INSIDE:

- Employing Elements of National Power in Schriever V
- A Space Doctrine for Soldier, Scientist, and Citizen: What It Will Take to Secure the Space Domain
- The Value of the Domain
- Coalition Space Operations: Lessons Learned from Schriever V Wargame
## Contents

### Introduction
- General C. Robert Kehler ................................................. 2

### Senior Leader Perspective
- Building the Political Consensus to Deter Attacks on Our Nation’s Space Systems
  - US Representative Terry Everett ........................................ 3
- Employing Elements of National Power in Schriever V
  - VADM Carl V. Mauney ....................................................... 9
- Schriever V Wargames: The Boundaries of Space and Cyberspace
  - Lt Gen Larry D. James .................................................... 12
- Schriever V - A UK Perspective
  - AVM T. M. “Timo” Anderson ............................................. 14
- A Space Doctrine for Soldier, Scientist, and Citizen: What It Will Take to Secure the Space Domain
  - Ambassador Lincoln P. Bloomfield, Jr. ................................ 17
- Political-Military Implications of Space Warfare on Homeland Defense and Allied Relations
  - BG Robert J. Felderman .................................................... 23

### Schriever V Wargame
- The Value of the Domain
  - Col Robert F. Wright, Jr. ................................................. 26
- Coalition Space Operations: Lessons Learned from Schriever V Wargame
  - Mr. Joseph D. Rouge and Mr. Dennis L. Danielson ................. 28
- Schriever V: Lessons Learned - A Canadian Perspective
  - Col François Malo .......................................................... 30

### Industry Perspective
- The Strategic Value of Schriever V: Policy and Strategy Insights for the Quadrennial Defense Review
  - Mr. Marc J. Berkowitz ...................................................... 32
- Schriever V: Managing and Understanding Consequences to Military Space
  - Maj Gen Franklin “Judd” Blaisdell, USAF, retired .................. 37

### Historical Perspective
- Schriever Wargames: The Battle for the Ultimate High Ground
  - Mr. James C. Mesco ........................................................ 38

### Book Review
- Wargaming for Leaders: Strategic Decision Making from the Battlefield to the Boardroom
  - Dr. Rick W. Sturdevant .................................................... 42

Next Issue: Space Acquisition
**Introduction**

**General C. Robert Kehler**  
**Commander, Air Force Space Command**

Over the past 10 years, the Schriever Wargame series has influenced space operations not only within the Air Force, but in joint and coalition space operations as well. While the wargame began as a venue to examine advanced space technologies in various scenarios, it has evolved into an opportunity to explore policy and strategy issues as well as diplomatic, economic, military, and information activities. Decision making and supporting command and control processes have emerged as some of the most important aspects of the wargame. Each wargame has also demonstrated the importance of integration at the national and international level. Just as real-world military operations have proven the value of coalition air, land, and sea operations, we have discovered the value of coalition space and cyberspace operations. Schriever V focused on the integration of the whole of government—reaching beyond Department of Defense and incorporating critical participation from national level decision makers, allies, civil space organizations, and commercial space companies and consortia. Some would say the complexity of space activities now calls for a “whole of nations” approach. The Schriever V game provided actionable insights for all participants to better prepare for a future conflict that would likely begin in cyberspace and soon extend to space. I am grateful for the outstanding support and participation of all our players—their contributions have helped in developing a strategy to protect US and allied space capabilities. This issue of *High Frontier* compiles the perspective of the game participants and highlights the complex nature of a conflict involving space and cyberspace.

The first five articles provide the “Senior Leader Perspectives” from civilian, Air Force, joint and allied participants in the wargame. Former Representative Terry Everett served as the game president during Schriever V and provides an insightful perspective on the national level issues that surfaced during the game. VADM Carl Mauney, deputy commander of US Strategic Command, discusses how elements of national power were combined in the two years of planning leading up to the wargame, and how the whole of government approach was effectively used during Schriever V. Lt Gen Larry James, commander, 14th Air Force, highlights the critical operational issues exposed during the wargame and future actions required to improve capabilities, especially in the area of situational awareness. AVM T. M. Anderson, assistant chief of the Air Staff of the Royal Air Force discusses the value of integrating coalition members into the wargame and advocates developing a standing Coalition Joint Task Force-Space. Ambassador Lincoln Bloomfield, Jr., chairman of the Henry L. Stimson Center, explores the many aspects of what it will take to properly secure the space domain. BG Robert Felderman, deputy director of plans, policy and strategy for North American Aerospace Defense Command and US Northern Command details the requirement for a family of systems approach including space and cyberspace capabilities for homeland defense.

The commander of the Space Innovation and Development Center (SIDC), Col Robert Wright, begins the “Schriever V Wargame” section by explaining how the game is structured to account for the global impact of warfare on space systems. Mr. Joseph Rouge and Mr. Dennis Danielson of the National Security Space Office highlight lessons learned on integrating and sharing information among coalition members and the way ahead. Col François Malo, director of space development at National Defence Headquarters, Canada, completes the section by emphasizing how global dependence on space necessitates a comprehensive approach to preserve and protect the domain.

Schriever V greatly benefited from industry representation and Mr. Marc Berkowitz, vice president, situational awareness, Lockheed Martin Corporation provides a unique point of view for the “Industry Perspective” section. His article explores the many questions policy makers must grapple with as space strategy and policy options are developed. Maj Gen “Judd” Blaisdell, USAF, retired, recommends industry intensify developments in support of operationally responsive space and space situational awareness.

Mr. James Mesco, historian, SIDC, provides a look back at the Schriever Wargame series, detailing participants and the significant findings of each game. His article chronicles the evolution of the games’ orientation from technology test bed to policy focused.

Dr. Rick Sturdevant concludes the journal with a review of the book *Wargaming for Leaders: Strategic Decision Making from the Battlefield to the Boardroom* a book that espouses the values of wargaming as a method of exposing both solutions and problems.

I hope you find the analysis of the Schriever V Wargame within this edition of the *High Frontier* exposes the complexities facing our nation and allies in dealing with space policy and conflict involving the space domain. Our next issue will focus on space acquisition. Air Force Space Command is unique because we are the only major command in the Air Force with our own acquisition arm. This hybrid structure creates opportunities that must be leveraged to achieve excellent program acquisition practices and mission success.
Building the Political Consensus to Deter Attacks on Our Nation’s Space Systems

US Representative Terry Everett (R-Alabama)
Senior Advisor to the Space Protection Program
Rehobeth, Alabama

Last March I had a most unusual experience—I played the president of the United States in the Schriever V wargame sponsored by the commander of Air Force Space Command (AFSPC), General C. Robert Kehler. The experience made two things very clear to me: First, we must have a strategy for space deterrence, and second, that strategy must realistically reflect the domestic and international politics of space. The Schriever game took on both issues by embracing a “whole of government” approach that not only included military options for protecting space but also brought to bear political, economic, and diplomatic measures as well. Wise policy counsel from knowledgeable team members who played the president’s cabinet and presented a full spectrum of government policy initiatives was invaluable to me in the course of the president’s cabinet and presented a full spectrum of government policy initiatives was invaluable to me in the course of eight days of game play.

Late one evening as I was preparing to record a message to the American people (in this case, the game participants) as player-president it was clear we were in the midst of a deepening crisis. The crisis had started as a dispute over natural resources and had rapidly escalated to attacks on our space capabilities. As I reflected on what I was about to say, I thought about everything our team had done to defuse the crisis that was unfolding. We had reached out with diplomatic measures, sought the counsel of our allies, we attempted to be clear and transparent in our actions in accordance with international standards—all to no avail.

I thought about the signals that were misread by our notional opponent who had not understood the grim challenges or the great risks that both nations would face. Neither did our opponent understand that we would not view the actions they had taken the same way they did. I wondered how to explain to the American people that we had worked tirelessly with our coalition partners to defuse a crisis which had already resulted in the loss of global transport and communication services—services which deprived the people of the world the information they needed every day for national security, commerce, to transport goods, and maintain their way of life.

My team members and I knew that the US clearly depends on space more than any space-faring nation, but we also recognized that all nations have become dependent on space assets for a number of reasons (see inset). As I reflected on what I was going to say, I knew one thing for sure: no real president should ever be put into the position and face the decisions that I was about to make.

It is a fair question to ask, why should we as a nation be concerned when there are so many other pressing problems facing us? Why is it necessary to develop solutions to a problem that seems so unlikely, compared to, say, cyber attacks? For two simple reasons: first, the future of our nation’s well being depends on space and, secondly, we must never confuse the un-

Our Growing Dependency on Space Capabilities

We have witnessed tremendous growth in commercial and civil uses of space; growth that was not imagined a few years ago. On the commercial side, the Space Foundation’s Space Report 2009 states that the global space industry grew to nearly $260 billion in 2008, despite the global economic turmoil.

Commercial aviation, shipping, emergency services, in-vehicle navigation, vehicle fleet tracking, and automated teller machine and financial transactions have come to rely on services from space. Agriculture has benefited from the application of the GPS and satellite imagery to track farm equipment, assess crop health, and forecast crop production. Most recently, rapid damage assessments and survivor search and rescue from Hurricane Ike were made with support from Global Hawk unmanned aerial vehicles which communicated to the ground via satellites. And the dependency will rapidly increase as space technology continues to improve.

Equally important, space capabilities underpin our nation’s conventional military superiority and provide us with an overall strategic advantage relative to any other country. General Kehler has stated that the loss of our space assets would make us dependent on 1950s technology while the former commander of AFSPC, General Lance W. Lord, has stated that we could not fight a war without space. I have explained in previous editions of High Frontier that I have often told members of Congress the aircraft, naval vessels, and land vehicles they have supported and funded could not be effective without the communication, navigation, and other services provided by our space capabilities.

These capabilities have revolutionized the way we fight. For example, in World War II we used as many as 1,500 B-17 sorties and 9,000 250 pound bombs to hit one target, while in June of 2006 al-Qaida leader al-Zarqawi was targeted with one F-16 sortie and two 500 pound bombs. This successful strike mission was heavily reliant on space, and used, among other things: high resolution satellite imagery to geo-locate the target within meters; satellite communications to the cockpit for real-time updates, and GPS guided precision munitions to minimize collateral damage.

Many in the space community have heard me make these points before, so why do I repeat these observations here? Because we still have not had a public debate on space and most of the public, including the Congress, takes these capabilities for granted.
likely with the unfamiliar. The loss of space capabilities, however unfamiliar such a circumstance might be, is unfortunately a real possibility. We can ill afford a 9/11 in space. It would be a catastrophe that would harm us as a country, perhaps for decades, and have dire consequences for every nation on earth.

Paradoxically, because cyber attacks occur every day on some part of the nation’s information technology infrastructure, we are starting to put in place measures to cope with these events. Secretary Robert M. Gates recently signed a directive establishing a subordinate unified Cyber Command under US Strategic Command. In doing so, Secretary Gates noted that our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. Events over the July 4th weekend proved his point: denial of service attacks were targeted against dozens of government and private sites, according to a report by the Associated Press. The report quoted Maj Gen Dale Meyerrose, USAF, retired, former chief information officer for the US intelligence community, as saying that at least some of the federal agency web sites got saturated with as many as 1 million hits per second per attack — amounting to 4 billion Internet hits at once.1

In the same vein, the Schriever Wargame should be understood as a cautionary tale about attacks occurring on our space systems. Indeed, simultaneous attacks on both space and cyber systems would not be a surprise. If there is one lesson to be learned from the game it is that we have an obligation to protect our assets. If we are careful, prudent, and wise, we may never face these circumstances. But creating a national and international consensus and making the necessary preparations to reduce the risk of encountering a future crisis in space will be a large, complicated undertaking. But that is exactly the point: while the US uses space more than any other country, all nations can ill-afford the possibility of losing the use of space. Even those nations which have no assets in space would suffer greatly if those assets were lost.

**The Need for an Effective Space and Cyber Deterrence Strategy**

The implications of our nation’s dependence on its space capabilities coupled with the potential vulnerability of these capabilities implies, at a minimum, that there is an urgent need to develop a modern strategy of deterrence. This strategy must encompass both space and cyber capabilities. This strategy must be based on a solid, bi-partisan political consensus across both the Congress and the executive branch. Ultimately, this consensus will need to extend to friends and allies as well.

Because of our obvious dependence on space capabilities, potential adversaries are showing increasing interest in counterspace capabilities; others who possess space-faring technology are developing significant counterspace capabilities.

Space is inherently an unstable environment for warfare, however. Unlike terrestrial conditions in which borders, coastlines, and mountain ranges exist, in which history holds at least some war-ending lessons, and in which there has been considerable thought applied to escalation control, there are no natural “firebreaks” if a war in space were to break out. If space warfare once starts—as some experts think could happen relatively early in a crisis or war—the consequences to the future use of space would be devastating and long lasting.

Key elements in traditional theories of deterrence—mutual assured destruction, secure second strike, flexible response, the nuclear triad—may not necessarily apply to space. An adversary in any case may not have bought into any of them. We do not know. Worse, there is a pervasive assumption that those theories that pertained to the Cold War, and nuclear warfare, are readily transferable to space. That is a dangerous assumption, especially in a deadly serious crisis, if it should prove to be unfounded.

In an article published a year ago, entitled “New Nuclear Realities,” former Secretary of Defense Harold Brown argued that much of the impetus for nuclear proliferation has come from US conventional superiority. He forcefully argued for policies to impede nuclear proliferation, but then added a critical caveat to this strategy: … to the extent that fear of the US motivates proliferation, the real drive for nuclear weapons capability in Iran and North Korea, as it was in Libya, does not come from fear of US nuclear capability or the content of US nuclear policy. It will not be eased by reductions in or the downplaying of US nuclear capability, justified as such actions are. Rather, it comes from US conventional power-projection capability and the concern that it may be used to intimidate, attack, or overthrow regimes, as it has done before. [emphasis added]2

I think it natural to extend Secretary Brown’s argument to space. Countries that seek to dissuade US intervention will look for other ways besides nuclear weapons to degrade or disable US conventional military capability. Counter-space (and counter-cyber) systems present an attractive alternative and some of these are relatively low-cost.

Because no country relies as heavily on space capabilities for supporting the operations of military forces as does the US any approach to deterring attacks on our space systems would inherently be asymmetrical. We would need to look elsewhere for leverage. And we might need to concede that even if an asymmetrical deterrent strategy could be found, attacks against some elements of our space systems would likely occur.

But the issue goes beyond our military capabilities. Fundamentally, the need for a deterrent strategy is one that concerns all nations. Any crisis that leads to attacks on space systems and services would instantly be felt around the world. No one
would be unaffected. The Schriever Wargame in this respect truly was a cautionary tale.

**Achieving a Practical Deterrent Strategy**

The fundamental starting point for devising a strategy of deterrence is to consider how space is used: the mission performed by space systems typically is to gather and deliver information for economic, civil, and military purposes. In short, only space can provide the critical needs of our nation. The need to preserve and maintain information, both in its timeliness and complexity, should therefore be linked to a strategy. A strategy which deters attacks on these systems and the consequences of the loss of critical information if these systems are attacked. This will require a new look at deterrence theory.

Much of the discussion to date within the Congress and executive has focused on the advisability of pursuing a conflict involving space systems, as if a decision one way or the other would resolve the matter. But the enemy gets a vote, too.

We therefore must take a close look at the extent to which previous deterrence theories would apply to potential adversaries, the degree to which other space-faring nations may or may not ascribe to those theories, and where there might be differences. At the very least, we need to understand the motivations of potential opponents and the circumstances under which they would contemplate attacking our space systems and services.

There has been little or no debate on pre-conflict deterrence, including how to limit threatening behavior that would constitute a red line that must not be crossed, or how to manage war termination stages. Moreover, little thought about escalation control in trans-conflict phases or how information needs would change during a conflict. As a result:

- Legislation passed by Congress focuses on space technology development and acquisition programs.
- There is no direction from Congress to the executive to give greater attention to a deterrent strategy that would drive operational planning and acquisition decisions, as would befit a reality where vital national interests are at stake.
- Debate on the elements of a deterrent strategy is notably absent in the executive branch and the Congress.
- There is no sense of urgency and specific solutions lack a strategic framework to guide concepts and operations.

To remedy this situation, an effective deterrent strategy would be based upon our uses of space for information gathering and transmission and an understanding of how potential adversaries perceive its importance to us and to themselves.

If this is a starting point for our deterrence strategy, there are nevertheless many issues that a practical implementation of that strategy would need to cover. To get started, I suggest three practical steps to take which together would significantly reduce the risk of any conflict escalating to space:

1. Instill in our civilian and military leadership the recognition that they must become relentlessly demanding customers of research and analysis that explains the motivations, goals, and risk-taking behavior of potential opponents as applied to space systems.
2. Establish programs that will deliver exquisite transparency in the operations of space systems.
3. Promote policy stewardship for developing and maintaining a deterrent strategy.

**Become a Demanding Customer.** Secretary of Defense Gates said in his national defense strategy that deterrence requires influencing the political and military choices of an adversary, dissuading it from taking an action by making its leaders understand that either the cost of the action is too great, is of no use, or unnecessary. He said deterrence also is based upon credibility: the ability to prevent attack, respond decisively to any attack so as to discourage an adversary from even contemplating an attack upon us.

I would take Secretary Gates exhortations to heart. Our civilian and military leadership must have a deep and multi-dimensional understanding of adversary behavior. In his seminal work on the history of deterrence, Dr. Keith B. Payne in the *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* points out that knowledge of the adversary is a lynchpin of a durable deterrence strategy.

He highlights the need to understand an opponent’s personal beliefs, goals, and values—and I would add politics—and the need to determine whether an opponent is motivated to practice a high risk form of brinkmanship. Indeed, he lays out a detailed framework for getting to know your enemy. For example, he lists a set of information requirements associated with identifying and describing those factors likely to affect an adversary’s decision-making in the context of a specific flashpoint and US deterrent threats.

In the course of the wargame I played, it was clear that the sides were misreading signals that were deliberately conveyed to reduce the chances of escalation of attacks on space systems. Why? In my view, both sides had caricatured the objectives and intentions of the other. We did not understand how to influence our opponents’ decisions nor did we understand the politics at play in the region. Most crucially, we were unable to understand the linkage between an unfolding crisis on the ground and how this might translate into threats against space systems.

A practical solution to this problem is to create customer demand for quality analysis of foreign leadership goals and intentions with respect to space. Our senior leadership should not take any research product from any source—academic institution or intelligence agency—at face value. They will need to

---

*There has been little or no debate on pre-conflict deterrence, including how to limit threatening behavior that would constitute a red line that must not be crossed, or how to manage war termination stages.*
Deterrence will continue to operate, even as a conflict unfolds, as will the need to have information available for sharing with our friends and allies—both before as well as during a crisis.

take the time to call in the analyst, to take the arguments apart and to be relentless questioners. Over time, our leadership will learn more and our analysts will become better. Analysts really do appreciate tough questions from policy makers. Believe me, I have seen this happen directly when I was serving in the Congress. Over time, they will become more responsive to those things that pertain to implementing an effective deterrence strategy. But no improvements will occur if we do not take these steps.

**Build Exquisite Transparency.** In any crises where a deterrence strategy comes under stress, the need for information will become intense. Deterrence will continue to operate, even as a conflict unfolds, as will the need to have information available for sharing with our friends and allies—both before as well as during a crisis. Satisfying this thirst for information will require exquisite transparency—having the means to understand what is happening in space and then to be able to share it and explain it quickly and completely. Often this is referred to as space situational awareness (SSA), but SSA is but one aspect of transparency.

Policy leaders will demand information that can be used with Congress as well as allies. There will be a call to release as much technical information as possible to describe what happened, to explain to Congress and the American people why this is important, to talk with trusted friends and allies.

There will be a need to brief governments as quickly as possible—we want governments to understand our position and be on our side from the beginning. For example, early on in the wargame we faced a kind of “mini-crisis” in space, in which an attack on a satellite (not ours) occurred. I consulted with my player-cabinet officers and we determined that in order to deal with the situation a number of key questions had to be posed to our analysts. Here is a sample list:

1. How do you know what happened and how do you assess your confidence in understanding what happened?
2. What alternative explanations are possible and what is your confidence that these alternatives can be ruled out?
3. How much does the attacked country know about the event? How confident are they about their knowledge?
4. What does the attacker know about the outcome? If this is a one-off attack, what was the intent of the attacker? How do we know it was not a miscalculation?
5. Why should I care about this? What steps or actions would make the situation worse (possibly leading to more attacks)?
6. What is the global reaction to the attack? How much is known publicly? How much privately? By who? What are the trends in the reaction?
7. What are the allies’ reactions? How are they interpreting the event? Is this seen as an economic issue, a political statement, or a military issue?
8. How much debris has been created? At what point will this problem impact our own space access?
9. What services have been disrupted and how could these services be replaced or substituted? How quickly could this be done?
10. Who uses similar space capabilities? Who owns and operates these capabilities? How could these suppliers be enlisted to replace the capability?

Many of these questions were posed, not just because we needed to plan to counter potential future actions, but because we needed the information to explain our position to our friends and coalition partners. You see, we will not be able to manage a crisis in space by ourselves. A good deterrence strategy presupposes that we will have our allies with us from the start. And that will not happen if we do not have a plan for conveying the details of a space crisis to them quickly and completely.

Of course the questions I listed are difficult to answer. They would become more difficult when time is short and would be virtually impossible to answer if we lack the means to collect the information. So we must be willing to invest in substantial improvements in the means to identify and determine the status of space operations. Under funding, or, an unstable baseline will not meet these critical needs.

Exquisite transparency in space operations must be defined in specific terms, however. Understanding the space-related actions (launches, orbital adjusts, de-orbits, deactivation, and more) of space-faring entities, and the space environment (including debris) are all elements of what we need to know. Improvements in our knowledge and willingness to share it would lead to greater stability because all parties could potentially know what is happening or what is about to happen. In times of peace, this knowledge would contribute to a greater confidence that we can distinguish between normal operations in space and those that could be the beginning of a threat.

Achieving the capability to determine what is happening with the requisite level of precision is not so simple. We need to understand what kinds of SSA data would best contribute to the stability of the space domain and how we can best share this information. We need to identify the types of data, uncertainty ranges, or latencies in data availability that would support this goal. Implementation of a transparency processes (the procedures for the actual sharing of information) will also be a complex undertaking. How much detail should be collected and shared? How quickly? Who should do the collecting? Under whose auspices? How will it be validated?

We would also need to consider economic arguments for transparency. Can transparency be promoted for economic benefit? What circumstances could arise where sharing of information would undercut particular commercial interests?
With the right degree of SSA and the right processes in place, we would have a chance to answer some of the questions a president would need to have answered in a space crisis. But we will also need to have the policy support apparatus in place to act upon this information in a timely manner. This brings me to the last practical recommendation:

**Promote Policy Stewardship.** This is the most critical of my three recommendations. Our government must make a sustained, properly organized, and appropriately funded initiative to ensure that we have the policy tools in place to actually deal with a space crisis before it becomes a crisis. And in the event deterrence fails, we must have skilled and experienced policy makers who can understand, promptly deal with, and hopefully contain a crisis involving space systems. Policy preparations will be vital because a war in space could start and escalate globally in the time it takes to hold a single meeting of the president’s National Security Council. There will be little time for debate and analysis of policy options.

The importance of policy stewardship can be understood by looking at the history of past attempts to develop a deterrent strategy.

In 1945, General Hap Arnold was given responsibility for standing up the US Air Force. Among his many challenges was to consider how to deal with a new strategic mission that involved the complex technologies of ballistic missiles, nuclear weapons, and computers. To figure this out, he called in experts from around the country, many of them who had previously served in the strategic bombing survey. This effort took considerable time and resources to mature. From 1945 to well into the 1970s, deterrent concepts were developed and debated. While some aspects were closely held, approaches to deterrence were hotly debated in the newspapers, journals, and at academic institutions and think tanks. Leaders in and out of government became well known for their contributions to these debates: Albert Wohlstetter, Thomas Schelling, Bernard Brodie, Herman Kahn, Jim Schlesinger, Andrew Marshall, to name a few. The public became educated and a general consensus grew up on how to best posture our nuclear deterrent forces. Weapons systems were designed and deployed to maximize their deterrent effect. None of this came easily, but with a sustained commitment came progress and results.

Today, we need to have such a national discussion on protecting our space assets. Indeed, we should have a global debate. We need to ask ourselves if we really want to rely on a code of good conduct for avoiding space incidents and, if an adversary decides to jettison the “code of conduct” (e.g., cross a red line), can we expect that avoidance measures and replenishment strategies will mitigate the consequences of an attack on space assets. This strikes me as necessary but not sufficient to protect assets that are vital to our national security and way of life. An effective deterrent strategy would include three more elements: a clear message to any opponent that attacks would not have the effect they seek, that they would pay a very high—an unacceptably high—cost for embarking on such a course of action, and a recognition by all sides that this strategy would be supported by the community of space-faring nations.

Good policy stewardship of a strategy to deter attacks on space systems will require a lot of effort. It will entail both a deep understanding of any opponents’ views of how war might come to space and a commitment to respond decisively if we come under attack. Among the tasks that our policy makers must contemplate are these:

1. Sponsoring a review and study of deterrence issues as applied to space and cyber.

2. Making sure that our plans for information sharing with respect to space are robust and compatible with the needs of our friends and coalition partners.

3. That there is a policy process in place to continuously assess whether a major crisis might escalate into space and to provide direct, operational support—including options and implications—in the event a crisis is approaching such a tipping point (think about the ten questions I posed earlier and the short timelines in which to act).

4. That we have a plan for war-ending which is designed to be consistent with our needs for space and preserving our way of life and our institutions.

Right now, none of these policy components are in place. Until they are, we will be exposing our military and our economy to an unacceptable degree of risk.

To close this window of vulnerability for our space assets we must first set about to frame a national debate on space deterrence strategy. How should this be done? Some would argue that the US should lead an international debate about how to craft a control regime in space that serves its national security interests and the broader interests of the international community. I am skeptical that considering a control regime with such a broad mandate would be in the interests of the US, especially in the absence of a clearly understood and articulated deterrent strategy. I do think that getting an international agreement on ways to remove space debris that interferes with free access to space is a good first step toward fostering wider national and global interest in space protection. Beyond that, I would call upon the private sector, particularly think tanks with a focus on national security and aerospace firms to take the following steps:

1. Promote the establishment of a private organization to analyze and explain this issue to members of Congress and to the public at large—a Committee on the Present Danger in Space.

---

*Our government must make a sustained, properly organized, and appropriately funded initiative to ensure that we have the policy tools in place to actually deal with a space crisis before it becomes a crisis.*
The decline of future investment and innovation would be most harmful in that it would lead to a strategy of merely defending the status quo in space, of trying to keep and defend the capabilities we have, while other nations build up their own space capabilities.

2. Encourage space communications companies and aerospace firms to develop policies and procedures for protecting their assets in the event of future crises. These procedures, developed in collaboration with the Departments of Defense and Homeland Security, should encompass space assets owned and operated by our friends and allies.

3. Develop and implement a broadly based education effort to debate the need for a space deterrent strategy and to promote the public’s understanding of our reliance on space for day-to-day activities and the fragility of these capabilities in wartime.

One Final Observation

Looking back over time, the US achieved its position in space through sustained investment and innovation. From being first to the Moon; to the Space Shuttle; intelligence, surveillance, reconnaissance; global navigation; the space station; planetary exploration—all of these achievements represented substantial commitment of national resources and talent and led to global recognition and acceptance that the US had leadership in the space domain.

The future of the US continues to be bound up with space. The decline of future investment and innovation would be most harmful in that it would lead to a strategy of merely defending the status quo in space, of trying to keep and defend the capabilities we have, while other nations build up their own space capabilities. Ultimately the US would be seen as losing its leadership in space and perhaps feed the ambition of those who would challenge our capabilities in space. So any strategy for deterring space attacks must be matched with a plan to continue a robust level of investment and innovation in space capabilities for both military and civil missions. Our continued leadership in space inevitably will become a critical element of a deterrent strategy.

Notes:

3. Of course, the same could be said of our cyber systems. In my view, a deterrent strategy that applies to space must also be constructed to apply to cyber capabilities as well, and vice versa. Because Schriever V focused primarily on space, however, the remainder of this article will examine components of a deterrent strategy as applied to space. I will leave for a future article the problems and issues of how to integrate space and cyber into a common deterrent framework.

6. This group ultimately became the RAND Corporation, which was established in 1945.

US Representative Terry Everett (R-Alabama) is a former eight-term Republican congressman from the Second Congressional District of Alabama (1993-2008) and currently is a senior advisor to the Space Protection Program. He served in the US Air Force from 1955-59 as an intelligence specialist. Stateside, he pursued a three decade career in journalism culminating in the ownership of a chain of newspapers in south Alabama. In Congress, Everett has served as Chairman and Ranking Member of the Strategic Forces Subcommittee, House Armed Services Committee, and Ranking Member on the House Permanent Select Committee on Intelligence’s Investigation and Oversight Subcommittee. In 1998, Congressman Everett received the “Excellence in Programmatic Oversight Award” from the House Republican Leadership for his probe into improper burial waivers at Arlington National Cemetery. In 2004, Everett became the first chairman of the newly-created House Armed Services Subcommittee on Strategic Forces. His efforts as chairman focused on improving space acquisition programs and he spearheaded key legislative initiatives in national security space, including: development of a space protection strategy, management of the space cadre and establishment of the Operationally Responsive Space Office. During his tenure as chairman of the Strategic Forces subcommittee, he held frequent hearings and classified briefings on national security space issues, including space control, threats, acquisition challenges, and space policy. Congressman Everett was awarded the Missile Defense Advocacy Alliance for his work in support of missile defense. Also, he was awarded the National Nuclear Security Administration’s (NNSA) Gold Medal from NNSA. Everett retired from the US House in 2008.
**Senior Leader Perspective**

**Employing Elements of National Power in Schriever V**

**VADM Carl V. Mauney, USN**  
**Deputy Commander**  
**US Strategic Command**  
**Offutt AFB, Nebraska**

In March, a team from US Strategic Command (USSTRATCOM) participated in the Schriever V Wargame hosted at Nellis AFB, Nevada by Air Force Space Command (AFSPC). The fifth in a series of AFSPC-sponsored wargames that focus on the space domain, Schriever V explored employment of full-spectrum space operations in the joint and coalition environment, including how to operate through and respond to the loss of space systems we use in support of national security operations. The wargame included a focus on present strategies, policies, and operations and on assessing new concepts and capabilities related to space. Additionally, Schriever V sought to explore potential means for deterring aggression in space and linkages to cyberspace operations.

Schriever V brought together professionals from all parts of the US military, from other government agencies in the US and from among our allies. Besides USSTRATCOM, participants included US Pacific Command, US Northern Command, Office of the Secretary of Defense, each of the services and other key partners such as the Federal Aviation Administration; the Department of State; the National Aeronautics and Space Administration; the Department of Interior; the Department of Treasury; the National Security Council; the director of national intelligence, and staff from several congressional committees.

USSTRATCOM is one of 10 unified combatant commands (COCOMs) and is unique in that its missions are global in nature—with particular regard to conducting military operations across borders or boundaries in meeting assigned objectives and supporting other COCOMs for deterrence, space, and cyberspace operations. Besides executing operations day to day in our main lines of operation—deterrence, space, and cyberspace—we also help to close gaps, operate across seams, facilitate planning, and foster joint capability development in missile defense, intelligence, surveillance, and reconnaissance, information operations, and in planning to combat weapons of mass destruction.

We like to say that we endeavor to “provide global security for America”—a complex challenge in a world where continuing changes in the global security environment, interaction among economies, and the availability of information and new technologies all serve as catalysts in driving the transformation of how we think about and maintain our nation’s security.

The Schriever V Wargame culminated over two years of planning, preparatory work and discrete stage setting events led by a superb team at AFSPC, supported by USSTRATCOM and including the wide set of space stakeholders. Each preparatory event focused on a different aspect of the national security space arena and served to bring key issues into clearer focus for the final wargame. Because of the depth and breadth of the preparatory work and the experience of the attendees, the wargame was an excellent venue in which we considered strategic and operational questions related to space operations and space protection in an increasingly crowded and potentially contested domain. Further, Schriever V added substantially to the foundation of work that has been done in other venues to better understand the roles of deterrence and cyberspace operations in the space domain. In looking beyond a pure military response to the postulated scenario, participants worked through and matured understanding about employing a whole-of-government approach to crisis management and to the postulated conflict to optimally bring all elements of national power to bear in a synchronized manner.

Schriever V additionally included clear objectives that generated focus and actions across a wide range of activities. These efforts included operational synchronization between supporting and supported combatant commanders, political and diplomatic efforts to limit the crisis and control escalation and finally, coordinated employment of commercial space systems. This integrated approach considered traditional interactions between US military and interagency organizations, but also facilitated crosstalks with the US space industry, allied governments and militaries, and the global commercial space sector at large. Diplomatic and military responses, as informed by suggested commercial actions, were developed throughout the wargame. The examination of the nexus of military, the rest of the government, and commercial space capabilities revealed insights into strengths and weaknesses of the present organizational construct in preparing responses to the postulated crisis.

The scenario included operations that crossed several COCOM regional boundary lines. In considering the space domain and the global nature of space operations, Schriever V challenged the ability of the COCOMs to align operational pri-

---

**The examination of the nexus of military, the rest of the government, and commercial space capabilities revealed insights into strengths and weaknesses of the present organizational construct in preparing responses to the postulated crisis.**

---

High Frontier
orities and objectives in order to best employ our high demand and low density capabilities.

During wargame execution, the ability for commanders to communicate in real time and to align information and decision flow between COCOMs and among relevant cells in the planning process was essential to synchronizing efforts to advance diplomacy, meet military objectives, apply scarce resources to the optimum axis, and react to belligerent actions. Clear command and control alignments, identification of supported and supporting relationships between commanders, and establishing personal contact at senior levels facilitated trust and confidence between commanders, and were vital to achieving effective application of combat power to achieve objectives.

We know that in the 21st century, we will continue to place emphasis on operations that are conducted in space or through space to assure our global information needs are met and for maintaining the security of our nation and that of our allies. We must continue to diversify our lines of communication and our space capabilities to prevent dependences on these capabilities from becoming vulnerabilities that others could exploit to preclude our success or threaten our security in the future.

Today, space capabilities are more than conveniences, they are fundamental to many aspects of modern life—from a military perspective as well as from commercial and civil perspectives. We use space-based capabilities to deter and prevent major war and, if deterrence fails, we will want to use our space systems in concert with a broad range of maritime, land, air, and cyberspace capabilities to help win our nation’s wars. Like conflicts that occur in other domains, the response to aggression in space and ultimate victory will not be brought about solely by military action.

For several years, we have been discussing within the Department of Defense (DoD) the need for a more robust approach to developing inter-agency solutions to the complex challenges we face in a globally-connected world. To realize our goals, the military must continue to participate in and indeed work to strengthen the collaborative partnership with inter-agency and allied stakeholders.

The DoD, the Department of State, and our other inter-agency partners along with our coalition partners must have constancy in our understanding of the security environment and must identify our common security objectives. Given the existing methods of safeguarding space information and capabilities, work needs to be done to develop the means to share relevant information in a time sensitive manner.

When faced with a terrestrial crisis where a space asset was attacked, the Schriever V interagency planning group identified and recommended specific actions via a holistic, whole-of-government approach to work toward conflict resolution. Options included employing diplomatic actions—bilaterally and at the United Nations—to:

- Reduce civil space cooperation with the offending state
- Increase civil space cooperation with the attacked state
- Employ economic sanctions
- Employ an information campaign to highlight the long-term impact of the offending states’ actions.

One of the strengths of the response options produced by the player cells was increased integration between DoD, the intelligence community, the US interagency and allied group that enabled synchronized actions by the key stakeholders in our national space enterprise. Blue actions appeared to gain effectiveness when conducted within the whole-of-government/nation(s) construct. When hostilities were imminent or had occurred, the diplomatic, economic, and information actions continued in parallel with military operations and were assessed as contributing significantly to conflict resolution.

Follow-on diplomatic actions included consultations with allies, coordination with neutral parties, and demarches/sanctions against belligerents. Economic actions, taken by industry, rather than government, communicated how hostile actions would negatively impact world markets. Throughout the wargame, an integrated strategic communications campaign produced consistent messages supporting coalition military and non-

![Figure 1. General C. Robert Kehler, commander of Air Force Space Command, discussing policy implementation during a senior leadership seminar at the National Reconnaissance Office in Washington DC.](image)
Among combatant commanders, the global nature of space capabilities dictates a robust method of sharing operational perspectives and developing mechanisms that will rapidly sort resources according to an agreed upon and continuously evolving set of priorities.

military actions, working to solidify international and civil support.

As one would expect, getting to this whole-of-government, use of national power approach to the conflict was challenging. The varied processes and diverse lexicons of all the players made quick communications and shared understanding of what to do difficult and time-consuming. The Schriever V Quick Look report pointed out that once these processes and lexicons were aligned, they formed “a powerful capability to bring synchronized national power to the fight.”

Particular Schriever V insights that may facilitate employment of all elements of national power effectively during a future conflict included:

1. Institutionalize the effective combination of diplomatic, economic, military, and information activities as a powerful formula for success.
2. Among combatant commanders, the global nature of space capabilities dictates a robust method of sharing operational perspectives and developing mechanisms that will rapidly sort resources according to an agreed upon and continuously evolving set of priorities.
3. Pre-planning and regular communications between the military and other agencies must occur with respect to actions needed to support military plans as well as diplomacy and other activities.
4. Organizational processes to facilitate interagency coordination and regular exercises will ensure that the implementation of developed plans can occur when needed.
5. By bringing allies and friendly space-faring nations into the process early, we can substantially broaden our capabilities.

The Schriever V Wargame provided an excellent opportunity to explore, at an advanced level, full-spectrum joint and coalition space operations in crisis and conflict. The robust scenario, coupled with relevant strategic objectives and an impressive array of participants across the spectrum of military, policy, and diplomacy arenas resulted in unique and high value insights that are already being employed in the 2010 Space Posture Review and in a multitude of other space venues. We will look to the further evolution of our space operating concepts and capabilities with the next Schriever Wargame in 2010.

Figure 2. Combined Air Operations Center-Nellis Game Floor. USSTRATCOM Cell participants work through a wargame vignette.
**Senior Leader Perspective**

**Schriever V Wargame: The Boundaries of Space and Cyberspace**

Lt Gen Larry D. James, USAF  
Commander, 14th Air Force  
Vandenberg AFB, California

The year is 2019. The US, along with its allies, is engaged in a regional conflict in which space and cyber capabilities are attacked and denied across many parts of the battlespace. This is the scenario for Air Force Space Command’s (AFSPC’s) Schriever V Wargame. Created as a biannual wargame in 2001, the 2009 execution of Schriever V focused on the strategic level, bringing in all elements of national and coalition power to execute operations and meet national objectives. Specifically for this year, the objectives were:

- Examine national policy implementation measures to enhance decision making in a contested space environment
- Explore ways the US could operate with commercial providers, allies, and coalition partners to assure space capabilities
- Investigate organizational relationships to improve space operations in a coalition environment
- Explore space capability requirements and force structure alternatives needed to expand multi-theater and homeland defense space support
- Test the effectiveness of alternative force postures, operational concepts, and operational plans against possible adversary courses of action.

In the execution of operations during Schriever V, there were several key lessons that were learned. These focus on space and cyberspace integration, the critical requirement for space situational awareness (SSA), the force multiplying capabilities of coalition partners, and the need to integrate commercial space capabilities into our overall operations.

### Intersections and Integration of Space and Cyberspace

In the operating environment of 2019, space and cyberspace operations are intertwined at multiple levels. Emerging threats may originate anywhere, at anytime, and increasingly take advantage of space and cyberspace domains. Common attributes across both domains include global effects, speed of attack, availability of information, and the ability to strike from remote locations. As such, our adversaries have an unprecedented and immediate access to information utilizing minimal resources. Space and cyberspace are truly contested domains and our nation’s critical information is more valuable than ever. It must be protected. While the cyber domain sphere of influence is much larger than just the space infrastructure, most of the elements of the space infrastructure are tied in some fashion to the cyber domain. Space and cyberspace capabilities continue to shape the world’s approach to warfare. They are embedded in an increasingly diverse arsenal of modern weaponry and are threaded throughout warfighting networks. When integrated, space and cyberspace operations will become an even more powerful force multiplier.

The rapidity of actions in unbounded global domains, as are space and cyber, introduces the concept of warfare at the speed of light. Characteristics of this concept include agile decision cycles, linked warfighting domains (space, cyberspace, and terrestrial), the requirement for established authorities and rules of engagement, and trained personnel who can operate in this speed of light environment. At the operational level, these speed of light strategies will have to be integrated into traditional lines of operation and schemes of maneuver to be truly effective.

During Schriever V, national decision makers needed near real time information to make appropriate decisions. However, in a contested space and cyber environment, this information can be difficult to obtain. Being able to attribute actions, know points of origin, and understand the redlines and triggers of an opposing force present significant challenges when the battlespace is 130 to 24,000 miles away in space or in the cyber realm. In addition, space and cyber capabilities boundaries cross the “whole-of-government.” Integrating knowledge and creating an effective response in this environment is a challenge.

Schriever V 2009 was the first attempt to bring cyber play to the wargame. The results clearly showed that in the operating environment of 2019, space and cyber will be inextricably linked. We must continue to operationalize our cyber capabilities. We must also understand the space/cyber linkages while actively developing effective doctrine, operational concepts, and the tactics, techniques, and procedures to operate in this integrated environment.

### Importance of Space Situational Awareness

SSA is more than just understanding the space environment, tracking objects and conducting conjunction assessments. It is the understanding of the location, status, capabilities, and purpose of man-made objects, and their owner’s intent. The threats presented in Schriever V, utilizing small satellites, micro-satellites, and ground based systems, created a very challenging environment for our SSA capabilities. Being able to accurately track space objects was critical, but the need for near real time intelligence to understand capabilities and intent was just as important. In addition, the game highlighted the need to rapidly integrate and fuse this information in a manner so that it was useful to senior decision makers. Without this complete picture, these decision makers were put at a disadvantage as they sought to define a clear plan of action and develop responses to adversary actions.
The need for integrated SSA capabilities was made clear during Schriever V. This includes a full suite of ground based sensors, ranging from optical to radar, as well as on-orbit capabilities. It also includes the intelligence and assessment capabilities to rapidly integrate and fuse this information to create knowledge that is usable and actionable for decision makers at all levels.

**Coalition Support and Integration**

One of the key components of Schriever V 2009 was the integration of our allies to a level that was unprecedented in past wargames. Coalition partners brought a multitude of capabilities to Schriever V operations, both space- and ground-based. Operating as a coalition inherently strengthens our abilities in this realm. This was evident as the US lost capability during the course of the game. Coalition partners could backstop and fill the gaps in many instances. As the game evolved, it became apparent that an integrated assessment and tasking mechanism was required. This resulted in the creation of the Coalition Space Operations Center (CSpOC). With appropriate caveats, each nation represented allowed their systems to be managed and tasked by one operations command and control entity—the CSpOC. This allowed unity of effort and rapid response, creating combined effects and capabilities that would not have been possible with each country operating independently.

Again, when warfare is at the speed of light, a CSpOC-like capability is essential. There is an absolute need to continue to explore how to operationalize a CSpOC construct to effectively manage coalition/US space capabilities. With the participation of coalition partners in Schriever V, it was widely recognized that formal agreements between coalition partners must be aggressively pursued to meet our common interests in order to combat our common threat.

**Integration of Commercial Capabilities in Our Operations and the CSpOC**

The DoD has a sound relationship with commercial space operators, particularly those commercial communication and remote imaging organizations that support US and national security activities. Despite our efforts and the milestones reached, we continue to face challenges. The DoD space community is in continuous pursuit of increasing the availability, timeliness, and accuracy of SSA data while protecting sensitive information. The DoD has engaged with most of the major commercial satellite operators who provide support to the US government to discuss their needs for SSA, our challenges, and their ability to provide inputs to our SSA.

During Schriever V, the utilization of commercial systems was important in maintaining coalition capabilities as coalition assets were degraded or denied. However, we did not have mechanisms allowing the coalition to make best use of commercial assets. In addition, the adversary recognized the value of commercial assets and effectively utilized them for their own purposes. The results clearly showed the need to develop better concept of operations for integrating commercial capabilities and to have “on the shelf” plans and agreements that allow this utilization during heightened tensions and hostilities. It also reconfirmed the need to better manage commercial satellite communication capabilities and how we procure these services. Additionally, both coalition and commercial representatives agreed that having a commercial service representative in the CSpOC would be highly useful. Sorting out how that can be implemented is one of the key actions out of Schriever V.

**Conclusion**

Schriever V was a watershed event that clearly identified critical areas requiring action from the space and cyber communities as we continue to build and improve capabilities in both domains. Warfare at the speed of light, integrated across the space and cyber domains, requires new constructs, operational concepts, and capabilities. Rapid and accurate intelligence, coupled with fused situational awareness, is key to providing decision quality information to our senior leaders. The power of the coalition was clearly seen, as well as the need to better integrate commercial providers in our planning and operational concepts.

Fourteenth Air Force and the Joint Forces Component Commander-Space will work closely with AFSPC and US Strategic Command to take the lessons learned from Schriever V and turn them into reality, ensuring our freedom of action in space as we move into this challenging future.

---

**Lt Gen Larry D. James**

**BS, Astronautical Engineering, USAFA; MS, Astronautical Engineering, MIT** is commander, 14th Air Force (Air Forces Strategic), Air Force Space Command (AFSPC), and commander, Joint Functional Component Command for Space (JFCC SPACE), US Strategic Command (USSTRACOM), Vandenberg AFB, California. As the US Air Force’s operational space component to USSTRATCOM, General James leads more than 20,500 personnel responsible for providing missile warning, space superiority, space situational awareness, satellite operations, space launch, and range operations. As commander, JFCC SPACE, he directs all assigned and attached USSTRATCOM space forces providing tailored, responsive, local and global space effects in support of national, USSTRATCOM, and combatant commander objectives.

General James’ career has spanned a wide variety of operations and acquisition assignments, including space shuttle payload specialist, Air Staff program element monitor, GPS satellite program manager and chief of operations, 14th Air Force.

General James has commanded at the squadron, group, and wing levels, and was vice commander of the Space and Missile Systems Center. He has served on the staffs of Headquarters US Air Force, US Space Command and AFSPC. He also served as the senior space officer for Operation Iraqi Freedom at Prince Sultan AB, Saudi Arabia. Prior to his current assignment, the general was vice commander, 5th Air Force, and deputy commander, 13th Air Force, Yokota AB, Japan.
Senior Leader Perspective

Schriever V – A UK Perspective

AVM T. M. “Timo” Anderson, RAF
Assistant Chief of the Air Staff
Whitehall, United Kingdom

On the day in 2007 that I took over as the Royal Air Force’s (RAF’s) assistant chief of the Air Staff, I flew to Nellis AFB, Nevada to lead the United Kingdom (UK) team at the Schriever IV Wargame. Readers who participated in Schriever IV may recall cussing the ally who inserted a large wrench into the smooth-running game, so I was both surprised and delighted to be invited to return in March 2009 for Schriever V. This time, I brought with me an 18-strong UK team of quality individuals who participated in all aspects of the wargame. Having briefed them all before departure about the strengths and success of Schriever IV, they all eagerly anticipated learning from and contributing to this signature space wargame—they were not disappointed.

After the event, General C. Robert Kehler invited me to comment on one of the key components (military, political, diplomatic, or economic influences) of the wargame. In thinking about how to address this, I found it very difficult to consider these influences separately; an action in one component will inevitably have implications and effects in some or all of the other components. Indeed, this fact lies at the heart of what we Brits call the “comprehensive approach” to crisis resolution. But coordinating and managing actions across this spectrum of ‘comprehensive’ activity is a hugely complex task and one that made significantly more so by the inclusion of the ‘coalition factor.’ Therefore, in this article I aim to reflect and offer observations on the ‘coalition’ aspects of the wargame, set against the context of the key components General Kehler has identified.

Coalition Integration

General Kehler and the game designers went to immense lengths to ensure that the non-US players were fully integrated into all aspects of the wargame. Even so, from my vantage point I perceived that some of the players, on all sides, still started the wargame with a mindset that there were two elements to the blue team: the US on the one side and ‘the allies’ on the other. Refreshingly, early on in the wargame, I sensed a groundswell of opinion that this approach was no longer preferable, nor tenable; that the term ‘the allies’ more properly described all the nations working collectively towards a common goal, with the whole indisputably greater than the sum of the constituent parts. And by the end of the wargame, the blue team was much closer to a properly integrated coalition making best use of all nations’ capabilities.

But even in the most integrated coalition, there must be unity of command, good leadership, and good followership. That the differences in allies’ cultures, capabilities, and governance structures need to be recognized and accommodated is self-evident and essential, but a team is not a team if everyone thinks they are the captain. Not that the concept of subordinating one’s actions, and perhaps even one’s objectives, to a higher purpose is in any way a novel concept. Many countries, including the US, are well used to providing forces to be employed by a commander from another nation. In the maritime, land, and air environments this is commonplace and has been for many years. We only have to look at recent operations in many theatres to see that equipping coalition commanders with operational control/tactical control (TOC) of assigned forces from other nations can work well. So, should space be any different? Joint Publication 3-14 states that:

Commander, US Strategic Command [CDRUSSTRATCOM] integrates and synchronizes Department of Defense [DoD] space capabilities to ensure the most effective use of these resources. US Strategic Command [USSTRATCOM] must be able to quickly plan, direct, coordinate, and control space assets and forces for daily operations, for crisis action planning, and in the event of war against the US and/or its allies.

Thus, there is already a single commander for US DoD space capabilities—born, I would presume to suggest, out of the experience that having multiple commanders of elements of US space capabilities was not an efficient construct. Furthermore, I would argue that this decision to bring all DoD space capabilities under a single commander has direct relevance for any space alliance or coalition. Surely any inefficiencies that competing services brought to the DoD space fight in the past would only be magnified if, or when, different nations bring their space capabilities to a multinational space fight?

I think we all saw at Schriever V that a possible way to maximise the efficiencies of coalition space operations would be to create a Combined Joint Task Force-Space (CJTF-Space) to “integrate and synchronize” all the coalition partners’ space capabilities. Such a CJTF-Space would provide the framework for nations to apportion forces to a single commander in support of a common aim, with the result that the harmonizing of complementary capabilities and resources would deliver maximum effect and build in much needed resilience. So, might we create a standing CJTF-Space today, or can we wait for an increase in tension, or a specific trigger event, and then create a CJTF-Space? It should be obvious that a standing CJTF-Space would enable us to respond to a crisis in space more rapidly and effectively than if we tried to invent procedures on the fly—indeed, given the potential pace and scale of events, threats and opportunities that Schriever V illuminated to us, it is perhaps hard to see how we would respond effectively and in a timely fashion to an international crisis without such a construct to help ease the path.

A standing CJTF-Space would allow like-minded nations to practice what we theorized about at Schriever V. As always, the devil would be in the details—who should command; how
We have to find the right answer that would allow us to transition seamlessly from peace to war; ‘train as you would fight’ is a maxim we forget at our peril.

would the command and control structure work; and what forces would be assigned and under what national caveats, and so forth—but we are not necessarily starting from a clean sheet of paper. The model of the joint force air component commander operating through a combined air operations center is mature and well practiced and, of course, in the US the commander of the Joint Functional Component Command for Space (JFCC SPACE) and Joint Space Operations Center (JSpOC) construct is proving to be very effective. I therefore believe that the ‘who should command’ question is simply answered. Whatever the is proving to be very effective. I therefore believe that the ‘who should command’ question is simply answered. Whatever the nature of any future coalition in space, it is probable that the US would provide the bulk of the space capabilities and would therefore likely provide the commander CJTF-Space. It seems to me to make sense that commander JFCC SPACE should be one and the same person.

Clearly, a commander CJTF-Space would need somewhere to command from and a staff to plan and help him/her execute his/her mission. So, in my vision of the future, what might commander CJTF-Space’s operations center look like? Commander JFCC SPACE already generates and operates the JSpOC, wherein exchange officers from Australia, Canada, and the UK are increasingly closely integrated. Were commander JFCC SPACE to be triple-hatted, the JSpOC could possibly form the core of commander CJTF-Space’s operations center. But as we enter an age of ever more distributed operations, is there a pressing need for geographical co-location, or could it be a virtual entity incorporating links to all the allies’ space operations centers? Might its virtual structure even be tailored in response to the defense readiness condition? Moreover, space is not just the preserve of departments of defense and ministries of defense. The intelligence communities, civil space operators, and commercial space operators are also very significant players in space and critical components of any cross-government(s) approach to a crisis. Should we incorporate these elements into the CJTF-Space construct—and, if so, how? Well, I believe the answer to the first part of this can only be yes, but how would we maintain national and commercial security within this multi-national, multi-agency construct? This is an area that will require much work and there are no clear answers yet. What is clear; however, is that only by joining these disparate elements will we be able to bring truly synchronized and effective international power to bear on the crises of the future. We have to find the right answer that would allow us to transition seamlessly from peace to war; ‘train as you would fight’ is a maxim we forget at our peril.

Day-to-day, should nations provide forces TACON to a commander CJTF-Space? Certainly the procedures would have to be regularly exercised, if only to answer basic questions such as ‘how do you apportion a space asset?’ With maritime, land, or air forces, it is usually easy to pass TACON to another commander for a period of time; in space would that work, or would we need to apportion based on geography, or on-board capacity, or on an agreed priority list—or some combination of the above? I would argue that answers to questions such as these would be even less easy to determine in the heat of a conflict; far better surely to address them now by trialling a standing CJTF-Space.

Complicating any suggestion of a future standing CJTF-Space operations center are the contemporary constraints that ‘releasability’ and ‘interoperability’ of information technology (IT) place upon us. At Schriever V we luxuriated in an environment where all the information was ‘releasable,’ provided that individuals had the appropriate clearances. Additionally, the IT systems allowed true multi-national collaboration. Nevertheless, readers who have worked previously alongside other nations’ personnel will understand that ‘releasability,’ and the associated difficulties of sharing information electronically, do significantly hamper multi-national operations. We should not underestimate, therefore, the difficulties we will face translating the idealized environment we experienced at Schriever V into the real world! But translate it we must if a future standing CJTF-Space operations centre is to be a feasible concept. A potential vision of the art of the possible is the JSpOC Version 3 that has been developed by Applied Minds, Inc. Their demonstrated capabilities certainly seem to be able to integrate multiple locations and multiple security levels into a seamless, virtual, whole. So, where there’s a will there may be a way.

Space Council

During Schriever V, I felt truly privileged to be able to work alongside a raft of highly able, intelligent, and far thinking experts in the Schriever V Space Council who represented a broad spectrum of the US administration and legislature and, indeed, our Australian and Canadian allies. But what the space council dimension of the wargame demonstrated most to me was that collectively, inter and even intra-governments, we lack a suitable peacetime construct for common and integrated space policy and legal development, even in areas that are clearly of mutual interest. It is obviously vital in any coalition operation to understand where our policies and legal opinions are aligned—and, even more importantly, where they are not. The time to determine these areas of agreement and potential difference is now, not when a crisis is looming, or worse, breaking over us. When the crisis does occur, there is likely to be an acute need for rapid decision-making that can meet the response times demanded by operations in space. Here, again, the benefits of a standing CJTF-Space seem clear to me. A commander CJTF-Space would intuitively understand his/her mission and constraints, having had the benefit of close visibility of the peacetime policy and legal work that would underpin them both. Partners would have enhanced confidence in chopping assets TACON, assured that the essential mutual understanding
of each others’ political objectives and constraints was in place to enable commander CJTF-Space to employ assigned assets to maximum effect—and with minimum friction or interference!

Not that the Schriever V Space Council was a panacea that fixed, or was capable of fixing, all national concerns—but the concept was an excellent start. However, I believe we would be failing ourselves, and our respective nations, if we arrived at Schriever 10 (SW 10) without having made some tangible progress in translating the ‘space council’ concept into the real world. I suggest that, at the minimum, we must agree in the interim what we are trying to achieve and set about constructing a roadmap to get there. In this regard, I see real value in the extant bilateral Space Cooperation Forums coming together in some manner, even if only periodically, to form an Allied Space Cooperation Forum within which objectives could be expressed and such a roadmap developed.

Way Forward

Unquestionably, a common understanding of the relevant political, legal, and military positions and capabilities is essential before any of us commit to coalition actions in space. Equally unquestionably, in my view, the time to develop this common understanding is now—not when we are faced with reacting to events in space. If not a recipe for failure, reacting to opponents’ maneuvers will surely limit our effectiveness and put success at risk—in such a fast moving and strategically vital domain as space, we must collectively act proactively, responsibly and highly responsive, if we are to stand any chance of achieving our security aims effectively, efficiently, and at least cost. A ‘space council’ and a CJTF-Space should be our common goals and, personally, I would hope to see formal movement on both before SW 10.

Throughout this article, I have of course been focussing on the space domain. In recent years, humans have constructed another domain that labours under the name of cyberspace. Space professionals reading this fully understand that swift decisions are required to operate and fight in the space domain—but even these decisions could be considered pedestrian when looking at warfare at, literally, the speed of light. For SW 10 to incorporate cyber will therefore be a massive challenge—but a necessary one from which we must not shrink. The Royal Air Force has just completed its own future air and space wargame, very ably and generously supported by our US Air Force colleagues. The most immediate impression I have of our own work in this area is that if we thought the ‘comprehensive,’ or whole-of-government, approach is highly complex and demanding today, it is likely to be completely overshadowed by the complexities of joint, combined and integrated operations in the cyber domain. It may be, therefore, that the sorts of actions I am promoting above may not just be a way of better facilitating actions in and through space, but a necessary precursor to the even greater challenges to come. One thing is for sure though, if General Kehler and the US Air Force will have us back, the RAF stands ready to contribute to the development and execution of SW 10, the operationalizing of coherent coalition space activities and strengthening the foundation from which we can all Fly, Fight, and Win … in Air, Space, and Cyberspace!

Notes:
1 Assistant chief of the Air Staff is a similar role to that of vice chief of staff of the US Air Force.
2 Joint Publication 3-14, Space Operations, 6 January 2009, xii.
3 Commander JFCC SPACE is already dual-hatted as commander 14th Air Force; command of a standing CJTF-Space would thus add a third hat.

AVM ‘Timo’ Anderson is a fighter ground attack pilot by background and commenced his flying career in 1983 operating the Tornado GR1. Successful tours on front-line squadrons, including with the Royal Australian Air Force flying the General Dynamics F111C, provided the early backdrop for several operational deployments. Following a senior staff tour in the Ministry of Defence (MoD), in early 1999 he assumed command of No 14 Squadron. Shortly after his arrival to the squadron, he was charged with leading the Royal Air Force’s (RAF’s) Tornado GR1 squadrons committed to NATO’s Operation Allied Force in the Former Republic of Yugoslavia and was appointed a Companion of the Distinguished Service Order as a result of his efforts in this regard. In 2000, he was promoted group captain and was granted command of RAF Brüggen in Germany, at the time home to the largest Tornado wing in NATO. He was promoted to air commodore and took post as MoD Director Equipment Capability (Deep Target Attack) in September 2003. Having attended the UK’s Higher Command and Staff Course in early 2005, in August that year he assumed the concurrent appointments of commandant of the Royal Air Force Air Warfare Centre, director of the UK’s Defence Electronic Warfare Centre and assistant chief of staff for intelligence at HQ RAF Strike Command. He was promoted to air vice-marshal and appointed as the assistant chief of the Air Staff in March 2007. He is a member of the Air Force Board and Head of the Service’s Operations Support Branch. His primary responsibilities range across the development of the RAF’s strategy, acting as the RAF’s designated ‘User’ in the MoD’s Through Life Capability Management process and leading the service’s engagement in the department’s annual financial planning rounds. He is the Release to Service Authority for all RAF aircraft and is chairman of the MoD’s Military Aviation Regulation and Safety Board. A non-executive director of the Civil Aviation Authority Board, he is also the MoD Senior Responsible Owner for both Space and UA Vs. He is president of RAF Rugby Union, president of the Northern Ireland Wing of the Air Training Corps, and vice-president of the No 14 Squadron Association.
Senior Leader Perspective

A Space Doctrine for Soldier, Scientist, and Citizen: What It Will Take to Secure the Space Domain

Ambassador Lincoln P. Bloomfield, Jr.
Chairman, The Henry L. Stimson Center
Washington, DC

Introduction: From the Iron Age to the Info Age in Ten Short Years

A decade ago, the dot-com revolution was in full swing, signaling the arrival of the 21st century, the end of the industrial age, and a growing reliance on information technology. The Pentagon, although busy addressing security challenges in Rwanda, the Balkans, the Taiwan Straits, Haiti, and elsewhere, was nevertheless living more frugally under post-Cold War budgets. President Bill Clinton claimed a ‘peace dividend’ after the fall of the Soviet Union. Vice President Al Gore promoted greater use by Department of Defense (DoD) of commercial off-the-shelf (COTS) products to avoid, where practicable, the long lead-times and high unit costs of items built to military specifications.

The US defense establishment energetically embraced the information technology revolution, and the military enhanced the performance of military specifications weapons and infrastructure with COTS equipment and services to achieve advances in intelligence, command and control, precision targeting, logistics management, and many other areas. Information carried on satellites—whether dedicated US government satellites or capacity contracted from commercial satellite providers—became a major enabler of US military operations. Policy and doctrine in the late 1990s began explicitly to acknowledge the importance, and vulnerability, of military equities in space.

With the initiation of post-9/11 operations in Afghanistan and Iraq, space-enabled military operations reached a new level of robust real time connectivity across long distances. Where 10 years earlier the defense policy concern was that impairment of its access to space communications could cause important but discrete disruptions in military operations, a mere decade later the recognition was already widespread that major functional capabilities in today’s military exist only by virtue of continuous full-fidelity utilization of space.

The Benefits of Wargaming

An astute adversary, observing the quantum improvement in the effectiveness of America’s global information technology-based military operations, and reading in US military journals about the revolution in military affairs and the transformation in warfighting, would naturally look to the informational backbone that made it possible. That backbone runs through space.

Among the earliest signals to the policy community that space was becoming more militarily significant occurred at the first major “Army After Next” wargame in January 1997, a 25-year look-ahead involving several hundred participants and commissioned by Army Chief of Staff, General Dennis Reimer. The “red” adversary team, finding itself hopelessly overmatched, detonated a nuclear device in low Earth orbit, destroying the space infrastructure on which the Army of the future would substantially rely.

The move was invalidated by the control team so as to permit the wargaming concepts in the game design to be tested through several moves. However, the acting US president at that game, then-senior DoD official Richard L. Armitage, in the executive out-brief, compared space to an exquisite crystal goblet, noting that technological infrastructure in space was at once fragile and empowering. In a National Defense Panel Report to the secretary of defense in December 1997, he and his co-panelists wrote, “If we do not control the military utility of space, the advantages we now hold in information operations and more traditional military operations could be put at risk…. [W]e must protect our space assets to include our commercial assets and deny our enemies the opportunity to gain military advantages through the use of space.”

Two seminal space wargames in 1998 and 1999, co-hosted by the Army Space and Missile Defense Command, the National Reconnaissance Office, and what was then US Space Command (prior to being merged with US Strategic Command [USSTRATCOM]) gave the undersigned and a policy “blue” team two rich, albeit artificial, week-long experiences set in the future. Our task as National Command Authority was to manage an escalating conflict and prevail, in a scenario where the US and its principal adversaries had fielded a range of destructive and disruptive space capabilities, and developed a suite of deceptive tactics to go with them.

That experience yielded the important recognition that space conflict featured characteristics that utterly defied the crisis management logic and protocols of past conventional or nuclear confrontation. The absence of warning, immediacy of adverse consequences, and complexity of tactical gameplay all pointed to a different paradigm than participants had ever encountered in the national security realm. Two of us published our insights, believing that these unique national-level policy issues needed

“... [W]e must protect our space assets to include our commercial assets and deny our enemies the opportunity to gain military advantages through the use of space.”

to be examined in detail given that the world was increasingly likely to view the US military’s reliance on space-based assets as a lucrative target in a future war.2

**Schriever V – A Civilian’s Policy Perspective**

As a participant on the US policy team at the Schriever V wargame, held at Nellis AFB, Nevada from 14-20 March 2009, the author was able to take stock of contemporary planning, concepts under development, and key questions of interest to the US Air Force in particular as the military proponent for the space domain. Informed by the gaming experiences of a decade earlier, this observer found that many of the fundamental dynamics perceived at that time regarding the military’s equities in space had been validated in the intervening years. In particular:

- The severe degradation or loss of space-based communications and intelligence would have a major and growing impact on global US capabilities and operations, making the prevention of such an occurrence an ever more urgent priority;
- The speed with which harm could potentially be inflicted upon critical space infrastructure used by the US military places a premium on the ability to know, fast, exactly what is occurring in such a scenario—the capability known as space situational awareness (SSA);
- Related to the very compressed timelines of an attack on US space-based capabilities is the military’s concern that rules of engagement (ROE) permit timely response, a concern that has, from the beginning, led many to posit the necessity of pre-delegated authority to a US commander already conversant with the space environment and the tactical dimensions of hostilities in space.

What Schriever V brought out, from a policy perspective, that had not been as evident in the earlier years of space wargaming, was a greater sensibility about terrestrial interests unrelated to the conflict that could be affected by escalation of hostilities into the space domain. The unfiltered participation of some allied experts brought to the policy discussion a rich appreciation that other governments and their populations have very substantial economic, scientific, and social interests in the uninterrupted benefits enabled by space-based transmission of communications.

Allied players were impressively conversant with norms of international law and policy pertaining to the world’s access to space. Whatever latitude for US action in space American legal advisors may determine to be permissible under the accumulated body of international norms, recent real-world experience has shown that the US will undervalue the views of other countries on issues of war at its peril, particularly when key democratic allies hold contrary views to the US on the necessity, hence legitimacy, of the use of force.

The central focus in Schriever V was not national policy but Air Force business: to examine whether the capabilities it had previously deemed essential proved in a simulated future operation to be useful and relevant to the mission of defending US space assets; to gauge how dependent on space our warfighting capacity has become, by simulating a sudden loss of space-based communications; and to probe the dynamics of an unfolding crisis through several moves to look for what worked well and to identify gaps in the US warfighter’s ability to operate successfully.

It is a core responsibility of the US Air Force Space Command, working with USSTRATCOM and other combatant commands, to ensure that the military is ready, if directed by the president in a future crisis, to provide operational capabilities able to counter potential threats to US interests in space. The Schriever wargaming franchise has proved to be a valuable tool for experimentation, challenging a sizable community of experts to focus on the direction and adequacy of the organizations, capabilities and doctrine aimed at fulfilling that responsibility.

**What a Military Game Will Not Try to Answer**

If there is a risk emanating from a major exercise such as Schriever V, it is the possibility that some in Congress and the national security community at large may conclude that all the truly important national questions about future conflict in space have been touched and dealt with in such an exercise, when the reality is that they have not. This is no shortcoming on the Air Force’s part: indeed, Schriever V stayed very properly within the boundaries of the defense mission.

As with so many well-organized, well-led, well-resourced DoD planning activities, we find there is no parallel civilian planning mechanism for policy and doctrine at the national level—no non-military franchise to focus on the decisions that our elected leaders will face, even though these are the most consequential questions of all. America’s future civilian leaders will face more than military questions should a conflict scenario arise in space—questions appropriately left outside the parameters of the Schriever V exercise. They include:

- Will there ever be a situation in which the US interest is best served by conducting destructive actions against space assets, either to deny capability to an adversary, to deter further conflict escalation, or to retaliate for comparable acts of aggression against the US?
- Is the US intelligence community prepared to estimate, for the president, the potential worldwide collateral impacts of military actions taken to compel an adversary which could result in degrading or eliminating space-based communications for substantial geographic areas of the world?
- Do legal counsels from outside DoD, for example, at the White House, State Department and the Justice Department, have jurisdiction to advise the president on whether and how US military actions in space comport with international treaty obligations and generally-observed norms? And, what weight should be assigned to the views of other countries when the US is considering military options potentially detrimental to the future space environment and the global interests it serves?
- Can the decision to take destructive actions in the space domain be made by anyone other than the president, notwithstanding the forbidding time constraints and daunting (for all but space ‘professionals’) complexity of the space systems environment?
These are among the issues that officials in Washington need to consider and address so as to ensure that prudent military planning will rest on a coherent foundation of national policy and strategy—a foundation that can come only from the president and Congress. Not to provide such a foundation would be a disservice to our military.

To Militarize or Not to Militarize – That is Not the Question

Almost from the start of DoD’s embrace of the information revolution, civilian defense planners and the senior military leadership have warned that military dependence on unimpeded use of space is so critical, and irreversible, as to warrant hardening of space assets and fielding of the capability to defend the space ‘domain.’ During this same time, other constituencies have viewed with mounting concern the prospect that space could become a theater of hostilities, given the physical risks that destructive activities in orbit could pose to satellites and activities supporting scientific inquiry and commerce, including manned space flight. This latter perspective has given voice to calls to keep space from being ‘militarized.’

The conundrum for US policymakers is that both perspectives have a valid point: the US military and its alliance and coalition partners are correct that their operations are highly vulnerable, and their capabilities susceptible to unacceptable degradation, if space communications are disrupted; and the scientific community is no less right that a significant increase of space debris, or other forms of impairment, could be devastating to the peaceful use of space, collateral affecting broad interests worldwide for potentially a very long time.

Has space been militarized? Yes and no. If, by “militarized,” one means that the effective conduct of significant US military operations fundamentally relies on access to and use of space, then space has been militarized for many years. On the other hand, with the exception of the 2007 anti-satellite test by China (followed in February 2008 by the US Navy shootdown of a failed and de-orbiting satellite), space has not been a locus of destructive acts by any state. So, while we are decades past the point that space could be regarded as separate from the national security interest, it remains accessible to all, including precious human and scientific cargoes that must traverse low-earth orbit. While the earth’s exoatmosphere is perhaps not pristine in terms of man-made debris, it remains as yet not devastated by the detritus of space warfare.

There is a divergence of views between the military who stand to lose so much from being targeted in space, and others who fear the deepening military dependence upon space could lead to an arms race in space and, eventually, destructive hostilities in space. Yet the interests of both, far from being divergent, are aligned, indeed inseparable. Both should be able to embrace the proposition that most closely reflects the true situation and the corresponding US interest. That is: the US needs to keep any aggressor from degrading or destroying space assets on which the US military depends, and at the same time it must seek to deter or prevent any erosion to the accessibility and fidelity of the space domain for technological utilization by all of humankind in perpetuity.

The National Interest in Space – Is Military Necessity Always Paramount?

Not just one, but two national interest goals present themselves as the proper object of US policy, doctrine, programs, and actions: preserving the US military’s equities in space, and taking care to preserve the rest of the world’s equities in space, including for future generations. If one were uncertain about the importance of this second goal, the reader is invited to consider what would happen if any party engaged in destructive acts in space.

Consider the implications for satellite manufacturers, insurance companies, the launch industry, and bandwidth providers. Imagine if low Earth orbit became sufficiently congested with debris that satellites were frequently at risk of catastrophic collision with very high-speed objects, or if some other impairment such as electromagnetic pulse in orbit were to inflict permanent damage on space-based electronics. Consider the reaction of governments and their citizens if the International Space Station became unsafe for habitation, and if manned and unmanned space travel alike were deemed too risky to justify the effort and investment. Now consider their perspectives if some of these adverse conditions were expected to persist for a generation, a century, or longer.

The world at large—the scientific community, the globalized private sector including financial markets as well as international traders in goods and services, and millions of ordinary people whose jobs and lifestyles rely upon space-enabled information services—would be justified in feeling that a part of their lives, and indeed their future, had been taken from them. The prestige, respect, and influence won by the country that landed men on the moon and exploratory unmanned missions on Mars would be forfeited if the US were seen to have had a role in so damaging the global economy and denying these scientific and aspirational horizons to others, never mind that the US likely would have acted in self-defense against a very threatening adversary.

The prospect of such a development has given rise to recommendations and proposals for multilateral prohibitions on such destructive acts. Yet, as this is written, neither the US nor countries that might hold at risk its space capabilities appear inclined to adopt common restraints on their freedom of action in space. One reason is that potential adversaries of the US do not appear to be suitably impressed or deterred by a recognition of the profoundly grave effects of hostilities in space. That being so, even the expectation of severe collateral damage that would be global in scope and generational in duration might be deemed a high but necessary price for the US president to prevail in a conflict with a future adversary. Such is the ultimate priority that war imposes on political leaders, and the burden war can impose on civil life.

What the US requires is a security doctrine that sacrifices neither the future of space as a permissive domain nor the ability of the American President to seek leverage and even dominance over an adversary in an escalating crisis. The beginning of wisdom in contemplating this doctrine is to recognize that among
the principal casualties of a destructive conflict in space—regardless of who ‘wins’—will likely be US military space-enabled capabilities. In other words, war in space is almost certainly not the optimal way to secure the national security domain of space.

The Warfighter’s Takeaways from Schriever V, Reexamined

If there is one theme that consistently emerges from the insights of participants in space wargames, it is that timelines for decision and action are radically compressed in comparison to past real-world experience with military conflict. As one senior mentor put it, in a space conflict events unfold at “net speed.”

Because of the physics of space orbit, entire constellations of critically-important space assets orbiting over hostile territory could potentially be destroyed in the time it would take to communicate effectively with the president and key cabinet advisors, and reach a decision on a military response. It is unarguable that with US space assets under attack, rapid action could spell the difference between preserving and losing capability, to say nothing of limiting the destructive consequences of the event. Figure 1 portrays this imperative.

1. Presidential Responsibility. Pre-delegation does not change the fact that the authority to use force is and remains presidential, once delegated. Therefore, any future warplans related to space contingencies are very likely to contain tight rules of engagement and precise ‘withholds’ specifically approved by the incumbent president—not a broad dispensation akin to a traditional executive order governing hostilities in a politically-confined geographic battlespace. As explained below, this is as much to protect military commanders as to satisfy a president’s penchant for control.

2. Presidential Knowledge. The common but unstated assumption is that because there is no time to brief the president on the complexities of defending space, he or she must pass the baton in advance to a knowledgeable military commander. Waiting for a presidential decision, it seems, would be tantamount to ceding the loss of America’s space assets. Yet this problem is not so easily solved. As the author has posited repeatedly in the wargaming arena with scenarios involving potentially severe consequences, a president will not authorize any course of action whose implications he or she does not understand. In other words, either in advance of a military crisis involving space, or at its outset, the president will have to be informed, educated, and advised to a level sufficient to support a decision to use force. Further, it is hard to conceive that once such a decision is taken, the president will not stay intimately engaged in managing the crisis.

3. The Political Dimension of Controlling Escalation. A crisis in space would presumably start with an adversary taking hostile action against militarily-important US space assets. In considering what happens next, one is drawn to the worst-case possibility that a rapid destruction of US space capability is underway. This compels the US Air Force to develop, and be prepared to execute, immediate counter-actions to deter, dissuade, and prevent such an outcome. The question for the National Command Authority is, what if the worst-case characterization of the threat is incorrect? What if the first destructive action was an accident? Or a one-off demonstration intended as a political warning to the US relating to broader issues between the two adversaries? What if the attribution to a particular adversary was incorrect—perhaps even manipulated through offensive cyber operations by a third party provocateur? The point here is two-fold. As with any escalating crisis, the protagonists in a conflict are political actors, and the issues being contested are geopolitical; and thus the US management of the crisis must of necessity include the civilian as well as military leadership. Second, a hair-trigger kinetic response in space by the US confers

Figure 1. Vulnerability of Assets and the Need to Act Fast.

Figure 2. The Damage Timeline.
more risk than advantage, and should be avoided as a matter of operational tradecraft, to allow a discrete period for better characterization of the intent of the adversary before irrevocably harmful escalation is undertaken. Figure 2 depicts the advantage of such an approach.

4. The Moral Burden. Imagine if a US military commander in August 1945, exercising his own discretion, had ordered the use of two atomic weapons against Japan, without a specific pre-approval from President Harry S. Truman. Or consider the decision calculus facing a contemporary US commander if he or she knew that a tactical course of action, in order to achieve its coercive effect, would at the same time raise the global temperature by two to three degrees Fahrenheit, or reduce the world’s potable water supply by over 50 percent. Would such a decision appropriately rest with that commander? The consequences of an escalation to conflict in space, should there be either a substantial loss of service to the civil sector or persistent degradation of the space environment, or both, would place a profound moral burden on the individual whose decision produced such an outcome. The authority to take such an action would, as noted, be the president’s alone, irrespective of pre-delegated ROE. Given the moral gravity of military decisions with such broad and enduring collateral consequences, this observer anticipates that any future decision to employ force in space will be withheld and exercised only by the president. The author’s prediction does not have to be correct more than once for a military space doctrine relying on the expectation of broad pre-delegated authority to fail.

The Reality of Space Security Today, and its Implications

For all the participants’ appreciation of “net speed” in the Schriever V wargame, today there are but two militarily significant developments that would have any prospect of occurring at net speed: an adversary could commit wholesale aggression and substantially destroy space assets used by the US military; and the US could do much the same against space assets used by an adversary.

What the US military has no prospect of doing today at “net speed” is acquiring real-time knowledge that its systems are confirmed to be under attack by an identified adversary. We might know quickly that data has ceased to be transmitted; after a period we would know that specific satellites were not following their anticipated trajectories; and there could be terrestrial indicators of hostile actions aimed at the space domain. However, the hard fact is that the US is years from having a level of SSA to support a timely assessment and reliable characterization of an adversary’s rapid escalation to hostilities in space.

Not only does this remove the strongest rationale for pre-delegating authority to respond with force in defense of US space assets—the presumption that the warfighter will know substantially more about the unfolding attack than the president, and in time to do something about it; but it means that until further notice, there may be no way for the US to know enough to act in time to prevent destruction of our space-based infrastructure. Lacking such knowledge, the utility of coercive response options is correspondingly diminished, as illustrated in figure 3.

The implications of a future space crisis, drawing further from the simulated test-bed of the Schriever V Wargame, are several:

First, while the US military must plan to defend US interests in space if and as directed by the president, the notion that threats to US space-based assets would best be countered by US military responses in space is highly questionable. Indeed, should US actions ever cause severe disruption or destruction in the space environment, it will bear responsibility for the collateral effects of those actions, and its posture as global champion of preserving space for all users and for all time, will be lost.

Moreover, hostilities in space will be nothing more, or less, than the extension into the space domain of a traditional conflict with an adversary country. The goal of any coercive US military actions against such an adversary will be the same, whether employed on land or in space. Having considered the nature of such a crisis for over a decade, this observer is not only prepared to consider the use of force against territorial targets in response to an adversary’s aggression in space: but the requirements of the national interest, fully defined, point US military response options decisively away from space and, by default, toward terrestrial targets. As counter-intuitive as it may seem to some, it will be better to bomb an adversary’s counter-space weapons in his homeland than to join him in causing the irrevocable degradation of space.

This has implications for command arrangements in a future conflict where threats are posed to US space-based assets. By remembering that “it’s the adversary, stupid,” the US will better focus on the decision calculus of that government and its own political-economic-security centers of gravity, which may not assign a comparatively high value to its own access to space. The US will identify options for holding at risk equities that government holds dear in any theater or domain, with an eye to minimizing collateral impacts on third-party countries and populations. Because the protection of space as a permanent preserve for one and all is the objective, the use of force by the US in a non-symmetrical fashion against the terrestrial interests of
an adversary who was threatening the world’s interests in space would be defensible.

**What the US Needs – A Doctrine to Keep the War Away from Space**

While the US Air Force, and DoD more generally, are continuing to examine and address the military dimensions of America’s growing security vulnerability in space, there are further steps that the senior civilian leadership should consider to ensure that the US has the full benefit of a space security strategy commensurate with the profoundly broad interests involved. Here are five recommendations:

1. **Invest Urgently in SSA.** The path away from extreme vulnerability begins with improving our ability to know what is occurring in space. Only when the US has sufficient warning indicators and near-real-time ability to perceive and attribute causes to anomalies in its space systems will it be in a position to exercise effective tactical responses to an adversary bent on degrading or destroying those systems.

2. **Draw a New Red Line in Space.** An action by any party to degrade or destroy space-based assets on which the US military depends would surely be, and therefore must be treated as, a hostile attack on the US Armed Forces. The president should declare this as the core of a new space security doctrine whose over-arching purpose encompasses both the military’s equities and the other fundamental US interest in space: its preservation for the benefit of all mankind, undisturbed by destructive or disruptive acts, for all time. By taking this step, the rest of the world will be on notice that by projecting hostilities into space, they risk war with no geographic constraints.

3. **Identify the Countries of Primary Concern.** No security purpose is served by pretending that we do not know who the countries are with potentially destabilizing military capabilities in the space domain. Russia and China see themselves as major powers; they merit special policy treatment for the purpose of ensuring that future disagreements do not escalate to the point of threatening US or global interests in space. Handled right, a country-specific focus, with serious dialogue between respective policy officials, could be a positive enterprise, reducing the potential for miscalculation on all sides.

4. **Let the Warfighters Meet and Talk—in Parallel with the Politicians.** Experience shows that senior military commanders from potentially adversarial camps, if they know each other and have a reliable channel of communications, may be able to defuse rising tensions when their political leaders cannot. In the interest of preventing escalating tensions from leading to hostile actions and permanent destruction in space, DoD should seek to establish regular bilateral US-Russia and US-China contacts between the senior military commanders responsible for space operations.

5. **While Planning for a Future Crisis, Be Prepared for One Today.** To simulate future conflict is to escape some of the constraints of the day. Activities such as the Schriever V wargame properly focus a community of expert players on the parameters of an effective defense posture not far into the future, and their insights can point current officials toward some programs and initiatives and away from others. But what happens if a threat is posed against US space assets two years from now? There may be merit in conducting a wargame based on current capabilities, resource availability, and global conditions.

The US military may face troubling vulnerabilities in space, but as yet it has lost nothing. Space systems continue to empower the national defense and thus America’s security. The domain of space is still preserved for present and future generations, with large and growing benefits to people everywhere. Scientific exploration of space continues apace, led as always by the US. Given the alternatives, the goal of perpetuating these favorable conditions is worthy of a comprehensive national policy commitment that clearly supports them all.

**Notes:**

3. The Stimson Center in Washington, DC, through its program on Space Security, provides a useful resource on potential measures to protect the domain of space. See: http://www.stimson.org/space/program-home.cfm.
Conflict in space, regardless of the geographic location of the adversary, has political-military implications for the homeland and allied relations. Due to the global nature of space, offensive counter space actions against US assets will impact the US Northern Command (USNORTHCOM) mission even if the conflict is not in the USNORTHCOM area of responsibility (AOR). During a space conflict, priority and consideration must be given to friendly and ally space impacts on the homeland as well as the impact to the geographic combatant command in the region of the conflict. Additionally, collaborating with allies at the highest possible classification level yields improved allied relations, identifies and resolves contentious political and economic issues, and ensures unity of effort while leveraging the right capabilities to achieve the desired end state.

USNORTHCOM recognizes there are many challenges to meeting its mission needs, while operating in a changing and uncertain security environment. The impacts to our nation’s security include shifting and evolving global geopolitical, economic, technological, and social trends. The unified command plan assigns USNORTHCOM to focus on the nations of Continental US (plus Alaska), Canada and Mexico, plus the dependencies of Puerto Rico, US Virgin Islands, British Virgin Islands, Turks and Caicos Islands, St. Pierre and Miquelon Islands, Bermuda, and the Bahamas. Threat challenges include man-made from rogue nations, terrorist organizations, and traditional such as states employing armies, navies, and air forces; and natural threats such as hurricanes, wildland fires, floods, or blizzards. USNORTHCOM must plan and be prepared for all challenges from strategic attack to security implications on space support assets to those incurred by the wrath of Mother Nature.

USNORTHCOM is a joint geographic combatant command, with the mission to anticipate and conduct homeland defense and civil support operations within the assigned AOR to defend, protect and secure the US and its interests.1 USNORTHCOM is co-located with North American Aerospace Defense Command (NORAD), a bi-national command which has missions of aerospace warning, aerospace control, and their newest mission of maritime warning. Significant in both commands operations is the use of cyber and space domain assets, in addition to the traditional domains of land, air, and maritime. Typically, these commands may be supported by, or collaborate with, many other agencies and organizations to include allies and regional partners, the intelligence community, the counterintelligence community, Department of Defense (DoD) departments and agencies, the other combatant commands, services, and other US federal, state, tribal, provincial and local agencies, government organizations, and the private sector.2

During Schriever V Space Wargame, as the space domain was threatened in a theater outside of the homeland, there were a significant number of conflicts and prioritization of space or cyber capabilities and resources that impacted NORAD and USNORTHCOM requirements for their mission sets. During the game, it became obvious that as other combatant commands focused on their missions, defense of the homeland capabilities, and resources were not coordinated or given priority, in a timely manner to ensure the NORAD and USNORTHCOM “no fail” missions in support of our homeland were not put at unreasonable risk.

Joint Publication 3-01, Joint Doctrine for Countering Air and Missile Threats, 19 October 1999, focuses on domination of air and space protection from threat missiles.3 This doctrine discusses counter air operations, command and control for operations, planning and procedures, and air and space control measures in theater. While USNORTHCOM focuses primarily on Phase II (seize the initiative) and Phase III (dominate) of our theater campaign plan, one area specifically impacted by support from space capabilities and resources is integrated air and missile defense (IAMD). In today’s theater area of operations there are control measures focused on specific areas, but not the entire AOR, such as ingress or egress to an area or to identify assets. Missile defense focuses on critical assets, based on a threat assessment. We focus IAMD forces and assets on specific lines of communication, force concentration, and high value assets over a specific period of time.

For IAMD in the homeland, we use the same tools as in any other theater, plus we have fixed sites like over the horizon radar and interagency assets like Federal Aviation Administration (FAA) radar. When a blip appears on the radar, we run an identification matrix, and if an aircraft does not comply with established air traffic procedures and appears to pose a threat of attack, we are prepared to shoot it down. This last resort course of action is not a mission we take lightly; but it is a mission we must, when directed, be prepared to execute without fail. Many of the assets used in an overseas theater are the same as those planned for use in the homeland. For defense support of civil authorities, we use DoD equipment, none of which was purchased solely for this mission.

Politically and constitutionally, use of military in the homeland is the last resort, unless it is defense of the homeland then the military has the lead. To the maximum extent possible, events or disasters are handled by civil authorities. This is our culture and the American way of life. For air security and de-
There is a spectrum of authorities, capabilities and actions depending on the nature of threat involving, the FAA, law enforcement (Transportation Security Administration, federal air marshalls, Federal Bureau of Investigation), Department of Homeland Security, and DoD. However, it is critical that military capabilities that are apportioned, allocated or assigned against these multiple homeland missions be maintained and capable ready for USNORTHCOM to support federal agencies responding to attacks or disasters in the homeland.

For our homeland area of operation, we have unique considerations. For scale, look at the theater and number of assets requiring protection in our AOR. US Airspace is the most permissive and freely accessible in the world. Over 70 percent of aircraft are general aviation that may or may not participate with the FAA management structure.

Unlike any other theater, North America is our home and we have no fallback position so the requirement to conduct our mission is never ending, it is 24 hours a day, seven days a week, 365 days a year. While commitments in other theaters may change, be reduced or come to an end, there is no exit strategy for our homeland.

Any event or response in a geographical combatant command AOR may likely have ramifications on the availability of resources to other AORs, and reliance on space capabilities is a fact of life. With that in mind, it is imperative that the global synchronization of any combatant commander actions be mitigated to determine the impact and risk to support of the homeland.

As USNORTHCOM gathers information from state plans and capabilities, there are gaps and seams to be filled by the National Guard, Federal Emergency Management Agency, or some other agency before coming to DoD. As we identify these gaps we incorporate them into our plans and prioritize capabilities to respond should they be needed. All of these capabilities may be impacted by the loss or degradation of space or cyber resources. We must also obtain a better understanding of force protection requirements and prioritization for critical space and cyber infrastructure in our AOR.

DoD activities conducted across the breadth of the active, layered defense constitute “national defense,” while homeland defense and civil support operations focus upon the homeland and approaches. USNORTHCOM is the last line of defense in the homeland. Whether it is a large scale strategic attack or a small isolated incident, we cannot fail in our missions of defend, protect, and secure because capability gaps, conflicts or prioritizations prevented us from doing what we need to accomplish. We need to help force planners in the identification and prioritization of forces and capabilities to better conceive, plan, and execute the activities that ensure our nation’s future.

The homeland requires a family of systems approach that depends heavily on space and cyber capabilities. We need to develop policy and governance between our interagency partners to ensure that these space and cyber capabilities are always available for this more restrictive homeland mission.

At this announcement on the 2010 defense budget, Secretary of Defense Robert M. Gates stated, “we must rebalance this department’s programs in order to institutionalize and enhance our capabilities to fight the wars we are in today and the scenarios we are most likely to face in the years ahead, while at the same time providing a hedge against other risks and contingencies.” He indicated an intention to reform how and what we buy. Already we have seen that impact to existing and future contracts that will further impact space and cyber support to the combatant commands.

In a paper describing the problem of mega-catastrophes, Dr. Paul Stockton writes, “…the need to focus on the core mission of DoD is an equally important rationale against assigning lead responsibility to the department.” This paper suggests he envisions additional capabilities that will require space and cyber resources, including support for command and control mechanisms, interoperable communications, and other measures designed to improve locality-to-locality and state-to-state reinforcement. Dr. Stockton includes terrorist attacks in his description of mega-catastrophes. While DoD is seen as the “resource of last resort” he gives support that the DoD may be better suited as the primary federal agency to respond to such mega-catastrophes, thus placing a more critical dependency on our space and cyber resources committed to the homeland mission.

There are some who believe the US is not ready for the next catastrophe. Significant steps have been taken to remedy this, and the US is clearly more prepared than it was seven or eight years ago. There is a continuing perception that there is still confusion about which federal agency and official is in charge, which responsibilities are borne by what agencies, and whether assets and capabilities are guaranteed or merely potentially available. Not only must we solve this confusion about roles and responsibilities, DoD must ensure that as today’s “resource of last resort” our resources and capabilities are supported by our space and cyber domain assets.

Access to capabilities that are now inextricably tied to space is critical to the ability of NORAD and USNORTHCOM to accomplish their missions. Our ability to anticipate, deter, detect, prepare for, prevent, and mitigate catastrophic attacks or events is directly tied to continued access to this domain. Loss or significant degradation of access or priority today would have severe and unthinkable consequences for the North American continent and its people.

Regional conflicts that spread to space impact homeland defense and allied relations. The same space assets that are used in a regional conflict outside the homeland are also critical to NORAD and USNORTHCOM. Space assets cannot be local-
ized to the conflict. Any engagement in space will quickly have an impact on the homeland from military, diplomatic, informational, and economic standpoint. Additionally, the impact of these actions must be considered from an allied political military standpoint. The impact on the global space environment can have significant impact on allied relations and support for US action. Careful consideration of allied capabilities, assets and requirements in multiple AORs must be part of the decision calculus prior to accepting risk to space based assets or increasing the level of conflict in this domain. As conflict in space becomes more of a reality, geographic commanders must understand the implications of their regional actions to homeland defense and to the allied partners.

The inclusion of allies in the highest possible classification level of planning is essential to coalition success, particularly as it pertains to space. The benefits of this are significant and myriad. The inclusion of allies at this level of planning enhances trust between the coalition members and ensures that no differences in national policy or perception prevent the smooth execution of military operations. In many cases, coalition members are unaware of the differences between themselves and other members and assume support particularly in critical operations including space. In addition to the differences, allied participation in course of action development allows them to identify benefits and issues early on and better understand the motivations and reasons behind specific choices which can be particularly effective in resolving political and military issues. Allies are critical to the space effort. In addition to providing assets, space assets are terrestrially based and regional basing issues can be as important to space conflicts as they are in terrestrial based conflicts. Lastly, complicity or participation in an action may have different consequences for a regional ally than for the US particularly in relation to trade and must be factored into the planning calculus. Including allies in the entire planning cycle and at the highest possible classification level ensures the effectiveness and synergy of the coalition and maximizes the impact of operations, particularly in space.

We must develop alternatives for mission assurance should there be conflicts of priority, loss, or degradation of space or cyber capabilities. We must identify and assess single points of failure across our critical infrastructure and key resources. This must include coalition sharing of space for early warning; position, navigation, and timing; communication, intelligence, surveillance, and reconnaissance; and more. We must consider a plan to implement war reserve modes, and to contract now with industry for excess capacity and prioritization.

Ultimately, looking to the future, the nation needs a national synchronizer for the whole-of-space; DoD, intelligence community, and civil and private industry. USNORTHCOM should lead a comprehensive approach for the alignment of all homeland defense plans. This approach should make certain space and cyber impacts on mission requirements in support of the homeland are addressed and understood. Remember, defense of the homeland is the #1 priority for the DoD.

The opinions, conclusions, and recommendations expressed or implied in this article are those of the author and do not necessarily reflect the views of the DoD, USNORTHCOM or North American Aerospace Defense Command.

Article contribution or review was made by Maj Daniel J. Knight, Mr. Barry Cardwell, and Maj W. Jarman.

Notes:
1 NORAD and USNORTHCOM Theater Strategy 2008, which has referenced NORAD and USNORTHCOM Vision 2020.
2 Ibid.
3 Joint Publication 3-01, Joint Doctrine for Countering Air and Missile Threats, 19 October 1999.

BG Robert J. Felderman (BS, Aviation Management and Flight Operations, University of Dubuque, Iowa; MS, National Security Strategy, National Defense University, Washington, DC) is the US deputy director of plans, policy, and strategy for North American Aerospace Defense Command (NORAD) and US Northern Command (USNORTHCOM), stationed at Peterson AFB, Colorado. He provides advice on USNORTHCOM long range strategy, doctrine, policy, and plans to support national objectives in the combatant command’s area of responsibility; and develops strategies and policies in support of US objectives in support of Homeland Defense and Civil Support missions. General Felderman also provides advice on bi-national strategy, doctrine, policy, and capabilities to conduct NORAD missions of air sovereignty, aerospace warning and defense, and maritime warning against traditional and asymmetrical attacks on North America. General Felderman represented the commander of NORAD and USNORTHCOM during the Schriever IV (2007) and V (2009) Space Wargames.

General Felderman has commanded at the company, battalion, and brigade level and is branch qualified infantry, armor (cavalry), aviation, medical service corps, and strategic plans. He is a master Army aviator with over 2,200 flight hours throughout 22 years of aviation duty serving in assault, attack, cavalry, medevac, and maintenance aviation units. Prior to receiving his commission, General Felderman served as an enlisted soldier in the Army, achieving the rank of sergeant, and as an airman in the Air National Guard as a weapons control systems specialist on the F-106 (Delta Dart). Prior to his current assignment, General Felderman served as the operations deputy director for National Guard matters at USNORTHCOM, special assistant to the chief of the National Guard Bureau (detailed as USNORTHCOM J3 deputy director), and as director of the USNORTHCOM Joint Operations Center.

General Felderman was recently published in the Combat Studies Institute Press, US Army Combined Arms Center, Fort Leavenworth, Kansas; “The US Army and the Interagency Process: Historical Perspectives, the Proceedings of the Combat Studies Institute 2008 Military History Symposium.” He was the symposium key note speaker on the subject “USNORTHCOM interagency coordination.”
The Schriever Wargame is a series of executive-level grand-strategy games sponsored by Headquarters, Air Force Space Command (AFSPC) and executed by the Space Innovation and Development Center. Over the course of five wargames, the Schriever Wargame has helped identify areas of improvement in our national space community to significantly bolster America’s national security. These improvements evolved as a result of changes in how military space agencies are organized and how they are integrated to operate across national, commercial, civil, and military enterprises. The focus of the games has developed into a fundamental discussion regarding US policy and rules of engagement (ROE), governmental process in the investment strategy, and alternative force structures of the space enterprise. This has served to provide a fertile ground for deliberation amongst senior space community leaders, Department of Defense (DoD) and Department of State officials, with leadership provided by the AFSPC commander.

For generations, the role of space support in warfare has been essential to our successes on the battlefield. Space effects providing enhanced positioning, navigation, and timing; military communications, intelligence collection, and nuclear deterrence have become more critical than ever before. Naval forces can reach across the world’s oceans; army forces plan and execute daily missions in and out of theater, while Airmen execute accurate weapons delivery through global reach and global power. With the lightning speed and global distances at which modern combat operations are conducted, space and cyber systems will be called on to provide even more critical capabilities to enable and secure the defense of the US and its allies. Our national leaders will continue to rely on space effects provided smartly by space warriors working alongside air, land, and sea warriors to provide timely and precise decisions during times of peace and the potential crises of war in the 21st century. Former Secretary of the Air Force, Dr. Jim Roche, stated, “Space capabilities are like oxygen, we sometimes take them for granted, but if we ever lost them, we would quickly realize we cannot survive without them.”

The Schriever series has focused on the application of effects and capabilities on the battlefield and in the battlespace. The games have allowed space leaders in government and industry to consider new and innovative policies, the advancement of international law, and the utility of emerging transformational concepts as we look to the future of combat support to the warfighter. The wargame provides a venue for experts from across the space domain to gather and trade ideas and concepts of current operations and future capabilities. Areas such as survivability of space systems, integration of air and space planning, constructs of command and control relationships, and essential partnerships with our allies and space partners. The insights from the Schriever Wargame series provide vital inputs for the Quadrennial Defense Review of our military strategy and force structure.

The series is structured around a game floor that provides organizations space to operate individually, but co-located to foster communication across forums. Departments, agencies, combatant commands, and warfighters gather and fight virtual wars of the immediate future, today. Reluctant players in the real world rapidly become advocates of real-world change during the game. Voices of consent can be heard after the final game out-brief, moving forward with new ROE, better understanding of lanes in the road, and further development of space support across the space community. These consenting voices including those from the National Security Space Enterprise, and our partner allies within the wargame series, influential US industry leaders and players on the world stage. AFSPC is the lead for all Air Force wargames where space is represented (e.g., uni-
Major issues that have been explored in the game series have been as diverse as worldwide opinion regarding space concepts and operations; innovative strategic space concepts; developing a single integrated campaign plan; and evolutions of Combined Space Operations Center construct.

The Schriever Wargame series is at the forefront of investigating these concepts for the DoD, the national security space community, space industry, and our allies. The wargame provided the space community with valuable information on emerging concepts and capabilities that have crucial military utility in delivering vital and decisive effects to the battlefield and battlespace. The importance of this work is magnified by the fact that these wargames provide an unequaled opportunity for developing policy and strategy to defend this nation’s, and the free world’s, vast space infrastructure for future generations.

Figure 2. Combined Air Operations Center-Nellis, Game Floor - 14th Air Force Commander Lt Gen Larry James, commander, 14th Air Force and Joint Functional Component Command for Space, discusses options with his space operations team.

Col Robert F. Wright, Jr. (BS, US Air Force Academy; MS, Systems Management, University of Southern California) is commander, Space Innovation and Development Center, Schriever AFB, Colorado. The Space Innovation and Development Center is the centerpiece of Air Force Space Command’s (AFSPC’s) efforts to fully integrate space into the daily operational Air Force. The center develops new techniques and procedures to apply space-based capabilities to military training, exercises, plans, and operations in support of Department of Defense front-line warfighters. Colonel Wright also provides oversight of the Air Force Tactical Exploitation of National Capabilities program.

Colonel Wright’s career in space and communications includes commanding two communications squadrons and a communications group, including a one year deployed tour supporting Operation Southern Watch. He has held several key staff positions, including executive officer to the director, National Reconnaissance Office as well as aide-de-camp and executive officer to the commander, United States Central Command. He also served on the Air Staff; in the office of the Secretary of the Air Force (Space Systems) staff as a program element monitor; at United States Central Command Headquarters J6, at Headquarters AFSPC, and as vice commander, 14th Air Force.

Colonel Wright completed the DoD Executive Leadership Development Program, is a distinguished graduate of Air Command and Staff College, graduated from the Armed Forces Staff College, was accepted in to the John Malone Fellowship in Arabic and Islamic Studies (Abu Dhabi and Qatar) and completed Senior Service School as a national defense fellow.
Schriever V Wargame

Coalition Space Operations: Lessons Learned from Schriever V Wargame

Mr. Joseph D. Rouge, SES
Director, National Security Space Office
Pentagon, Washington DC

Mr. Dennis L. Danielson
Senior Engineering and Technical Manager
Jacobs Technology
National Security Space Office
Pentagon, Washington DC

The Schriever V Wargame, in March 2009, included participants from Australia, Canada, United Kingdom, and the United States, including government civilians, military, support contractors, as well as non-government civilians from the commercial space sector and industry. US participants included representatives from Departments of Commerce, Defense, Homeland Security, State, and a number of agencies including National Aeronautics and Space Administration, National Oceanic and Atmospheric Administration, and the intelligence community. Allied participation also extended beyond defense departments. In this sense, the wargame was a logical next step in the Schriever wargame series. This article highlights some of the lessons learned and way ahead.

Wargame Preparation
Preparation for the wargame included workshops attended by representatives from each country and organization as appropriate. During these workshops, a smaller group worked to develop a notional “Cooperative Security Space Defense Agreement (CSSDA),” to provide a framework for cooperation among the four countries’ defense departments. The framework assumed a senior-level space council existed for governance of the agreement, supported by a steering group that would meet periodically to address issues. It was assumed for the start of the game that this agreement was signed and in place. Under this agreement, it was also assumed that there was a high level of information sharing between space operations centers of the four allies at the start of the game. This information sharing was in support of each country’s national space operations with very limited combined operations in place. In effect the wargame was set to begin with a de facto parallel command structure in place as used in Joint Publication 1.

Wargame Execution
Soon after the start of the wargame, it was apparent to the operators that it would be much easier and timely to conduct coordinated operations among the four countries if the force structure was integrated rather than operating in parallel. The result was to create a “Combined Joint Task Force (CJTF)-like” organization within the wargame supported by a Combined Space Operations Center (CSpOC). With these structures in place it was much easier to coordinate planning and execution among the four countries. The notional construct used during the remainder of the wargame is depicted in figure 1.

The value of this construct was further underscored as wargame events developed highlighting the need to refine coalition rules of engagement (ROE) and agree on redlines with national caveats as appropriate. Although ROE were discussed during workshops leading up to the wargame, the “reality” of the wargame necessitated refinement of the ROE and highlighted the need for national caveats to respect the differences among the four nations due to policies and laws. While these differences were not large, they were important to note and necessary to account for in planning. It was also necessary to integrate commercial space and industry into the process of assessing events in the wargame and planning for an appropriate response. With the CJTF-like structure and CSpOC constructs in place, it was possible to draw a clear picture of agreed ROE, redlines, and note nuances between the nations where they existed.

The wargame play was facilitated by use of a shared computer system to which all par-
Participants had access according to their play in the game. This greatly facilitated the game play and information sharing among the different teams. It highlighted of course the contrast with the real world where even among US national security space actors there are challenges in getting the right information to the right people in a timely manner. US systems are not designed to accommodate multi-level security and information sharing with allies. Processes that exist are cumbersome at best and allow for very limited exchange of information. No one experiences this frustration more than allied exchange officers that are restricted in doing their job because of the inability to operate on computer systems used by their US co-workers.

**Lessons Learned**

Integration between allies, commercial space, and space industry is needed and must be pre-planned. The steps to accomplish this are as follows:

1. Using the wargame notional CSSDA as a model, the US should establish a real-world security space defense agreement among the four countries with other nations to follow in the future. Such an agreement provides an umbrella under which a CSPoC can be developed and operated to include personal exchanges where agreed. It will also facilitate discussion of and development of a standing “CJTF-like” organization for space. Such an agreement is a starting point that could be expanded if required. Australia, Canada, and the United Kingdom are our closest allies and it only makes sense to put such an agreement in place.

2. Expand the Joint Space Operations Center (JSpOC) Mission System (JMS) program of record to create a CSPoC. This can be done by looking for an appropriate entry point in the JMS program. This effort must also include computer systems with appropriate multi-levels of security that can bridge connectivity challenges between the four allies. Information sharing policy and implementation needs to support cooperation. The CSPoC also needs to include representation from or have connectivity with commercial space and industry. The CSPoC can either be a facility in one location or a virtual facility through connectivity with a number of locations.

3. Real world ROE, redlines, and national caveats should be developed and put in place for use by the CSPoC and “CJTF-Space.”

**Conclusion**

There is no shortage of articles espousing that space is becoming congested and contested. The question is what are we going to do? For the 450 or so people representing four of the US combatant commands, North American Aerospace Defense Command and defense departments of our three closest allies, the answer is clear—we need to move decisively in the direction of coalition space operations. This wargame demonstrated the need for this solution and highlighted a few of the challenges ahead. The alternative is not acceptable—it is time to move forward together now!
It is now widely understood that space capabilities, and the critical information they deliver, are vital to any military’s ability to exercise strategic decision-making, to conduct operational planning and to execute tactical operations. Over the last twenty years, space capabilities have emerged from being a force multiplier to a fundamental enabler of effective military operations. Our commanders depend on the precision provided by GPS to enhance the agility of forces and to synchronize precise joint fires in complex operating environments. Satellite communications enable us to exercise command and share comprehensive situational awareness on a global scale through secure, protected, dedicated, and survivable links. Space based search and rescue capabilities contribute to force protection while satellite surveillance and reconnaissance of areas, otherwise inaccessible, support our commanders’ information requirements.

Space capabilities also support other key elements of national power. Today, people in developed and developing countries rely on space in their daily activities. Our financial system, electrical grid, telecommunications, commercial fishery, agriculture, natural resource management, and aircraft movements rely on positioning, navigation and timing signals provided by the GPS constellation. Likewise, satellite communication is critical to civil and commercial activities on a global scale—a demand that has generated the capacity now heavily leveraged by military forces worldwide. The information that fuels our national power flows through these space line of communications (SLOC).

Our dependence on space-based capabilities is such that militaries must now question their ability to achieve operational success in theatres where access to space capabilities would be denied or severely limited. Space is a challenging environment to exploit. It is both austere and contested. It is subject to natural harmful electromagnetic phenomena and even though it has limitless expanses, its increased usage has created a demonstrated risk of collision between resident space objects. Today any state, even many non-state players, can afford some degree of space access as well as the ability to interfere with our collective right, guaranteed under the Outer Space Treaty, to exploit the medium of space for peaceful purposes in the pursuit of national and international objectives. Ultimately, space assurance requires collective engagement. Space control, as a means to assure the domain, exists to protect national and military SLOC. Space control exists to maintain information superiority.

These facts now resonate within Canada’s Department of National Defence. The experience and insight acquired over the last four Schriever games helped shape our understanding of the role space plays in support of the defense and security agenda. What has also become increasingly evident over the last few years is that no nation can deliver and guarantee all of the space effects our commanders’ demand. There is therefore a certain logic to pooling space capabilities for the benefit of many. This is especially true for space-based intelligence, surveillance, and reconnaissance assets as they can inherently serve more than one combatant command in a single orbit. Implementing a coalition approach to space support can provide redundancy, increase robustness, and generate deterrence effects. To properly manage and responsively apportion a coalition’s space capabilities requires a coalition command and control capability empowered with the right authority to manage the delivery of space effects.

The need for a coalition approach to space control is also...
evident. After a 19 year hiatus, Canada is resuming in 2011 its 30 year participation in the space surveillance network with the launch of SAPHIRE, a space-based space surveillance system. Assets such as this require a collaborative management structure. The concept of coalition space operations, articulated in Schriever V as the Coalition Joint Space Operations Center (CJSPOC) or the Coalition Joint Task Force (CJTF) for Space, is viable and should therefore proceed from the concept to the design stage. The CJTF for Space construct would facilitate the request for forces process as well as provide the means to apportion forces, delegate authorities and rules of engagements as well as be a means to communicate allied request for space effects. The construct would also facilitate the sharing of the space common operating picture with coalition partners and leverage a distributed network of space analysis capabilities to serve the intent of the CJTF for Space. The CJSPOC, empowered with the right authority, would be the system of choice to effectively generate space domain awareness and defend coalition space systems from natural and intended threats.

The diplomatic, informational, military, and economic, or comprehensive, focus of Schriever V reinforced what we have learned in other theaters—a comprehensive approach is critical to achieve strategic effect. This is especially true in the deterrence and defensive phases of the space campaign plan. Greater emphasis must be placed on seeking better synergies between diplomatic, economic, and military effects. Nations should not shy away from pointing out to the world when an actor intends to or has behaved in a manner contrary to established international law/norms. Failing to do so would jeopardize our future aspirations. We cannot afford a day without space—our global economy is fuelled by space effects. Militaries may have more redundancy to operate, but national infrastructure and economies would be devastated as a day without space would, due to regeneration constraints, actually be months, if not years without space. The military mandate is to protect the homeland—that now includes Canadian civil, commercial, and military space. Only focusing on the latter would be misguided as at the end of the day, space security must be pervasive. A day without space would be a military failure. Our collective strategic objective must be to maintain freedom of access and responsible use of space. That objective can only be achieved through a synchronized and comprehensive coalition engagement.

Canada appreciates the opportunity to conceive futures through the Schriever Wargames. The future we have seen suggests that a hands-off approach will not yield a desirable outcome. We look forward to future engagements to eventually shape a Grand Space Strategy.

Our collective strategic objective must be to maintain freedom of access and responsible use of space. That objective can only be achieved through a synchronized and comprehensive coalition engagement.
Would it be helpful when formulating US grand strategy to address the challenges posed by complex, hybrid warfare to have insights into the nature of armed conflict conducted at the speed of light in the global commons of outer space and cyberspace? Would it be valuable to have a better grasp of the relationships among the space, cyber, and other operating domains? Would it be useful to understand how global effects created in those domains might impact the whole-of-nations and influence the course and outcome of conflict at the strategic, operational, and tactical levels? Would it be constructive to have a better sense of the policy and operational challenges posed by greatly compressed decision-making timelines required for mission success in those operating environments? These are rhetorical questions since the obvious answer to each is, of course, yes.

The Schriever V Wargame was auspiciously timed to help inform the analysis and formulation of national security policy and defense strategy. The output of the game aligns with the opportunity for a new administration to examine strategic issues about how to protect and advance US national interests while it is carrying out both a Quadrennial Defense Review and a Space Posture Review. Insights from the game can serve as useful inputs to both reviews and help ensure that the roles of space and cyber capabilities are properly considered in the development of a new National Security Strategy to deal with our dynamic and dangerous world.

Schriever V was the latest in a series of wargames sponsored by Air Force Space Command to examine policy, strategy, doctrine, operations concepts, rules of engagement, requirements, force structure, and other issues related to space activities. The game was the largest and most sophisticated of the series. It included over four hundred participants from Department of Defense components, the intelligence community, other US government departments and agencies, industry, and US allies. All five space sectors—defense, intelligence, civil, commercial, and international—were well represented.

This author was fortunate to participate in the Executive or National Command Authority cell in all of the games as either a player or mentor. During Schriever V, the executive cell deliberated on a range of topics that closely approximated the complicated, substantive issues a US president and National Security Council would likely confront in a deep crisis and conflict. While observations gleaned from a wargame should be scrutinized carefully for their validity and relevance before extrapolating them to the “real world,” Schriever V proved an excellent forum to illuminate key issues that should be addressed by senior government officials, policy analysts, and national security planners. This article provides an overview of some of the main policy and strategy issues highlighted by the wargame.

**Space and Cyber Security**

Outer space and cyberspace increasingly are interdependent and interconnected domains. The key intersection between them is information. Space capabilities are of course major components of the global, national, and defense information infrastructures. They collect, generate, and relay information around the world operating simultaneously in both the space and cyber domains. Moreover, the information infrastructure controls physical infrastructures and provides applications that are integrated into nearly every sector of our critical infrastructure including telecommunications, energy, finance, transportation, and emergency services. The issue of space and cyberspace security thus has attained national prominence because of its profound implications for our society.

Given the many and varied relationships and overlaps among space control, information operations, and cyber operations, how should the seams among them be coordinated, deconflicted, and, where appropriate, integrated? What are the correct offense-defense relationships in the space and cyber domains? Effective protection and defense of space assets and supporting infrastructure will require a clear understanding of the range of capabilities and effects of information operations and cyber measures and countermeasures. There will be a synergistic benefit if the US space protection effort employs non-materiel solutions such as strategic communications, military deception, and psychological operations along with materiel information assurance, computer network defense, electronic countermeasures, infrastructure protection, and other solutions to defend our space assets. This is a broad policy issue that cuts across Title 6, 10, and 50 statutory authorities, policy and oversight responsibilities, command and support relationships, and other related management and organization matters. Consequently, resolution of the issue will require new operational constructs between organizational entities to ensure mission effectiveness.

**Understanding the Stakes**

National security interests are typically defined as values, conditions, and geographic factors of major importance to the preservation and well-being of the nation. They include broad ideals such as freedom, human rights, and economic prosperity.
They also include such specific geographical concerns as territorial integrity, access to global markets and natural resources, and international order. Vital interests are those interests that are of overriding importance to the nation’s survival, integrity, and vitality. Freedom of access to and use of outer space and cyberspace clearly are vital national interests. But space and cyber activities are transparent to many Americans who simply take them for granted.

A fundamental issue is how to ensure that our national decision-makers truly understand the stakes for the US in those domains before there is a conflict? While most participants in a space wargame tend to have some familiarity with the subject, national decision-makers typically are focused on other issues. The question thus is how best to get the attention of policy makers in the executive and legislative branches of the US government, inform them about our national interests in space and cyberspace, and ensure the US is adequately prepared to protect and defend those interests. This is not a trivial problem given the array of daunting domestic and international issues the country needs to confront. But it is essential that our national political leadership comprehend why unimpeded access to and use of space and cyberspace are vital nation interests.

This will require an appreciation of the value of space and cyber activities to US prestige, influence, economic vitality, and national security. It will also require an understanding of the importance of such capabilities to global commerce, trade, and security. Moreover, it will require comprehension that the consequences of disruption or loss of critical space and cyber mission capabilities will increase the risk of strategic surprise, undermine the functioning of the globally interdependent, information-based economy, decrease the combat effectiveness of our armed forces, increase the risks and costs of military operations and intelligence activities, and complicate our ability to support our foreign policy and defense commitments to allies and friends. Denied freedom of action to employ force multipliers in those domains, for example, the combat power of our terrestrial forces will be reduced to that of a 1950s-era force.

**Shaping the Environment**

Outer space and cyberspace are global, cross-cutting domains. They are global commons like international waters and airspace that encompass the terrestrial mediums of land, sea, and air. Space and cyber are also mediums—like the land, sea, and air—within which the US conducts intelligence activities and military operations to achieve our national security objectives. In that regard, the space and cyber domains potentially are flanks to any terrestrial battlefield. Moreover, they are now contested operating environments where our assets are held at risk. A closely related issue thus is what measures should the US undertake now to shape the space and cyber environments in ways that will help us to protect and defend our national interests?

Actions taken during the pre-crisis or pre-hostilities phase are of course critical to deterrence, dissuasion, and prevention of armed conflict. The US must actively promote the peaceful uses of space and cyberspace, facilitate a code of conduct to establish norms of responsible space fairing and cyber behavior, establish a leadership position in international deliberations of legal and regulatory matters affecting space and cyber activities, and protect our space- and cyber-related commerce, trade, and security equities within international regulatory bodies. Moreover, while controls on exports of space and information technology goods and services with military applications are required to prevent technology from getting into the wrong hands, the export control process should not hamper our international competitiveness or erode our technological leadership.

A “whole-of-government” or, more accurately, a “whole-of-nations” approach will be required to properly shape the space and cyber domains given the mutual interests of our allies and friends and the likelihood of alliance or coalition involvement in a future contingency. All tools of statecraft must be brought to bear and wielded synergistically to achieve such strategic effects. Yet there are substantial challenges to focusing all the elements of national or coalition power to achieve this objective. Diplomatic, informational, and economic actions must be developed, coordinated, deconflicted, and synchronized to effectively and efficiently apply soft power. Moreover, they must be reinforced by military capability to message, signal, and condition in order to shape the environment. Persistent, active engagement leveraging smart power will be required to influence behavior positively in the space and cyber domains.

**Alliances and Coalitions**

Throughout US history, we have relied upon alliances and coalitions to secure and defend our interests around the world. The fact that there is safety or strength in numbers is a truism that likely applies to the space and cyber domains just as it does to other operating environments. A comprehensive, whole-of-nations approach that brings many countries diplomatic, information, military, and economic resources to bear will contribute both to shaping the space and cyber environments and strengthening deterrence. Any potential adversary’s risk calculus would have to take into account the prospect of engaging not only the US but our allies or coalition partners as well in response to space or cyber attack. Similarly, both deterrence and warfight-

---

The US must actively promote the peaceful uses of space and cyberspace, facilitate a code of conduct to establish norms of responsible space fairing and cyber behavior, establish a leadership position in international deliberations of legal and regulatory matters affecting space and cyber activities, and protect our space- and cyber-related commerce, trade, and security equities within international regulatory bodies.
ing would be enhanced by the ability to rely upon alliance or coalition space and cyber resources, especially for situational awareness (SA), force enhancement, or reconstitution, instead of just our own.

The political-military cohesion of any alliance or coalition of course may become a center of gravity for the US in the event of armed conflict in outer space or cyberspace. Additionally, the complexity of decision-making increases as a function of the number of participants involved. Individual nation’s policy views and red lines will have to be addressed and accommodated in campaign planning and operations. Moreover, alliance or coalition decision-making processes, command and control arrangements, and rules of engagement will have to address the challenge of achieving decision advantage in warfighting conducted at light speed.

**Deterrence and Dissuasion**

There are a plethora of questions about whether or how the US can deter aggression against our interests in the space and cyber domains and dissuade an adversary from pursuing capabilities to threaten our assets. While we successfully relied upon the threat of nuclear retaliation to deter the expansion of Soviet power and influence through aggression during the Cold War, how does deterrence work in a multi-polar international security environment with other great powers, lesser regional powers and rogue states armed with weapons of mass destruction, and non-state actors such as transnational terrorist groups? What are the implications of states, groups, and individuals having access to powerful computing and encryption, ubiquitous telecommunications, global remote sensing and geospatial information, precise positioning, navigation, and timing, and environmental monitoring and forecasts that can be employed for military purposes? Will the prospect of despoiling space with thousands of pieces of debris that could stay in Earth orbit for a millennium provide a restraint comparable to the horrors of thermonuclear war? Is it possible to dissuade a nation state or subnational group from pursuing anti-satellite (ASAT) or computer network attack capabilities that could disable critical infrastructures?

How might we dissuade China, for example, from conducting another ASAT test or emplacing malicious software into our critical infrastructures? Should we rely on deterrence through punishment (i.e., retaliation) or denial? How can deterrence, including intra-war deterrence and escalation control, work given the current asymmetry of value between our reliance/dependence on space and cyber assets compared to potential adversaries? Rather than being an approach to avoid the costs of mission protection, does not deterrence require us to diminish the vulnerability of our space and cyber assets so as not to provoke attack? Will the vulnerability of our space assets and critical infrastructures controlled by computer networks lead us to be self-deterred? Can we extend deterrence to protect the space and cyber assets of our allies, coalition partners, and friends? Given the absence of knowledge about foreign cultures, history, and leadership intentions, how do we create credible military options that will ensure the costs of aggression in the space and cyber domains outweigh its risks to an adversary?

**Diplomacy and Arms Control**

The Obama administration entered office having campaigned that it would emphasize an international, cooperative approach to space security. Consequently, this raises the question of what diplomatic efforts would be useful to enhance international security and order in the space and cyber domains? How do we countervail foreign efforts to constrain US national security space activities and protect our interests in space? A diplomatic strategy is needed to shape the international policy and legal regime in a manner that complements, rather than constrains, our national security space program. A key piece of that strategy must be a strategic communications campaign to frame the terms of the policy debate and inform international opinion.

Russia, China, France, Canada, and other nations have proposed various measures to prevent an arms race in space. Should the US pursue an international code of conduct, rules of the road, or incidents in space agreement? Some of the questions that must be addressed in this regard include should the US pursue restrictions or bans on ASAT development, testing, or deployment? If so, how do we address fundamental problems regarding the definition of an ASAT weapon, the commonality of civilian and military technology, verification, and enforcement? Should we pursue arms control or confidence building measures through tacit or formal arrangements? Do we negotiate on a bilateral or multilateral basis? How should we ensure that such measures are not used inappropriately to constrain US national security space activities?

**Intelligence and Situational Awareness**

Knowledge of one’s adversary is of course a prerequisite for achieving decision advantage and victory in warfare conducted in any domain. Given the importance of understanding foreign capabilities and intentions, another issue to consider is whether US intelligence activities adequately support space and cyber activities. Are the allocation of intelligence collection and analytical resources to assess the threat to US space and cyber assets and operations commensurate with our growing dependence and vulnerability? Are gaps in our knowledge being systematically addressed and closed? Is intelligence support for characterizing and attributing hostile intentions and actions being given a high priority in the competition for intelligence collection and analytical resources?

The intelligence community must address a broad array of national intelligence priorities. In the process, difficult choices must be made about how to allocate scarce resources. Nonetheless, the ability to protect and advance our interests in space and cyberspace requires adequate intelligence capabilities to manage support to space and cyber missions, drive collection, close critical information gaps, preclude surprises, and provide indications and warning. Similarly, intelligence is essential to answer key questions pertinent to space and cyber policy and strategy formulation, defense planning, architecture development, acquisition programs, and operations.

Space and cyber intelligence, surveillance, and reconnaissance (ISR) are integral to space SA. The scope of the SA mission has expanded to become a national mission supporting
all of the government space sectors as well as commercial and foreign entities. Vast amounts of relevant data are available to help accomplish the mission if the policy, legal, and other non-technical barriers to intersector and international cooperation are addressed. These issues, including collaboration with multinational corporations and international consortia, must be resolved long before the crisis to enable the information access, sharing, and integration necessary to operate effectively in an alliance or coalition environment. Providing appropriate SA services to commercial and foreign entities as well as establishing cooperative relationships that can leverage allied and friendly ISR capabilities is prudent and necessary. Such relationships will enable the establishment of organizational arrangements, integrated deliberate and crisis action planning, and combined operations.

SA is absolutely essential to answering the basic questions national decision-makers and combatant commanders will have in the event of crisis or conflict in space. ISR and space situational awareness (SSA) will provide the means necessary to establish hostile intent and hostile acts required for self-defense. Indeed, the availability of actionable, decision-quality SA information is critical to the process of obtaining pre-delegated authorities necessary to operate at the speed of need. Moreover, monitoring, verification, and enforcement of compliance with any new international code of conduct, rules of the road, or incidents in space agreement will be dependent upon our SA capabilities. Yet it should be recognized that the space and cyber mediums pose unique and difficult challenges for characterization, attribution, and producing credible evidence on which to act and justify action. There will likely be a gap between the fidelity of information policy makers would like to have and what is available. Ensuring policy makers and decision processes are prepared to deal with the inevitable ambiguity and uncertainty will be an important matter.

New Technology and On-Orbit Operations

The advent of small, micro- and nano-satellite technologies and new operational concepts for their on-orbit operations raise many potential issues. Such new satellite technology has been demonstrated not only by the US, but several other nations as well. Despite such foreign space activities, how the US chooses to behave will be key to establishing the precedent and the de facto norm for conducting on-orbit operations with such new technology. Using micro- and nano-satellites for self-inspection and servicing, for example, may become routine for civil and commercial space operations.

The application of such technology for ISR, SSA, or other intelligence or defense missions involving non-cooperative space objects, however, may be considered qualitatively different and more politically sensitive. There are clearly insights to be gained by examining analogous activities from other operational mediums such as the seas and air. Vessels on the high seas and aircraft in flight must be operated in a manner that does not pose a danger to navigation. Similarly, signaling to communicate intentions is the norm when maneuvering in proximity to another ship or aircraft.

Consequently, it will be important to evaluate to what extent does the US want to pursue such capabilities and concepts—not just because technology permits us, but because its wise to do so. Careful consideration of this matter is necessary since the risk is helping to create a norm that effectively licenses the conduct of such operations involving our own space assets by foreign entities. In that regard, it would be prudent to prepare appropriate policy and operational responses, including defensive countermeasures, against such capabilities.

Space Protection and Defense

The overarching issue is what defense activities are required to deter threats to US space assets and operations or, in the event of hostile acts, provide adequate protection? Closely related is the question of what is the proper mix of passive and active defenses? It would be imprudent to rely on deterrence alone as the chief means of mission protection. Given the nature and extent of our susceptibilities and vulnerabilities to a broad range of plausible threats, it will take a layered, defense-in-depth employing a range of approaches to solve the problem.

So what is the best approach to reduce the vulnerability created by our dependence upon space and cyber assets for security and commerce? How should we ensure the endurance, continuity, and survivability of such assets in the event of conflict? How do we prepare to deal with surprise, withstand a cheap shot, and recover from subsequent attrition? Can we condition potential adversaries and channel threats into areas where we are better prepared defensively? Have we established the correct protection priorities and requirements? To what extent should we prepare to protect commercial and allied assets and operations? How should we establish collective and coalition defense arrangements?

The global proliferation of space systems, technology, and know-how poses challenges to US and allied military forces and operations. The ability to hold space and cyber assets at risk would support the credible threat of force required to support deterrence and its effective use in defense of our assets in response to aggression. The question of what role active defenses could play for protection and defense, however, inevitably raise a series of policy issues. While the “weaponization” of space remains an emotive hot button issue, similar political sensitivities are likely to emerge regarding offensive operations in the cyber domain.

Response Planning

Policy makers will want to maintain the maximum degree of flexibility and be presented with a range of options before deciding how to respond to deliberate interference with US freedom of action in space and cyberspace. No responding to aggression is not an attractive option. Diplomatic and economic responses should of course be considered and may have utility. But they may prove to be insufficient to persuade or compel an aggressor to cease is aggressive behavior. Consequently, defense planners must be prepared in advance for the contingency.

What should be the symmetric or asymmetric responses available to military commanders and national decision makers? Should the action be a response-in-kind or should it entail verti-
cal or horizontal escalation? If the adversary does not own or operate space systems, or does not use them in a significant way, a tit-for-tat response will not be useful. National decision-makers will be concerned about discrimination and restraint in the use of force. What is necessary to ensure that flexible deterrent options and major attack options control escalation? At the other end of the planning spectrum, will policy makers be willing to cross an adversary’s homeland threshold with non-kinetic or kinetic weapons to retaliate or disarm an enemy who has attacked a US satellite, but not inflicted casualties or loss of American lives? What escalation risks are policy makers willing to take to respond to an enemy’s campaign against our space assets?

The speed of weapons effects from nanoseconds to minutes in the cases of cyber, electronic, and kinetic attacks will greatly compress the timelines for decision-makers. Consequently, what are our pre-planned redlines, thresholds, and triggers? Are redlines established during the Cold War with respect to missile warning and nuclear command and control sufficient? Have we properly communicated those redlines and thresholds to potential adversaries?

Moreover, how well have those thresholds and triggers been tied to space and terrestrial postures and conditions to enable the policy and operational responses necessary to deal with the potential speed of battle? What rules of engagement, command and control arrangements, and pre-delegated authorities are required to enable the effective and efficient execution of defensive actions? How should campaign planning as well as the policy review and approval of war plans take into account the decision making processes as well as command and control relationships involved in extending protection to allied, friendly, and commercial space assets, particularly in the context of space operations in a coalition environment? Given the compressed timelines, the uncertainties involved in space conflict, and the potential consequences of inaction, will policy makers be willing to shift from an “observe-decide-act” approach to a “decide-observe-act” posture?

Conclusion

The strategic value of the Schriever V Wargame was that it effectively explored the challenges of conflict in space and cyberspace and yielded timely policy and strategy insights that can benefit both the Quadrennial Defense Review and Space Posture Review. The game highlighted numerous strategic issues that should be taken into consideration as the Obama administration analyzes and formulates national security policy and defense strategy. The understanding gained from Schriever V could help the US national security establishment to address the challenges posed by complex, hybrid warfare involving outer space and cyberspace. It should be useful to understand the roles of space and cyber capabilities and effects on deterrence and warfighting. Observations from the game should also contribute to the design of decision-making processes and procedures to deal with speed of light space and cyber warfare.

The US has vital national interests to protect and advance in the space and cyber domains. By providing a window to the future, Schriever V presents both challenges and opportunities for government officials, policy analysts, and national security planners. There are many questions that must be answered if the US is going to understand the stakes of space and cyber warfare, shape those environments, and implement a comprehensive, whole-of-nations approach with our allies or coalition partners to prevent or, if necessary, fight and win such conflicts. No future president and commander in chief should be placed in the position of having to tackle those issues in the midst of a deep crisis or conflict. The time to do so is now. Evaluating and addressing the policy and strategy issues highlighted by the game will help to ensure that America is prepared to deal with the complex, hybrid warfare we may have to confront in our dynamic and dangerous world.

The author served as a mentor to the Executive Decision Team and as national security advisor for part of Schriever V.

Mr. Marc J. Berkowitz (BA, with Distinction, Security Studies, George Washington University, Washington DC; MA, National Security Studies, Georgetown University, Washington, DC) is a vice president of Martin in 2003, Mr. Berkowitz served in the Office of the Secretary of Defense as a career senior executive in the positions of assistant deputy under secretary of defense for space policy and director of space policy where he lead the analysis, formulation, and oversight of US Government and Defense Department policy guidance for the conduct of defense and intelligence activities in outer space. Mr. Berkowitz also was the director of space studies at National Security Research, Inc., a professional staff member in the Foreign Technology Center of SRI International, a foreign affairs analyst in the Congressional Research Service’s Foreign Affairs and National Defense Division, and an intelligence specialist in the Department of State’s Bureau of Intelligence and Research. Since leaving the Defense Department, he has also served as a consultant to the Defense Department and the intelligence community.

Mr. Berkowitz was awarded the Defense Department’s highest civilian award, the Defense Distinguished Civilian Service Award, twice.

Industry Perspective

Schriever V: Managing and Understanding Consequences to Military Space

Maj Gen Franklin “Judd” Blaisdell, USAF, retired
Director, Space and Air Force Programs, Raytheon Company
Arlington, Virginia

As the players experienced in the Schriever V Wargame, space is not only critical to US interests, it is critical to the operation of an entire interconnected world economy. Space has become a “must have” element in the domains of credit card transactions, stock market prognostications, and banking transfers to cell phone communications, video presentations, and live news broadcasts. The military applications are critical and extend from missile warning, weather, GPS targeting and timing, intelligence, surveillance, and reconnaissance (ISR), and communications, to blue and red force tracking, as well as status of logistics/supply chains. The Schriever V Wargame capitalized on a world space dependency and did so at a very strategic level. It pushed all participants (including the coalition) into addressing the “whys and wherefores” of losing key elements of national power together with the next order tasks of replacing the must have systems. The fact that space has been viewed in many circles as an operational medium sheltered from attack with its resources immune from calculated disruption, will not pass the litmus test anymore.

As a former space commander on two separate occasions, a number of strategic questions come to mind in this type of worldwide wargame. The first is the number of “space players” we have in the world today and what consideration is being given to who will play in a regional conflict and who will sit on the sidelines. There are more and more countries today that are eager to gain “use of the high ground” for political, economic, and military purposes. This recent phenomena has manifested what we now call the drive for “pridesats” or nations putting up payloads in orbit simply to gain national prestige. If there was ever a conflict in space between two major regional powers, then the consequences of several nations’ assets needs to be considered (those that are in conflict … but equally those that will sit on the sidelines and wait for their chance to leverage their opportunities). The dependencies upon warning, navigation, and timing, ISR, communications and so forth, presents a distinct advantage to those countries with surviving assets and a command and control system ready to piece together economic, military, and political instruments of power. The US and its coalition partners must consider a continuity plan, as well as, a minimum implementation plan for surviving key economic, military, and political necessities.

Secondly, the need for operationally responsive space (ORS) assets (both for the US and coalition) can not be emphasized strongly enough. The inability to provide economic structure, military capabilities, or effective political tools in a fast-paced and highly-charged environment will keep the US “reactive” instead of “proactive” in a crisis. Consideration should be given to “on-orbit” assets (which is the ultimate in responsiveness). These can be stored, hidden, or postured in many ways but the key is they are on-orbit and ready in the event of crisis. Many feel the ORS mission today is not getting the attention it needs to demonstrate several levels of the responsive concept. A concentrated effort to utilize “plug and play” opportunities on small payloads to supplement larger constellations is a good initial way to diversify risk as well as solve interim needs. Hosted payloads and smaller “free flyer” launches offer ready capability while the technological challenges of future generation constellations are being tested. Capability now through small payload diversification allows time for more testing and risk reduction activities on the larger constellations.

Thirdly, industry needs to play a bigger role in contributing data for space situational awareness. To clarify, industry needs to do their part in cataloging and tracking the disposition of transponders, circuits, payload capabilities, and status of satellites on orbit. Clearly in a world of heightened tensions, information about what is riding on a payload or operating under contractual agreements with multinational industries is important to decision makers. This may even be expanded to include terrestrial wireless and fiber services tied to space which many fail to consider as part of the puzzle. The ability to understand the strategies of an adversary in space or the rest of the net-centricities that are tied to space is an important ingredient for resolution of conflict. An adversary’s assets co-mingled with your capabilities on a commercial platform presents a real challenge when both parties are facing conflict.

Finally, the time to make decisions as General C. Robert Kehler has pointed out, is very short (speed of light). Plans, strategies, reconstitution of assets, tripwires, engagement policies, all need to be done in advance of any conflict. Public declarations of how nations should view the medium of space, their assets, and what constitutes hostile intent, freedom on navigation, and particularly the various consequences of management and the threat triggers that are constantly changing require a lot of work. The great news is that wargames like Schriever V contribute to that opportunity. There is no doubt in my mind that this type of intellectual rigor needs to continue. The rewards for the nation are worth the effort and the sacrifices.
Historical Perspective

Schriever Wargames: The Battle for the Ultimate High Ground

Mr. James C. Mesco
Historian
Space Innovation and Development Center (SIDC)
Schriever AFB, Colorado

Several decades from now, the important battles may be ... space battles, and we should be spending a certain fraction of our national resources to ensure that we do not lag in obtaining space supremacy. The mission is to maintain peace.
~ General Bernard A. Schriever, commander, Air Force Systems Command

General Bernard A. Schriever, over forty years ago, recognized the importance of space to America’s defense and projection of national policy. It was therefore appropriate that the only wargame focused on space bear his name. Prior to the development of the Schriever Wargame series, Air Force Space Command (AFSPC) provided planners, players, and assessors to Air Force, Army, and Navy Title 10 wargames around the globe. Though these wargames included space events, the wargame planners never fully explored the possible extent to which space capabilities affected the battlefield.

Schriever 2001 was the first Air Force wargame focused specifically on space issues and space play. The Space Warfare Center (SWC, [later re-designated the Space Innovation and Development Center or SIDC]), headed the work on Schriever 2001. The SWC’s Analysis and Engineering (SWC/AE) Division team designed the wargame. Besides supporting events like other wargames, this wargame provided a forum for discussion and debate on the development and employment of future aerospace systems, and their contributions to our national security objectives. To apply all possible space capabilities, SWC/AE incorporated many of the space capabilities seen in other wargames, such as Global Engagement (now Unified Engagement), but the SWC expanded these to encompass every possible capability available to commanders in the year 2017. To bring all of these aspects of the wargame together, AFSPC and the SWC brought together the finest experts on space power available. These included retired senior Air Force, other service and space industry leaders as well as those leaders in charge of space forces at the time. The wargame mentors included: General Thomas S. Moorman, Jr., USAF, retired, former Air Force vice chief of staff; Lt Gen Eugene Santarelli, USAF, retired, former vice commander of US Pacific Air Forces; VADM Lyle Bien, USN, retired, former deputy commander-in-chief, US Space Command; Lt Gen Jay Garner, USA, retired, former Army vice chief of staff; Mr. Mark Berkowitz, who worked in the office of deputy under secretary of defense for space; Mr. Keith Hall, former director of the National Reconnaissance Office (NRO); and Ms. Natalie W. Crawford, senior fellow, RAND Corporation. The senior military leadership included: Maj Gen Brian Arnold, director of space and nuclear deterrence, Office of the Secretary of the Air Force for Acquisition; Maj Gen Thomas Goslin Jr., director of operations, Headquarters US Space Command; Maj Gen William Looney, commander, 14th Air Force; Maj Gen David MacGhee, vice commander, Air University; Maj Gen Lance Smith, commander, Air Force Doctrine Center; Brig Gen Carol Elliot, vice commander, Air Intelligence Agency; and Brig Gen Craig Weston, director, Corporate Operations Office and chief information officer, NRO.

The Schriever 2001 Wargame began on 22 January at Schriever AFB, Colorado and concluded on 25 January 2001. The SWC/AE Wargames and Exercise office designed two key innovations into this wargame never seen before in other Title 10 events; the creation of a Blue Commander-in-Chief Space (CINCSPACE) team which allowed an in-depth examination of the spectrum of CINCSPACE to commander joint task force roles, responsibilities and relationships required to plan and prosecute a space campaign and a commercial team, composed of representatives from the commercial space industry, which allowed the examination of the relationships between government and commercial entities in a time of crisis. SWC/AE designed the vignettes and events to frame key time slices during the conflict. Schriever 2001 showed a better understanding of advancing space power in the world of the future and provided insight that was important to the ongoing major Department of Defense (DoD) military capability projections such as the Quadrennial Defense Review.

The success of the first Schriever Wargame led AFSPC and Air Force leadership to provide funding and resources to support additional Schriever Wargames. On 20-28 February 2003, the SWC held Schriever II (S-II) at Schriever AFB. The S-II Wargame examined many factors and weapons systems the DoD would contend with by 2017. The S-II Wargame again brought together the best minds in the DoD, federal govern-

Besides supporting events like other wargames, this wargame provided a forum for discussion and debate on the development and employment of future aerospace systems, and their contributions to our national security objectives.
During the wargame, the wargame team concentrated on collecting the key insights of the discussions, to include those that came from command developed analytical research questions as well as any emerging issues that develop during the wargame.
Notes:
1 Air Vice Marshal Ron Dick, Reach and Power, the Heritage of the United States Air Force in Pictures and Artifacts (Air Force History Program, Washington DC, 1997), 466.

Mr. James C. Mesco (BA, History, Slippery Rock State University; MA, History, Georgia College and State University) is the historian for the Space Innovation and Development Center (SIDC), Schriever AFB, Colorado. He is responsible for collecting, organizing, analyzing and interpreting documents and writing the history of the organization's operations and special programs in peace and war. He served on active duty from 1980–2004 and retired from the Air Force. He became an Air Force civilian in 2004. Since May 1999, he has served as the SIDC historian.

Mr. Mesco entered the US Air Force in September 1980. His initial assignment was as a missile combat crew member and completed over 300 combat alerts. In 1985, he became a historian in the Air Force History Program. He served as a historian in the 28th Bomb Wing, Ellsworth AFB, South Dakota; 90th Strategic Missile Wing, F.E. Warren AFB, Wyoming; 26th Tactical Reconnaissance Wing, Zweibrucken AB, Germany; Warner Robbins Air Logistics Center, Robins AFB, Georgia; 21st Space Wing, Peterson AFB, Colorado and 50th Space Wing, (then Falcon AFB, Colorado, later renamed Schriever AFB) and the Space Warfare Center (later renamed the SIDC), Schriever AFB. He deployed and served as the historian for the 4404th Composite Wing, King Abdul Aziz, AB, Saudi Arabia; NCO historian for Headquarters, European Command, Patch Barrack, Stuttgart, Germany; the Balkans Combined Air Operations Center historian, Dal Molin AB, Italy and 379th Air Expeditionary Wing, Al Udied, AB, Qatar.

Mr. Mesco received recognition for his efforts as a historian with the 1988 - USAFE Program Services Award, 1997 - AFSPC Historian Achievement Award, and 1999 - USAF Excellence in Wing History Program Award. He published articles in Air Force Journal of Logistics, and QUEST, The History of Spaceflight Quarterly.

Subscribe to High Frontier Electronically

It’s as easy as 1, 2, 3 ...

1 Log on to the “Subscription Center” at the Air Force Link web site http://www.af.mil/information/subscribe/index.asp

2 Select AFSPC High Frontier Journal, enter your name and e-mail address

3 Click on the “submit” button

You will receive an e-mail asking you to reply in order to confirm your subscription. You will not receive your subscription unless you reply to that message. Your electronic subscription is free.

In an effort to reduce costs of printing, Air Force Space Command’s High Frontier, the quarterly journal for space and missile professionals, is available as an electronic publication.

Every quarter you will receive an email notification that the journal is available for download on the Air Force Space Command web site.

A limited quantity of hard copies are available at installation public affairs offices.
Dear Reader

High Frontier, Air Force Space Command’s professional journal, is designed with all space, missile, and cyberspace professionals in mind across the Department of Defense, the National Security Space community, our friends in Congress, allies, and partners in industry.

We are interested in what you think of High Frontier and request your feedback. We want to make this a useful product that stimulates intellectual thought and debate on a variety of subjects important to space, missile, and cyberspace professionals.

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) 554-3731; Fax: (719) 554-6013
Email: afspc.pai@peterson.af.mil

C. ROBERT KEHLER
General, USAF
Commander

GUARDIANS OF THE HIGH FRONTIER
Book Review

Wargaming for Leaders: Strategic Decision Making from the Battlefield to the Boardroom


Historians can identify multiple origins for wargaming. The roots lie in ancient Egypt, Rome, China, and India. Modern wargaming, however, began to take form in early nineteenth-century Europe and came to America in the 1880s. Around the same time, modern civilian wargaming also appeared. A half-century later, commercial wargaming arose and grew fantastically in popularity from the 1950s through the 1990s. By the beginning of the twenty-first century, despite skepticism in some quarters about modern wargaming’s efficacy, the integration of techniques drawn from commercial and military wargames was proving beneficial on levels ranging from education and training to doctrinal development and operational planning.

In Wargaming for Leaders, three eminently qualified members of the Booz Allen Hamilton (BAH) corporate team draw from their many years of relevant experience to acquaint readers with the potential benefits from, and limitations of, modern wargaming. The glue binding together their book’s three sections—Military Wargames, Wargames for Business, and Global Crisis Wargames—and individual chapters is the concept of “cognitive warfare.” The authors use this term to describe what happens when expert players’ minds interact with one another to spawn “unexpected and often startling outcomes” (p. 4). They emphasize two necessary conditions for any successful wargame: the client’s specification of a clear objective, and the presence of key groups with different equities. Even when those conditions are met, however, wargames and their scenarios are “designed to be plausible, not predictive” (p. 251).

Mark Herman, Mark Frost, and Robert Kurz summarize the development and outcomes of more than a dozen wargames they personally designed over the past couple of decades. One called “Desert Crossing” demonstrated, in June 1999, how the collective play of the participants in a nonthreatening environment “can reveal unpleasant truths about a particular strategy or set of goals” (p. 47). Another, centered on Swissair’s strategic planning, showed that just because something is called “a game does not mean its outcomes are capricious.” Sometimes a wargame can “tell a very disturbing story” (pp. 122-123). In December 2001, a bioterrorism wargame emphasized the importance of leadership and cooperation, instead of the competition central to most military and business wargames. For each example, the authors specify “The Big Idea”—the primary lesson learned—from having played the game.

While US Department of Defense employees, uniformed or civilian, might be inclined to think only the first third of this book is pertinent to their tastes, rest assured all three sections offer ample food for thought. Just as BAH’s military wargames were “designed and conducted to test a strategy or battle plan in a virtual environment before the civilian and military leadership committed the nation’s blood and treasure in the real world” (p. 81), commercial clients could test strategic plans, potential acquisitions or alliances, and new technologies in advance of making a real-world decision. Some readers will find the third section on global-crisis wargames most enticing, because it introduces the concept of “megacommunity”—“a network of organizations, drawn from the business, government, and civil sectors, that comes together to engage critical problems of mutual interest that are too big for any one of them to solve alone” (p. 227). Pioneered and promulgated by BAH, the notion of megacommunities could prove extremely useful in wargames focused on international terrorism, space protection, or asymmetric conflict.

Although Wargaming for Leaders offers outstanding examples of highly successful wargames, some readers might wish it contained more about how and why some games failed. Nonetheless, the three authors have written a truly engaging, unquestionably useful book. They pride themselves in objective and unbiased wargaming that is “about problem solving or, at a minimum, problem exposing” (p. 250). One of the most challenging problems is finding a way to manage risk when you cannot understand it, which often is the case when unforeseen change upsets traditional patterns and introduces significant discontinuities. In such circumstances, leaders cannot simply straight-line past successes into a potentially treacherous future. Rather, they must reinvent risk in a new environment, and wargames provide a mechanism for doing it.

Herman, Frost, and Kurz seek to create imagined futures “in which players can observe, work together, make decisions, and learn from outcomes in a risk-free environment” (p. 250). Within an evolving strategic environment, one where events can cause priorities to change quite rapidly and “a crisis can spin out of control even if the correct decisions to contain it are made in what once was considered good time” (p. 11), the authors of Wargaming for Leaders take pride in being able to design informative exercises in days instead of weeks or months. More importantly, they take satisfaction in knowing that revelations from wargaming help foster success on battlefields and in boardrooms around the world.

Reviewed by Dr. Rick W. Sturdevant, duty command historian, HQ Air Force Space Command.

High Frontier
We are interested in what you think of the *High Frontier* Journal, and request your feedback. We want to make this a useful product to each and every one of you, as we move forward to professionally develop Air Force Space Command’s space and missile workforce and stimulate thought across the broader National Space Enterprise. Please send your comments, inquiries, and article submissions to: HQ AFSPC/PA, High Frontier Journal, 150 Vandenberg St, Ste 1105, Peterson AFB, CO 80914-4020, Telephone: (719) 554-3731, Fax: (719) 554-6013, Email: afspc.pai@peterson.af.mil, To subscribe: hard copy, nsage@cols.com or digital copy, http://www.af.mil/subscribe.