Management of Information Security,* 67-68.

[20] Whitman and Mattord, 68-69.

[21] Whitman and Mattord, 77.

[22] Whitman and Mattord, 79.

[23] Whitman and Mattord, 80.

[24] Whitman and Mattord, 82.

[25] Whitman and Mattord, 83.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Whitman and Mattord, *Management of Information Security,* 84.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Rodgers, "A Sense of Urgency," 32.

[35] Rodgers, 33.

[36] Hussong, 2005.

[37] Rodgers, 34.

[38] Action Officer, Warfighting Integration and Chief Information Officer, Knowledge Information Management Branch, Washington DC, personal meeting, 14 October 2005.

Dr. Michael R. Grimaila (BS, MS, PhD, Texas A&M University; CISSP, CISM, GSEC) is currently an Assistant Professor in the Systems and Engineering Management department and a member of the Center for Information Security Education and Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Dr. Grimaila serves as Editor of the Journal of Information Assurance, Security, and Protection (JIASP), Editorial Advisory Board member of the Information System Security Association (ISSA), and is a member of the International Systems Security Engineering Association (ISSEA) Metrics Working Group. He also holds memberships in the ACM, IEEE, IRMA, ISACA, ISC2, ISSA, ISSEA, and the SANS Institute.

Maj Kaylin Freedman is currently an Intermediate Developmental Education student at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio, and is pursuing a Master in Strategic Leadership with an Information Assurance sequence, which will result in also earning the National Training Standard CNSSI No. 4012 certification. After graduating from the University of Texas, she attended Officer Training School, Maxwell AFB, Alabama. Major Freedman has served the Air Force for over 12 years in a variety of positions from adjutant to missileer to orbital analyst. Prior to her current position, she was an Operations Officer at Detachment 1, 533d Training Squadron, Schriever AFB, Colorado.

Book Review

Into the Unknown Together: The DoD, NASA, and Early Spaceflight

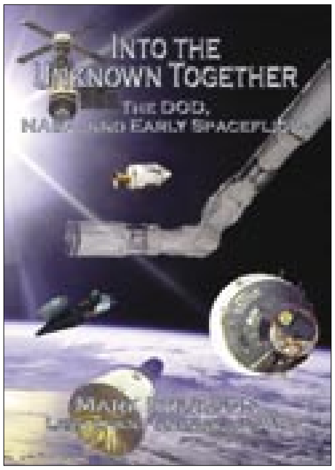
Into the Unknown Together: The DoD, NASA, and Early Spaceflight. By Lt Col Mark Erickson, USAF, PhD. Maxwell AFB, AL: Air University Press, 2005. Notes. Glossary. Index. Pp. 668. Free to Airmen! Available from http://www.au.af.mil/au/aul/aupress/Books/Erickson/erickson.pdf

This book fills in a huge, gaping hole in space historiography by examining the NASA-DoD relationship during the heyday of human spaceflight, the 1950s through the 1970s. By focusing on NASA's Projects Mercury, Gemini, and Apollo, and DoD's Dynasoar and Manned Orbiting Laboratory (MOL) projects as a lens with which to illustrate NASA-DoD relations, Lt Col Mark Erickson examines the geopolitical, domestic political, and bureaucratic environments of the American space program(s). In doing so, the author, and active duty Air Force space professional, concludes that the Air Force, as the agency directly responsible for both Dynasoar and MOL, "failed in its attempts to evaluate and use humans in space for military purposes" (p. 1).

Using a big-to-little approach, the author examines the grand strategy behind the NASA-DOD relationship in human-spaceflight programs by looking at three issues before drilling down into the details. First of all, he looks at the attitude of Presidents Dwight D. Eisenhower, John F. Kennedy, and Lyndon B. Johnson toward the use of space exploration as a tool to secure international prestige and national pride in the Cold War. By examining what role each man specifically wanted space exploration to play in the geopolitical struggle with the Union of Soviet Socialist Republics (USSR), he analyzes each president's pronouncements on such topics as space for peaceful pursuits, human spaceflight, and space for prestige purposes. Each president's specific actions in the field of space policy, human-spaceflight projects, and cooperation with the USSR in space are key pieces of the puzzle. For example, Eisenhower did not believe the United States should race to the moon in search of prestige because "the quest for reliable reconnaissance of the Soviet Union was the fundamental driving force behind Eisenhower's space programs and policy" (p. 3). This is an important point: in the Eisenhower administration, reconnaissance satellites were more important than moon landings. On the other hand, Kennedy believed and reoriented American space policy toward the moon specifically for prestige purposes. Johnson "continued this lunar landing goal but refused to expand American space policy beyond it as he grappled with the demands of Vietnam and the Great Society" (p. 2).

Next, the author looks at the institutional relationships between NASA and the DOD—the level of support, coordination, and rivalry during each president's administration. The third area the book focuses on is the actual projects themselves: Mercury, Gemini, Apollo, Dynasoar, and MOL. The author shows that neither doomed project—Dynasoar or MOL—failed due to NASA's urging, but rather, the "complex mixture of financial, political, international, and institutional factors . . . eventually led to their demise" (p. 3). Unfortunately, he does not offer an answer to the question "What was the NRO's role in the demise of these two programs?" a question that may, in the end, be outside the scope of this book or even impossible given security constraints. In the end, the author concludes that "During its first few years, NASA was heavily dependent on the DOD, and particularly the Air Force, for launch vehicles, top-level managers, national ranges and tracking stations, and expertise in the initiation and administration of large aerospace systems" but that "NASA-DoD interaction continued to involve supporting each other (but mostly the DoD supporting NASA)" (p. 528).

What is the value of this book for the space professional? First of all, this is a good book on the necessary preconditions and development of the space race that covers the issues and documents the history of the fundamentally critical NASA-DoD relationship, without being as difficult to read as the Pulitzer Prize-winning book on space by Walter A. McDougall, . . .*the Heavens and the Earth: A Political History of the Space Age* (New York: Basic Books, 1983). Although Erickson naturally covers some of the same ground as McDougall, this examination of the evidence goes in a different direction, further amplifying its usefulness. This book's utility is aided by the fact of its easy availability: electronic downloads are free and so are paper copies to Airmen when ordered through the Air University Press website. It is a shame that this book was not published by a more traditional academic press because it will not receive the same kind of widespread distribution it deserves. On the other hand, the largest shortcoming of this book is that it is very heavily reliant on its past as a PhD dissertation: for example, many of the author's points are supported by what other historians and political scientists have written on the subject (page 537 has a two-paragraph stretch with footnotes referring to what four other historians have written). Although admirably demonstrating that his thesis sits firmly in the John Logsdon school of space and politics, the book, which comes in at 668 pages, could have benefited from a culling of the "dissertation-ese" to reduce its already hefty throw-weight. However, this is a minor criticism since space professionals can gain a quick tutorial in what other space historians and policy wonks have said while learning about the most critical intragovernmental relationship of the space race.



Lt Col David C. Arnold, executive officer to the Director of Strategic Planning, HQ USAF. His book, Spying from Space: Constructing America's Satellite Command and Control Networks (College Station: Texas A&M University Press, 2005). Lt Col Arnold is also the editor of Quest: The History of Spaceflight Quarterly journal.

We are interested in what you think of ***High Frontier*** and request your feedback. We want to make this a useful product to each and every one of you as we move forward in the development of our space professionals and to stimulate intellectual thought. Please send your comments, inquiries and article submissions to: HQ AFSPC/PAI, High Frontier Journal, 150 Vandenberg St, Ste 1105, Peterson AFB CO 80914-4020, Telephone: (719) 554-3978, Fax: (719) 554-6013, Email: afspc.pai@peterson.af.mil, To subscribe: nsage@colsa.com

U.S. AIR FORCE

AIR FORCE SPACE COMMAND

AFSPC/PAI
150 Vandenberg St.
Ste 1105
Peterson AFB, CO 80914
Telephone: (719) 554-3978
Fax: (719) 554-6013
For more information on space
professional development visit:
www.peterson.af.mil/spacepro

Air & Space Power Journal:
www.airpower.maxwell.af.mil/airchronicles/apje.html